§1 Introduction

Definition 1.1 Let $(G, *)$ be a non-empty set with a binary operation $(*)$.
G is a group if the following axioms hold:

(G1) $\forall a, b, c \in G \quad (a*b)*c = a*(b*c)$ Associativity

(G2) $\exists e \in G$ s.t. $\forall a \in G \quad e*a = a = a*e$ Identity

(G3) $\forall a \in G \quad \exists a^{-1} \in G$ s.t. $a*a^{-1} = e = a^{-1}*a$ Inverse

binary $* \; G \times G \longrightarrow G \quad (g,h) \mapsto g*h$ Often omit $*$, write $\cdot$, $+$, etc...

e.g. $\mathbb{Z}, +$ binary $(\forall x, y \in \mathbb{Z} \; x+y \in \mathbb{Z})$, $\{1,2,3\}, +$ NOT binary $(3+2 = 5 \notin \{1,2,3\})$

(a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ ✓

(b) $(\mathbb{Q}, \cdot)$ $e = 1$ but 0 has no inverse ✗

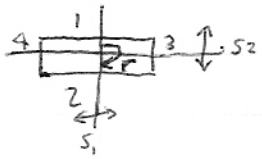
(c) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ ✓ where $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

(d) $(M_{m,n}(\mathbb{R}), +)$, $(GL_n(\mathbb{R}), \cdot)$

(e) $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ $\quad \bar{i} \bar{+} \bar{j} = \begin{cases} \overline{i+j} & \text{if } i+j < m \\ \overline{i+j-m} & \text{if } i+j \geq m \end{cases}$

(f) permutation groups.
↓ Galois (1811 - 1832)

Symmetries



s_1: $1 \to 1$, $2 \to 2$, $3 \to 4$, $4 \to 3$

s_2: $1 \to 2$, $2 \to 1$, $3 \to 3$, $4 \to 4$

r: $1 \to 2$, $2 \to 1$, $3 \to 4$, $4 \to 3$

$id = e$.

$s_1 \circ s_2$ (2nd, 1st): $1 \to 2 \to 2$, $2 \to 1 \to 1$, $3 \to 3 \to 4$, $4 \to 4 \to 3$ $= r$

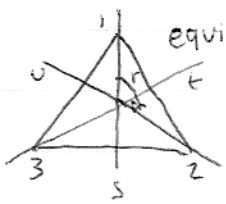
$s_1 \circ s_2 = r = s_2 \circ s_1$

$s_1 \circ s_1 = e \quad s_2 \circ s_2 = e$

$r \circ r = e \quad r \circ s_1 = s_2 = \ldots$

	e	s_1	s_2	r
e	e	s_1	s_2	r
s_1	s_1	e	r	s_2
s_2	s_2	r	e	s_1
r	r	s_2	s_1	e

$\times$	a
b	$b \times a$



equilateral triangle

	1 ↓	2 ↓	3 ↓
r	2	3	1
r^2	3	1	2
s	1	3	2
t	2	1	3
u	3	2	1

$r \curvearrowright 120°$

$r^2 = r \circ r \curvearrowright 240°$

$id = e = r^3 = r \circ r \circ r \curvearrowright 360°$

$u = s \circ r$: $1 \to 2 \to 3$, $2 \to 3 \to 2$, $3 \to 1 \to 1$

etc $\rightsquigarrow$ composition is a binary operation.

$(\{e, r, r^2, s, t, u\}, \circ)$ group?

$=id$	id	r	r^2	s	t	u
$e=id$	id	r	r^2	s	t	u
r	r	r^2	id	t	u	s
r^2	r^2	id	r	u	s	t
s	s	u	t	id	r	r^2
t	t	s	u	r^2	id	r
u	u	t	s	r	r^2	id

$r \circ r^2 = r^3 = id.$

$s \circ r = u \quad r \circ s = t$

$1 \to 1 \to 2$
$2 \to 3 \to 1$
$3 \to 2 \to 3$

- each element turns exactly once in each row and column
- $id = e$
- each element has inverse.
- composition of maps is associative