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.