

Ch. 2 Groups

① Binary operation

Def. Let G be a set

A binary operation on G is a map

from $G \times G$ to G

i.e. it assigns to every ordered pair $(a, b) \in G \times G$
an element in G , usually written as ab .

Examples:

① $G = \mathbb{Z}$ integers

binary operation: $+$

$(n, m) \mapsto n+m$

$$\textcircled{b} \quad G = \{0, 1, 2, \dots, n-1\}$$

binary operation: addition mod n

it assigns to $(r_1, r_2) \in G \times G$ the number $r_1 + r_2 \pmod n$

e.g. $n=5$

$$(3, 4) \mapsto 7 \pmod 5 = 2$$

\textcircled{c} can do same for multipl.

i.e. multid. defines binary op. for \mathbb{Z}

and multipl. mod n " " " for $\{0, 1, \dots, n-1\}$

\textcircled{d} S any set

$$G = \{f: S \rightarrow S \text{ map}\}$$

binary operation: concatenation of maps

$$(f, g) \rightarrow fog$$
$$fog(x) = f(g(x)) \quad x \in S.$$

example: $S = \{1, 2\}$

have 4 elements in S

$$f_1: \begin{array}{l} 1 \rightarrow 1 \\ 2 \rightarrow 1 \end{array}$$

$$f_2: \begin{array}{l} 1 \rightarrow 1 \\ 2 \rightarrow 2 \end{array}$$

$$f_3: \begin{array}{l} 1 \rightarrow 2 \\ 2 \rightarrow 1 \end{array}$$

$$f_4: \begin{array}{l} 1 \rightarrow 2 \\ 2 \rightarrow 2 \end{array}$$

Def. (Group)

Let G be a set with a binary operation. (usually referred to as multiplication). G is called a group if our binary operation satisfies

- (a) Associativity: $(ab)c = a(bc)$ for all a, b, c in G
- (b) Identity element: There exists an element e in G such that $ae = a = ea$ for all a in G
- (c) Inverse: For every $a \in G$ there is an element $b \in G$ such that $ab = e = ba$

Examples:

① $(\mathbb{Z}, +)$ i.e. integers with operation addition.

Remark: we will be somewhat casual about associativity at this point. usually holds for any reasonable operation.

check: identity element: 0 $0+n = n = n+0$ ✓

inverse: for given n we have
 $n+(-n) = 0 = (-n)+n$ ✓

same works for $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$

② $G = \{0, 1, \dots, n-1\}$ addition mod n

group with identity 0

for given $a \in G$ inverse is number $b \in G$

s.t. $a+b \pmod n = 0$ take $b = n-a$

$\Rightarrow a+b \pmod n = a+(n-a) \pmod n = n \pmod n = 0$

$\Rightarrow n-a$ is inverse of $a \pmod m$.

③ what about multiplication? (for \mathbb{Z} , or \mathbb{R} ?)

observation: 0 can not have an inverse for multiplication!

identity elem. for multiplication: $1 \cdot n = n = n \cdot 1$ ✓

problem: find inverses:

$0 \cdot n = 0$ for all $n \Rightarrow 0$ can not have an inverse.

5 can not have an inverse in \mathbb{Z} for multiplication

$5 \cdot n \neq 1$ for any integer n .

result 1: $(\mathbb{Z} \setminus \{0\}, \cdot)$ can not be a group with operation \Rightarrow multiplication

result 2: $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group

identity: 1

inverse of p/q is q/p ✓

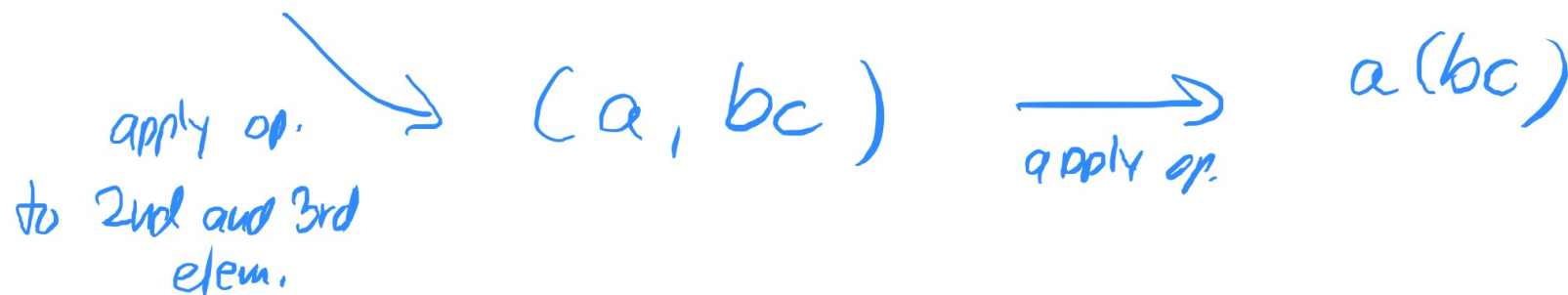
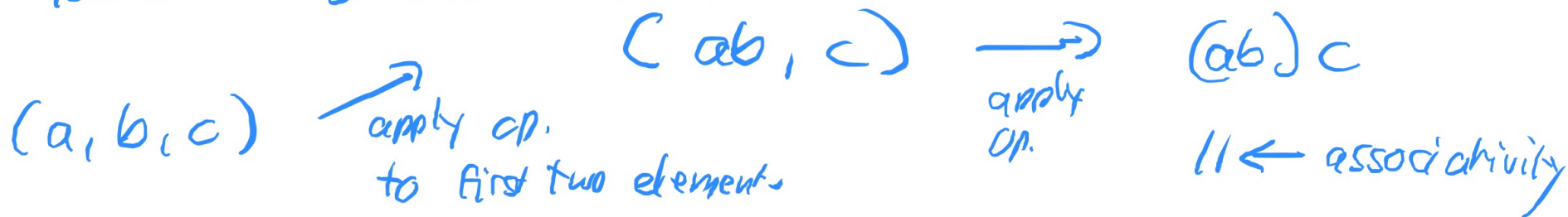
④ consider $(\mathbb{Z}, -)$ not a group.
- is not associative.

e.g. $(5-3)-2 \neq 5-(3-2)$

$$\begin{array}{ccc} & & \\ & \parallel & \parallel \\ & 0 & 4 \end{array}$$

associativity means:

if you have 3 elements of your set, say a, b, c



5

consider 2×2 matrices (over \mathbb{R})

operation: matrix multiplication

can show: associative (not here)

• identity element: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}$

$$\mathbf{I}A = A = A\mathbf{I}$$

for any 2×2 matrix A

• inverse? A has inverse $\Leftrightarrow \det(A) \neq 0$

Given $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$\det A = ad - bc$$

check: $AB = \mathbf{I} = BA$

Result: The set $GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{R} \right\}$
 $ad - bc \neq 0$

with operation matrix multiplication
is a group

Observe: in general $AB \neq BA$ for arbitrary 2×2 matrices
 A, B .

Def. A group G is called Abelian if $ab = ba$ for all
 a, b in G .

Rem. Our last example $GL(2, \mathbb{R})$ shows that not
every group is Abelian!
All other examples so far were Abelian.

⑥ have seen: $\{0, 1, \dots, n-1\}$ is a group
for addition mod n

what about mult. mod n ?

again: identity elem. for mult. = 1.

inverses? again: 0 can not have an inverse.

consider $(\{1, 2, \dots, n-1\}, \cdot)$

$n=3$

$\{1, 2\}$.

$$1 \cdot 1 = 1$$

$$1 \cdot 2 = 2$$

$$2 \cdot 1 = 2$$

$$2 \cdot 2 = 4 = 1 \pmod{3}$$

inverse of 2 = 2

Result: $(\{1, 2\}, \cdot)$ mult. mod 3 is a group

Challenge: show:
 $\{1, 2, 3\}$ is NOT a group
for mult. mod 4
(can assume associativity).