Algebra I

Group Theory

Book 1

A <u>group</u> 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.

$$\left.\begin{array}{l} 0+x=x \\ (x+y)+z = x+(y+z) \\ x+(-x) = 0 = (-x)+x \end{array}\right\} \quad \text{for all } x,y,z\in\mathbb{R}$$

$(\mathbb{R},+)$ 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.

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

$$\begin{array}{l} 1a = a \\ (ab)c = a(bc) \\ a\cdot a^{-1} = a^{-1}\cdot a = 1 \end{array} \qquad a^{-1} = \tfrac{1}{a} \qquad \text{for all } a,b,c\in\mathbb{R}^\times.$$

$(\mathbb{R}^\times,\times)$ 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

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

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

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

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

$$7=3$$
$$\Rightarrow 7-5 = 3-5$$
$$\Rightarrow 2=-2$$
$$\Rightarrow (2)^2 = (-2)^2$$
$$\Rightarrow 4=4$$

$$\begin{aligned}(x*y)*z &= (x+y+7)+z+7\\ &= x+y+z+14\\ &= x+(y+z+7)+7\\ &= x*(y*z)\end{aligned}$$

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

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

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

$\pi \notin \mathbb{Q}$

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

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

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

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

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

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

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

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

$(\mathbb{Z},+) \underset{\text{subgroup}}{\leq} (\mathbb{Q},+) \underset{\text{subgroup}}{\leq} (\mathbb{R},+) \leq (\mathbb{C},+)$; but $(\mathbb{R}^\times, \times)$ is not $\not\leq$ a subgroup $(\mathbb{R},+)$ (although $\mathbb{R}^\times \underset{\text{subset}}{\subseteq} \mathbb{R}$)

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

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

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

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

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

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

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

$GL_n(\mathbb{R})$ 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 $\begin{bmatrix} 2 & 0 \\ 1 & 5 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ -1 & 7 \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ -4 & 38 \end{bmatrix}$.

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

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

$$\begin{tikzcd} X \arrow[r, "h"] \arrow[rr, bend right, "g\circ h"'] & Y \arrow[r, "g"] \arrow[rr, bend right, "f\circ g"'] & Z \arrow[r, "f"] & W \end{tikzcd}$$

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

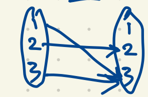
$f\circ g \neq g\circ f$

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

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

$$G = \mathrm{Sym}\,X = \{\text{bijections } X \to X\} = \{\text{permutations of } X\}.$$

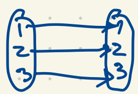
Not a bijection (neither one-to-one nor onto)



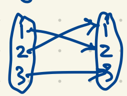
eg. $X = [3] = \{1,2,3\}$. (Notation: $[n] = \{1,2,3,\dots,n\}$.)

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

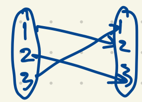
$n! = 1 \times 2 \times 3 \times \cdots \times n$ (n factorial) is the number of permutations of $[n]$.



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



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

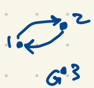


$|S_3| = 6$. S_3 is a nonabelian group of order 6.

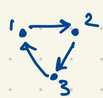
S_3 is the smallest nonabelian group.

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

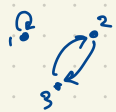
( )



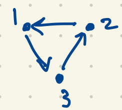
(12)



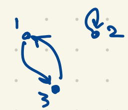
(123)



(23)



(132)



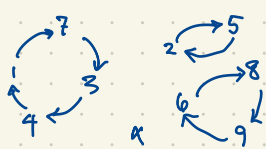
(13)

cycle notation for $\mathrm{Sym}[3] = S_3$

(12)(3)

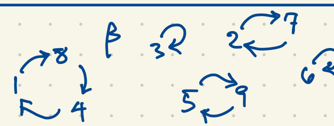
$= \{(\,),\ (12),\ (13),\ (23),\ (123),\ (132)\}$

Eg. $n = 9$



α

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	8
7	3	2	5
8	9	4	1
9	6	5	2



β

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

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

$(4,1,8) = (1,8,4) = (8,4,1)$

$(3) = (\,)$

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

$\alpha\beta = \alpha \circ \beta = (1,9,2,3,4,7,5,6,8) = (1734)(25)(689)(184)(27)(59)$

$\beta\alpha = \beta \circ \alpha = (129648573) = (184)(27)(59)(1734)(25)(689)$

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

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

$|S_n| = n!$

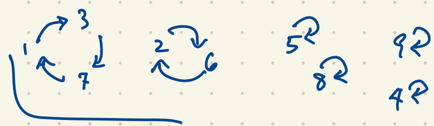
$|GL_n(\mathbb{R})| = \infty$

S_n is nonabelian for $n \geq 3$.

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

In S_n, disjoint cycles always commute, e.g. in S_9, $(137)(26) = (26)(137)$

If two permutations commute, must they have disjoint cycles?



$\alpha = (135)(246)$

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

Note: The two 3-cycles in α intersect with the three 2-cycles in β.

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

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

S_n acts on $[n] = \{1, 2, \ldots, n\}$ (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 <u>act</u> on things (generically called points).

Typically, groups describe <u>symmetries</u> 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.

number of edges

$12 \times 4 = 48$

number of symmetries fixing each edge

number of vertices

$8 \times 6 = 48$

number of symmetries fixing each vertex

how many symmetries map each face to each of the other faces

$6 \times 8 = 48$

number of faces

In a group G with identity e, an element $g \in G$ has <u>order</u> n if $g^n = e$ but no smaller power of g equals e.

$$g^n = \underbrace{g * g * \cdots * g}_{n \geq 1}$$

If G is the symmetry group of a cube, every reflection has order 2.

Also a 180° rotation about any axis has order 2.

A 120° rotation of the cube about an axis joining two opposite (antipodal) vertices has order 3.

The cube has axes of symmetry joining centers of opposite faces, and a 90° rotation around such an axis has order 4.

In any group, the identity has order 1.

S_3 has 1 element of order 1, i.e. $()$
3 elements of order 2, i.e. (12), (13), (23)
2 elements of order 3, i.e. (132), (123)

$|S_3| = 6$

The order of an n-cycle. If $\alpha = (1, 2, 3, \cdots, n)$ then $\alpha^n = ()$ but $\alpha^k \neq ()$ for $k = 1, 2, \cdots, n-1$.

S_4 has 1 elements of order 1, i.e. $()$
9 " " " 2, i.e. $(12), \ldots, (13)(24), \ldots$ (six $= \binom{4}{2}$ 2-cycles $(i\,j)$; three permutations $(i\,j)(k\,l)$ having the same cycle structure as $(13)(24)$)
8 " " " 3, i.e. $(123), \ldots$ (eight 3-cycles $(i\,j\,k)$, the same " " " (123))
6 " " " 4, six 4-cycles e.g. (1234)

$|S_4| = 24$