

Algebra I

# Group Theory

Book 1

A group is a set  $G$  with a binary operation  $*$  which has an identity element; the operation is associative; and every element has an inverse.

Eg.  $\mathbb{R}$  = set of real numbers under addition '+'. Its identity element is 0.

$$0 + x = x$$

$$(x+y) + z = x + (y+z)$$

$$x + (-x) = 0 = (-x) + x$$

for all  $x, y, z \in \mathbb{R}$

$(\mathbb{R}, +)$  is a group.

$(\mathbb{R}, \times)$  (real numbers under multiplication) is almost but not quite a group. (0 does not have an inverse). 1 is the identity.

$\mathbb{R}^* = \{\text{all nonzero real numbers}\} = \{a \in \mathbb{R} : a \neq 0\}$  is a group under multiplication.

$$1a = a$$

$$(ab)c = a(bc)$$

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

$$a^{-1} = \frac{1}{a}$$

for all  $a, b, c \in \mathbb{R}^*$ .

$(\mathbb{R}^*, \times)$  is a group.

$\mathbb{R}$  with the operation  $x * y = x + y + 7$ . This is a group  $(\mathbb{R}, *)$ . For all  $x, y, z \in \mathbb{R}$ ,

$$(x * y) * z = (x + y + 7) + z + 7 = x + y + z + 14 = x + (y + z + 7) + 7 = x * (y * z)$$

so  $(\mathbb{R}, *)$  is associative. Note that  $-7 \in \mathbb{R}$  is an identity element since

$$\left. \begin{array}{l} -7 * x = (-7) + x + 7 = x \\ \text{and } x * (-7) = x + (-7) + 7 = x \end{array} \right\} \text{ for all } x \in \mathbb{R}. \quad \text{So } -7 \in \mathbb{R} \text{ is an identity element for } '*'$$

$$\left. \begin{array}{l} (-x-14) * x = (-x-14) + x + 7 = -7 \\ x * (-x-14) = x + (-x-14) + 7 = -7 \end{array} \right\} \text{ for all } x \in \mathbb{R}. \quad \text{So } -x-14 \text{ is an inverse element for } x.$$

$$(x+y) * z = x * (y+z)$$

$$\Rightarrow (x+y+7) + z+7 = x + (y+z+7) + 7$$

$$\Leftrightarrow x+y+z+14 = x+y+z+14$$

so  $(\mathbb{R}, *)$  is associative.

$$\Rightarrow 7-5 = 3-5$$

$$\Rightarrow z = -2$$

$$\Rightarrow (z)^2 = (-z)^2$$

$$\Rightarrow 4 = 4$$

$$(x+y) * z = (x+y+7) + z+7$$

$$= x+y+z+14$$

$$= x + (y+z+7) + 7$$

$$= x * (y+z)$$

$(\mathbb{Q}, +)$  is a group.  $\mathbb{Q} = \{\text{rational numbers}\}$

$(\mathbb{Q}^*, \times)$  is a group.

$\mathbb{Q}^* = \mathbb{Q} - \{0\} = \{\text{all nonzero rational numbers}\}$

$(\mathbb{N}, +)$  is not a group

$$\mathbb{N} = \{1, 2, 3, 4, \dots\} = \mathbb{Z}^{>0}$$

$$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \dots\} = \mathbb{Z}^{\geq 0}$$

$$\mathbb{Z} = \{\text{integers}\} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

$(\mathbb{Z}, +)$  is a group.

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

Subgroup      Subgroup

$$-\frac{5}{3} \in \mathbb{Q}$$

$$\frac{172}{100} = 1.72 \in \mathbb{Q}$$

$$\pi \notin \mathbb{Q}$$

$$\sqrt{2} \notin \mathbb{Q}$$

but  $(\mathbb{R}^*, \times)$  is not a subgroup  $(\mathbb{R}, +)$

In  $\mathbb{R}^*$ ,  $2 \cdot 3 = 6$  but in  $(\mathbb{R}, +)$ ,  $2+3=5$

(although  $\mathbb{R}^* \subseteq \mathbb{R}$ )  
subset

$GL_n(\mathbb{R}) = \{ \text{invertible } n \times n \text{ matrices with real entries} \}$  is the general linear group

$GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$ ,  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ,  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$GL_n(\mathbb{R})$  is a multiplicative group with identity  $I = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$

$GL_n(\mathbb{R})$  is not commutative for  $n \geq 2$ .

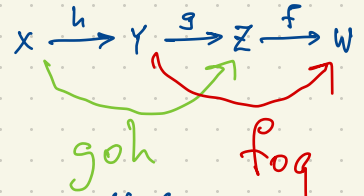
$GL_1(\mathbb{R})$  is commutative.

$(G, *)$  is Abelian if  $x * y = y * x$  for all  $x, y \in G$ .  
(abelian)

$GL_n(\mathbb{R})$  is abelian for  $n=1$ ; nonabelian for  $n \geq 2$ .  $\begin{bmatrix} 1 & 3 \\ -1 & 7 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 1 & 5 \end{bmatrix} = \begin{bmatrix} 5 & 15 \\ 5 & 35 \end{bmatrix}$  whereas  $\begin{bmatrix} 2 & 0 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ -1 & 7 \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ -1 & 38 \end{bmatrix}$ .

$GL_1(\mathbb{R}) \cong \mathbb{R}^*$  (these are isomorphic groups i.e. essentially the same group. Since  $\mathbb{R}^*$  is abelian, so is  $GL_1(\mathbb{R})$ .)

Function composition is associative:  $(f \circ g) \circ h = f \circ (g \circ h)$



If  $x \in X$  then  $h(x) \in Y$ ,  $g(h(x)) \in Z$ ,  $f(g(h(x))) \in W$ .  
 $(f \circ g \circ h)(x)$

Because matrix multiplication is expressing the composition of linear transformations, it is associative but not necessarily commutative.

If  $X$  is any set, the bijections  $X \rightarrow X$  (i.e.  $f$  one-to-one and onto) form a group under composition. This is the Symmetric group

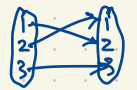
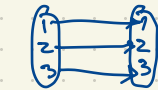
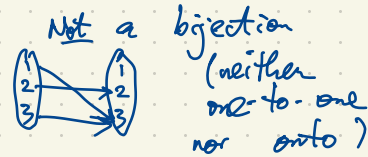
$$G = \text{Sym } X = \{ \text{bijections } X \rightarrow X \} = \{ \text{permutations of } X \}$$

eg.  $X = [3] = \{1, 2, 3\}$

(Notation:  $[n] = \{1, 2, 3, \dots, n\}$ .)

There are exactly  $3! = 6$  bijections  $[3] \rightarrow [3]$ .

$n! = 1 \times 2 \times 3 \times \dots \times n$   
( $n$  factorial) is the number of permutations of  $[n]$ .

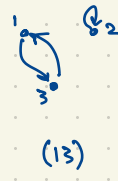
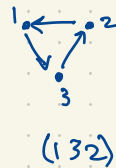
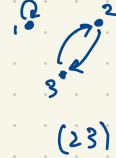
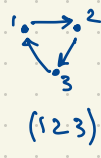
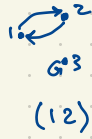
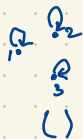


$x$	$f(x)$
1	1
2	2
3	3

$x$	$f(x)$
1	2
2	1
3	3

$|S_3| = 6$ .  $S_3$  is a non-abelian group of order 6.  
 $S_3$  is the smallest non-abelian group.

In  $S_3$ ,  
 $(12)(13) = (132)$   
 $(13)(12) = (123)$



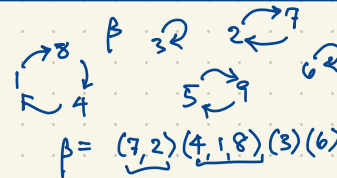
cycle notation for  $\text{Sym } [3] = S_3 = \{ (1), (12), (13), (23), (123), (132) \}$

eg.  $n = 9$



$$\alpha = (1, 7, 3, 4)(2, 5)(6, 8, 9)$$

$n$	$\alpha(n)$	$\beta(n)$	$\alpha\beta(n)$
1	7	8	9
2	5	7	3
3	4	3	4
4	1	1	7
5	2	9	6
6	8	6	2
7	3	2	5
8	9	4	1
9	6	5	2



$$\beta = (7, 2)(4, 1, 8)(3)(6)(5, 9) = (1, 8, 4)(2, 7)(5, 9)$$

$$(7, 2) = (2, 7)$$

$$(4, 1, 8) = (1, 8, 4) = (8, 4, 1) \quad (3) = (1)$$

$$\alpha\beta = \alpha \circ \beta = (1, 9, 2, 3, 4, 7, 5, 6, 8) = (1, 7, 3, 4)(2, 5)(6, 8, 9)(1, 8, 4)(2, 7)(5, 9)$$

$$\beta\alpha = \beta \circ \alpha = (1, 2, 9, 6, 4, 8, 5, 7, 3) = (1, 8, 4)(2, 7)(5, 9)(1, 7, 3, 4)(2, 5)(6, 8, 9)$$

If  $\alpha, \beta$  are permutations then  $\alpha\beta \neq \beta\alpha$  in general but they have the same cycle structure.

The order of a group  $G$  is  $|G|$ , the number of elements in the group. (finite or infinite)

$$|S_n| = n!$$

$$|GL_n(\mathbb{R})| = \infty$$

$S_n$  is nonabelian for  $n \geq 3$ .

$S_2 = \{(1), (12)\}$  is abelian.

In  $S_n$ , disjoint cycles always commute, e.g. in  $S_7$ ,  $(137)(26) = (26)(137)$

If two permutations commute, must they have disjoint cycles?

$$\alpha = (135)(246)$$

$$\beta = (12)(34)(56)$$

Note: The two 3-cycles in  $\alpha$  intersect with the three 2-cycles in  $\beta$ .



$$\alpha\beta = (135)(246)(12)(34)(56) = (145236)$$

$$\beta\alpha = (12)(34)(56)(135)(246) = (145236)$$

$S_n$  acts on  $[n] = \{1, 2, \dots, n\}$  (the  $n$  points that we are permuting)

Do not confuse  $S_n$  with  $[n]$ . **THIS IS NOT THAT.**  $|S_n| = n!$ ,  $|[n]| = n$ .

Typically, groups act on things (generically called points).

Typically, groups describe symmetries of things.

A cube has 48 symmetries forming a group  $G$  of order 48.  $|G| = 48$ .

24 of these are direct symmetries preserving orientation: these are rotations.

24 of these are virtual symmetries which cannot be obtained by physical motion.

