2018-03-06

Definition : binary operation

S : set, $*$: binary operation
$* : S \times S \to S$
$*(a, b) = a * b$
$< S, * >$ (* : 적절한 조건 $\to$ Group(군), Ring(환), Field(체))

1.

Z = set of integers
$(Z, +)$

2.

$Z_n = \{0, 1, ..., n-1\}$ (when n : 양의정수)
$(Z_n, +_n)$
$+_n$: modulo n

3.

$< M_n(R), + > < M_n(R), \cdot >$

4.

$R_{2\pi} = [0, 2\pi)$, $+_{2\pi}$
$< R_{2\pi}, +_{2\pi} >$

5.

$U_n = \{z \in C | z^n = 1\}$ (n-th root of unity)
$< U_n, \cdot >$ ($\because (ab)^n = a^n b^n = 1$)
when $z = 1(cos\frac{2\pi}{n} + isin\frac{2\pi}{n}), z^n = 1$
$U_n = \left\{1, z, z^2, ..., z^{n-1}\right\}$

6.

$u = z \in C||z| = 1$ (circle)
$< u, \cdot >$

not binary operation

1.

$< Z, / >$

2.

$< M(R), + >$ ($M(R)$은 모든 크기에 해당하는 행렬)

Definition

$< S, * >$

commutative

$a * b = b * a$

associative

$(a * b) * c = a * (b * c)$

Commot(?)

$|S| < \infty$
$S = \{a_1, a_2, ..., a_n\}$
for all i, j, $a_i \cdot a_j = a_k$ for some k

Definition : issomorphism

$< S, * >, < S', *' >$
$\phi : S- > S'$
1) ϕ : one to one, onto.
2) $\phi(a * b) = \phi(a) *' \phi(b)$ (homomorphic property)
$\Leftrightarrow$
ϕ is issomorphism
S, S' 사이에 ϕ가 존재한다면 $S \;= S'$ (isomorphism)

1.

$< R(¸), + >, < R + (X¸), \cdot >$
$x- > a^x$ (some $a > 0$)
one to one

2.

$U_n = \left\{1, z, z^2, ..., z^{n-1}\right\} < U_n, \cdot > \simeq < Z_n, +_n >$
$z^i \to i$
$\phi(z^i \cdot z^j) = \phi(z^{i+j\%n})) = i + j\%n$

3.

$< Z, + >, < 2Z, + >$
$Z \to 2Z \ n \to 2n$
one to one
$\phi(n+m) = \phi(n) + \phi(m)$

How to proof not issomrophism

$(S, *)! \simeq (S', *')$
assume $< S, * > \simeq < S', *' >$
then " ... ..." holds
structure prop.
$< Q, + >, < R, + >$
$|Q| = |Z| = \aleph_0$
$|R| > \aleph_0$

1.

$< Z, \cdot \ >! \simeq < Z+, \cdot \ >$
if) ϕ exists
$x = 0 or 1 \Leftrightarrow x \cdot x = x \Leftrightarrow \phi(x) \cdot \phi(x) = \phi(x) \Leftrightarrow \phi(x) = 1$
$\phi(0) = 1, \phi(1) = 1$
not one to one
contradiction. so, $< Z, \cdot \ >! \simeq < Z+, \cdot \ >$

2.

$< Z, + >! \simeq < Q, + >$
$|Z| = |Q|$
if) ϕ exists $x is None \Leftrightarrow x + x = 3 \Leftrightarrow \phi(x) + \phi(x) =$
$\phi(3) = c in Q$
$\phi(v) = \frac{c}{2}$
v is None
contradiction. so, $< Z, + >! \simeq < Q, + >$

3.

$< R, \cdot \ > \simeq < C, \cdot \ >$
$C = \{a + bi | a, b in R\}$
$|C| = |R|$
$x^2 = -1$
?????

I don't know

????
$(G, \ \cdot \ )$: Group $G \simeq G'$
n = dim V ¡ inf $V \ = F^n (F is R or C, i think?)$
$|G| = n$
when n=4
$Z_4, Z_2 x Z_2$

Group

$< G, * >$: Group
$\Leftrightarrow$
0) * : binary operation (it might be) (closure)
1) * is associative
2) exists e in G s.t a * e = a (= e * a) (some a in G)
e : identity
3) for all a in G, exists a' s.t. a*a' = e (= a'*a)
a' : inverse of a
()로 약화해도 됨 * 기준으로 방향 중요.

uniqueness of e

if exists e, e'
$e = e * e' = e'$
contradiction

uniqueness of a'

if exists a', a''
$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$
contradiction

2018-03-08

Group 정의 정리

Definition : abelian group

Group 이며,
$a * b = b * a, (a, b \in G)$ 인 경우 (교환법칙 성립)

0.

semi-group, mono-group 언급을 함.

1. $(\mathbb{Z}, +)$

2. $(\mathbb{Z}_n, +_n)$

1. 결합법칙 성립
2. $e = 0$
3. $a' = 0$ if $a = 0$ else $n - a$

3. $(Q, +), (R, +), (C, +)$

4. $(M_{m \times n}(R), +)$

5. $(Q^*, \cdot), (R^*, \cdot), (C^*, \cdot)$

$Q^* = Q - \{0\}$
$(Z^*, \cdot)$은 역원이 없어서 안됨

6. $(GL(n, R), \cdot)$

GL : General Linear
$GL(n, R) = n \times n$ matrix : invertible
$(M_n(R), \cdot)$은 역원(역행렬)이 없어서 안됨
$n = 1, GL(1, R) = R*$
$n \geq 2, |GL(n, R)| = \infty$ and not abelian (교환법칙 성립 X)

7. S_n

$S_n = \{\sigma : I_n \to I_n\}$, $I_n = \{1, 2, ..., n\}$
$n = 1, 2$: abelian
$n \geq 3$: not abelian
$|S_n| = n!$

8. $(Q^+, *)$ when $*$ is $a * b = (ab/2)$

$e = 2, a' = 4/a$

결합법칙 성립하면, 동형인 것도 결합법칙이 성립한다

1.

$(U_n, *) \to (Z_n, +_n)$은 동형, 둘다 결합법칙 성립
$\phi((z^i z^j) z^k) = \phi(z^i (z^j z^k))$
$\Leftrightarrow$
$(i +_n j) +_n k = i +_n (j +_n k)$

note

$(G, *)$
$* \to +$
$e = 0, a' = -a$
$(G, \cdot)$
$* \to \cdot$ or None
$e = e, a' = a^{-1}$

정리

$(G, *)$: group
1. 2. : cancellation law

1. $a * c = b * c \Rightarrow a = b$

right cancellation law
양변 오른쪽에 c'을 $*$하면 된다.

2. $c * a = c * b \Rightarrow a = b$

left cancellation law

3.

$\forall a, b \in G, \exists x, a * x = b$
$x = a' * b$
x is unique
if $a * x = b = a * x', x = x'$ (cancellation law) $\square$
$\forall a, b \in G, \exists x, x * a = b$

머지

1. $(\mathbb{Z}, +)$

$2 + x = 5$
$-2 + (2 + x) = -2 + 5$
$x = 3$

2. $(\mathbb{Q}^*, \cdot)$

$2x = 5$
$2^{-1}(2x) = 2^{-1}5$
$x = 5/2$

Cor(corollary)

$(G, *)$

1. uniqueness of e, a'

cancellation law

2. $(a * b)' = b' * a'$

하면 됨

3.

if $|G| < \infty$
$|G| \times |G|$로 $*$ 값을 table로 나타내면, 각 행의 $|G|$개의 값은 다르다. (by left cancellation law) 마찬가지로, 각 열의 $|G|$도 다르다. (by right cancellation law)

Remark:

$(G, *)$가 다음 3개를 만족해도 Group이다. (왼쪽만 성립하는 경우, 오른쪽도 마찬가지)
1) association
2) $\exists e, e * a = a$
3) $\exists a', a' * a = e$

Lemma:

$(G, *)$ with 1), 2), 3) $\Rightarrow (c * c = c \Rightarrow c = e)$
pf. $c' * (c * c) = c' * c$
$(c' * c) * c = c' * c$
$e * c = e$
$c = e$ $\square$

To Show : $a * a' = e$ and $a * e = a$

$(a * a') * (a * a') = a * (a' * a) * a' = a * e * a' = a * a'$
by Lemma, $a * a' = e$
$a * e = a * (a' * a) = (a * a') * a = e * a = a$

머지

$|G| = 1$

$G = \{e\}$

$|G| = 2$

$G = \{e, a\}$
then, $a * a = e$ ($\because a * a! = a * e$)
$\cdot \to +_2$
$e \to 0$

$a \to 1$
이러면, 동형인 것을 알 수 있다. $G \simeq \mathbb{Z}_2$

$|G| = 3$

$G = \{e, a, b\}$
e a b e e a b a a b e b b e a
일 수 밖에 없다.
$\cdot \to +_3$
$e \to 0$
$a \to 1$
$b \to 2$

$|G| = 4$

$G = \{e, a, b, c\}$
e a b c e e a b c a a e c b b b c a e c c b e a
$\cdot \to +_4$
$e \to 0$
$a \to 2$
$b \to 1$
$c \to 3$
e a b c e e a b c a a b c e b b c e a c c e a b
$\cdot \to +_4$
$e \to 0$
$a \to 1$
$b \to 2$
$c \to 3$
위 두개는, $\simeq Z_4$
e a b c e e a b c a a e c b b b c e a c c b a e
$\cdot \to +_{2\times 2}$
$e \to (0,0)$
$a \to (0,1)$
$b \to (1,0)$
$c \to (1,1)$
위는 $\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$

What is $G_1 \oplus G_2$

$G_1 \oplus G_2$
$(a_1, b_1) + (a_2, b_2), (a_1, a_2 \in G_1)(b_1, b_2 \in G_2)$
$(a_1 + a_2, b_1 + b_2)$

Proof $\mathbb{Z}_4 ! \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$x * x = e$을 만족하는 갯수
$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 는 4개
$\mathbb{Z}_4$ 는 2개
동형일 수 없다.

Klein 4-group

뭔가를 저렇게 부른다.

Note

$G_6 ! \simeq S_3 : Z_6$은 교환법칙 성립, S_3은 성립안함
G_6의 동형은 Z_6 밖에 없다.

2018-03-13

SubGroup 정의

Definition : SubGroup

$< G, * >$: group
$H \subseteq G$
$< H, * >$: group
$\Leftrightarrow$
H: subgroup of G

Note

$H \leq G$
$H < G \Leftrightarrow H \leq G, H! = G$

1.

$< \mathbb{C}, + > \geq < \mathbb{R}, + > \geq < \mathbb{Q}, + > \geq < \mathbb{Z}, + >$

2.

$< \mathbb{C}^*, * > \geq < \mathbb{R}^*, * > \geq < \mathbb{Q}^*, * > \geq < \mathbb{Z}^*, * >$

3.

$< \mathbb{C}, * > \geq < \mathbb{U}, * > \geq < \mathbb{U}_n, * >$

4.

$< GL(n, \mathbb{R}), * > \geq < SL(n, R), * > \geq < SO(n, R), * >$
SL : $detA = 1$
SO : $A^t A = I$

5.

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$
$\mathbb{Z}_4 \geq \{0, 2\} \geq \{0\}$

6.

V = eabc eeabc aaecb bbcea ccbaa
abelian group
$V \geq \{e, a\}$ $V \geq \{e, b\}$ $V \geq \{e, c\}$ $V \geq \{e\}$

Theorem : SubGroup

$< G, * >$: group
$H \subseteq G$
$H \leq G$
$\Leftrightarrow$
1. *: closed in H
2. $e_G \in H$
3. $\forall a \in H, a_G^{-1} \in H$

1. by definition of group

2. proof

$e_H \in H$
$e_H x = x = e_G x$
$e_H = e_G$

3. proof

$a_H^{-1} \in H$
$a a_H^{-1} x = e = a a_G^{-1}$
$a_H^{-1} = a_G^{-1}$

Note $\Leftarrow$

association
because they are in G

Note

$< G, + >, < G, \cdot >$
$a + b, a \cdot b$
$(a + b) + c = a + (b + c), (ab)c = a(bc)$
$0, 1(ore)$
$-a, a^{-1}$
$ma + na = (m + n)a, a^m \cdot a^n = a^{m+n}$

proof of last eqation

$m > 0, m \geq 0, n > 0, n \geq 0$나눠서

??

$z =$ root of unity (when 12)
$|\{z^n | n \in \mathbb{Z}\}| = 12$
$|\{n2 | n \in \mathbb{Z}\}| = \infty$

Theorem. That is subgroup — subgroup generated by a

G : `group`
$a \in G$
$H = \{a^n | n \in \mathbb{Z}\} \leq G$

proof

1) closed
2) $a^0 = e$
3) $(a^s)^{-1} = a^{-s} \in H$

1.

$H =< a >$, call as "subgroup generated by a"

2.

if $\exists a, G =< a >$, G : cycle group

3.

$| < a > | = \infty \Leftrightarrow$ a is infinite order
$| < a > | = n \Leftrightarrow$ order of a is n

Ex 1.

$|\mathbb{Z}_4| = 4$
$\mathbb{Z}_4 =< 1 >=< 3 >$
$| < 2 > | = 2$

Ex 2.

$|\mathbb{Z}| = \infty$
$\mathbb{Z} =< 1 >=< -1 >$
if $n \neq -1, 1, < n > \neq \mathbb{Z}$

Ex 3.

$\mathbb{Z}_{\nparallel} \not= =< 1 >=< -1 >=< 5 >=< 7 >$

4.

$H = \{a^n | n \in \mathbb{Z}\} \leq G$
H : smallest subgroup of G contains a
1. $H \leq G$
2 if $K \leq G, a \in K \Rightarrow H \leq K$

Theorem

$G =< a > \Leftrightarrow G$: abelian
proof. $a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r$
역은 성립안함. Klein 4-gourp

To show

$G =< a >$
$|a| = \infty \Rightarrow G \simeq < \mathbb{Z}, + >$
$|a| = n \Rightarrow G \simeq < \mathbb{Z}_n, +_n >$

Division Algorithm for $\mathbb{Z}$

There is unique q, r s.t. $m = qn + r, 0 \leq r < n$
있다는 것은 수직선에 그림그려서
유일하다는 것은 같은 것이 두 개 있다고 가정하면
$n | r_1 - r_2 = 0$

Theorem

$G =< a >$
$H \leq G \Rightarrow H$: cyclic
proof.
1) $H = \{e\}, H =< e >$ finish
2) $H \neq \{e\}$
$\exists n \neq 0, a^n \in H$
We can choose the smallest $m \in \mathbb{Z}_+$

Claim $H =< a^m >$

$\because < a^m > \subseteq H$
proof $H \subseteq < a^m >$
$a^n = b \in H$
$n = qm + r, 0 \leq r < m$
$a^n = (a^m)^q \cdot a^r$
$a^{n-mq} = a^r$
$r = 0$ (if $r > 0, r < m$)
So, $H =< a^m >$

2018-03-15

gcd

$d = gcd(r, s)$
1) $d|r, d|s$
2) $d'|r, d'|s \Rightarrow d'|d$

Check

$H \equiv \{nr + ms|n, m \in \mathbb{Z}\}$
then
$H =< gcd(r, s) >$

1. subgroup

$(n_1r+m_1s)+(n_2r+m_2s) = (n_1+n_2)r+(m_1+m_2)s$
$0r + 0s = 0 \in H$
$(-n)r + (-m)s$

2.

$d|(1r + 0s = r)$, $d|(0r + 1s = s)$
$r = d'k, s = d'l$ 이면 $d'|d$을 보이자.
$\exists n_0, m_0 \mid d = n_0r + m_0s$
$= d'(n_0k + m_0l)$
so, $d'|d$

relative prime

*

r, s : 서로소
$r|sm \Rightarrow r|m$
$\because 1 = ar + bs \Rightarrow m = arm + bsm$

Structure Thm of Cyclic grps

$G =< a >$
1) $|G| = \infty \Rightarrow G \simeq < \mathbb{Z}, + >$
2) $|G| = n \Rightarrow G \simeq < \mathbb{Z}_n, +_n >$

pf 1.

Claim 1

$a^m \neq e, \forall m \in \mathbb{Z}^+$
suppose $a^m = e, m \in \mathbb{Z}^+$
$G = \{a^s|s \in \mathbb{Z}\}$
$|G| <= m < \infty$

Claim 2

if $h \neq k, a^h \neq a^k$
wlog $h > k$
$a^{h-k} = e$, 모순 by Claim 1.

proof

$\phi(a^i) = i$
$\phi(a^i \cdot a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j)$

pf 2.

Claim 1

$\exists m \in \mathbb{Z}^+ \mid a^m = e$
suppose $\forall m \in \mathbb{Z}^+ \mid a^m \neq e$
Claim2 in pf1 $|G| = \infty$

proof I

m_0 : the smallest positive integer
$\exists a^{m_0} = e$ (to show $m_0 = n$)
$G = \left\{e, a, a^2, ..., a^{m_0-1}\right\}$
$|G| = n = m_0$
$(a^h \neq a^k \mid \mathtt{when} m_0 > h > k)$
$\because a^{h-k} = e \mathtt{and} h - k < m_0$

proof II

$\psi(a^i) = i$
$\psi(a^i \cdot a^j) = \psi(a^{i+_nj}) = i +_n j = \psi(a^i) +_n \psi(a^j)$

*

$a \in G =< a >$
$| < a > | = n \Leftrightarrow n$ is the smallest pos. integer $\exists a^n = e$

Structure Thm of Finite Cyclic grps

$\mathbb{Z}_n$

Thm

$G =< a >, |G| = n$
1) $a^s = b \in G, H =< a^s >\Rightarrow |H| = \frac{n}{\mathtt{gcd}(n,s)}$
2) $< a^s >=< a^t >\Leftrightarrow \mathtt{gcd}(s, n) = \mathtt{gcd}(t, n)$

(A)

$d = \texttt{gcd}(n, s)$
$\frac{n}{d}, \frac{s}{d}$ 서로소

pf 1.

$| < a^s > | = m \Leftrightarrow (a^s)^m = e$ (m 은 smallest pos integer)
$\frac{sm}{n} \in \mathbb{Z}$
$\frac{(s/d)m}{(n/d)} \in \mathbb{Z}$
$(n/d)|m$ m이 smallest pos integer이면, $m = (n/d)$ positive

pf 1. (other proof)

$d = an + bs$
$a^d \in < a^s >$
$\therefore < a^d > \leq < a^s >$
$a^s \in < a^d >$ $(\because d|s)$
$\therefore < a^s > \leq < a^d >$
$\therefore < a^s > = < a^d > = n/d$

pf 2.

$\Rightarrow$

by 1)

$\Leftarrow$

$d = \texttt{gcd}(s, n) = \texttt{gcd}(t, n)$
$< a^s > = < a^d > = < a^t >$

Cor.

$\mathbb{Z}_n = < 1 > = < r >$ $(\texttt{gcd}(r, n) = 1)$

?

G : group

Note

$\{i | i \in I\}$
$\bigcap_{i \in I} S_i = \{x | x \in S_i, \forall i \in I\}$

Thm

$H_i \leq G$, $(i \in I) \Rightarrow \bigcap_{i \in I} H_i \leq G$

??

전체 G
어떤 집합 S를 포함하는 모든 subgroup들을 가진 집합을 K라 하자.
K의 모든 원소들의 교집합은 G의 subgroup이다.
??
??

Thm

$S = \{a_i | i \in I\}$
$< S > = \left\{ a_{i_1}^{n_{i_1}} a_{i_2}^{n_{i_2}} ... a_{i_k}^{n_{i_k}} \right\} \equiv K$
K는 결합법칙 성립 항등원 있고, 역원있음 : group
$< S > \subseteq K$??
$K \subseteq < S >$??

Eg

$\mathbb{Z}_6 = < 1 > = < \{2, 3\} > = < \{0, 1, 2, 3, 4, 5\} >$

2018-03-20

Cayley Digraphs

directed graph
Graph = verice(s) + edge(s)
$xa = y$면 $x \to y$인 Edge를 만들자.
$< S = \{a, b, c\} >= G$라 하면, a로 인해 생성되는 간선, b로 인해 생성되는 간선, c로 인해 생성되는 간선이 있다.
$b^2 = e$인 경우에는, $b^{-1} = b$이므로 양방향 간선으로 표현해도 된다.

Eg.

$\mathbb{Z}_6 =< 1 >=< 2, 3 >$로 그래프를 그릴 수 있다.
이 때, 3에 대해서는 $3 +_6 3 = 0$이므로 양방향 간선으로 연결 가능

성질 4가지. I, II, III, IV.

I. 경로가 무조건 존재한다.
II. 정점 a에서 b로 가는 간선은 하나뿐이다.
III. 적절한 수를 곱하면 a에서 b로 한번에 갈 수 있다. (??)
IV. 특정 경로 a와 b가 같다면, 어느 지점에서 a와 b를 적용해도 같다. 생략
vertex, arc with (I) - (IV) $\Rightarrow \exists G$, G : group / Cayley Digraphs

뭔가 정의하고 군임을 증명함

1. pick e
2. G = set of vertices
$G \times G \to G$
$(g, h) \to g * h$
is well define 된다. (위의 성질 4가지에 의해서)
G는 Group이다.
1. 결합법칙 성립
2. 항등원 존재
3. 역원 존재 (역경로)

Permutation

A : set
$S_A \equiv \{\sigma : A \to A, 1-1, onto\}$
$S_A \times S_A \to S_A$
$(\sigma, \tau) \to \sigma \times \tau \equiv \sigma\tau$

check

$\sigma\tau$ is $1-1, onto$

Thm. It is Group

1. 결합법칙 성립
2. 항등원(I)
3. 역원

Remark

$A \to B$ (by function F, 1-1, onto)
$\Rightarrow S_A \simeq S_B$ as groups
$|A| = n = |I_n| = |\{1, 2, 3, ..., n\}$
$S_A \simeq S_{I_n} \equiv S_n$

Why?

$\sigma \in S_A \to \phi(\sigma) \in S_B$
$a- > \sigma(a)$
$f(a)- > f(\sigma(a))$
$S_A \to S_B$ (byϕ)
$\sigma \to \phi(\sigma) = \bar{\sigma}$
$\bar{\sigma}(f(a)) = f(\sigma(a))$로 생각

Check

1. $\bar{\sigma} \in S_B$, 1-1, onto $(B \to B)$
$\bar{\sigma}(b_1) = \bar{\sigma}(b_2)$
$\bar{\sigma}(f(a_1)) = \bar{\sigma}(f(a_2))$
$f(\sigma(a_1)) = f(\sigma(a_2)) \to a_1 = a_2$ 1-1
$\forall b' \in B$
find $b \in Bs.t.\bar{\sigma}(b) = b'$
슥삭슥삭
2. ϕ : 1-1, onto
3. $\phi(ab) = \phi(a)\phi(b)$