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.

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

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

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

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

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

So $-7\in\mathbb{R}$ is an identity element for '$*$'.

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

So $-x-14$ is an inverse element for x.

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

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

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

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

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

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

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

$\pi \notin \mathbb{Q}$

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

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

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

$(\mathbb{N}, +)$ 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</u> <u>linear</u> <u>group</u>

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

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

$GL_n(\mathbb{R})$ 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 $\mathbb{R}^*$ 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 $h(x) \in Y$, $g(h(x)) \in Z$, $\underbrace{f(g(h(x)))}_{(f\circ g\circ h)(x)} \in W$.

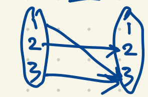
$f\circ g \neq g\circ f$

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 <u>symmetric group</u>

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

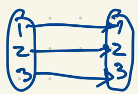
Not a bijection (neither one-to-one nor onto)



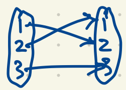
eg. $X = [3] = \{1,2,3\}$. (Notation: $[n] = \{1,2,3,\dots,n\}$.)

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

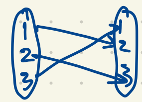
$n! = 1 \times 2 \times 3 \times \cdots \times n$ (n factorial) is the number of permutations of $[n]$.



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.

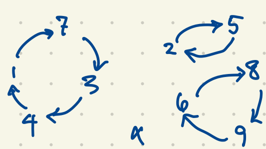
In S_3, $(12)(13) = (132)$
$(13)(12) = (123)$

( ) (12) (123) (23) (132) (13)

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

(12)(3)

Eg. $n = 9$

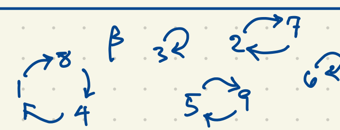


α

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

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

β



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

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

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

$(3) = (\,)$

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

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

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)

$|S_n| = n!$

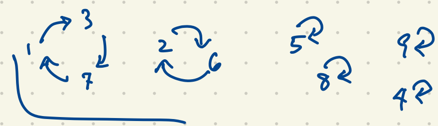
$|GL_n(\mathbb{R})| = \infty$

S_n is nonabelian for $n \geqslant 3$.

$S_2 = \{(\,), (12)\}$ 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 $[n] = \{1, 2, \dots, n\}$ (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 <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 $\underbrace{g^n}_{\underbrace{g*g*\cdots*g}_{n \geq 1}} = e$

but no smaller power of equals e.

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. $(12), \cdots, (13)(24), \cdots$ (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. $(123), \cdots$ (eight 3-cycles $(i\,j\,k)$, the same " " " (123))
6 ...... 4, six 4-cycles e.g. (1234)

$|S_4| = 24$

$$\binom{m}{n} = \binom{m}{m-n}$$

$\binom{m}{n}$ = number of n-subsets of an m-set, e.g. $\binom{4}{2} = 6$: a 4-set (set with 4 elements, e.g. $[4] = \{1,2,3,4\}$) has six subsets of size 2 : $\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}$

$$= \frac{m!}{n!\,(m-n)!} = \frac{m(m-1)(m-2)\cdots(m-n+1)}{n(n-1)(n-2)\cdots 1}$$

so $\binom{4}{2} = \frac{4\cdot 3}{2\cdot 1} = 6$. $\binom{4}{3}\cdot 2 = 4\cdot 2 = 8$ $\binom{4}{3} = \frac{4\cdot\cancel{3}\cdot\cancel{2}}{\cancel{3}\cdot\cancel{2}\cdot 1} = 4$

$S_5 = \{$ permutations of $[5] = \{1,2,3,4,5\}\}$ is a group of order $|S_5| = 5! = 120$.

$(1\ 2)(1 3) = (1 3\ 2)$

How many elements of each order does S_5 have?

$\underline{1}$ element of order 1 : $(\ )$

$\underline{25}$ elements of order 2 : $(i\ j)$ $\binom{5}{2} = 10$ cycles of length 2

$(i\ j)(k\ l)$ $5 \times 3 = 15$ elements which are a product of two disjoint 2-cycles

or: $\underbrace{10}_{\text{how many choices of 2-cycle } (i\ j)} \times \underbrace{3}_{\text{how many 2-cycles } (k\ l) \text{ disjoint from } (i\ j)} \div 2 = 15$

since $(i\ j)(k\ l) = (k\ l)(i\ j)$

A 2-cycle $(i\ j)$ (i.e. cycle of length 2) is a <u>transposition</u>.

$\underline{20}$ elements of order 3 : 3-cycles $(i\ j\ k)$ $\binom{5}{3} \times 2 = 10 \times 2 = 20$

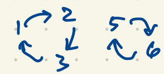
$\underline{30}$ elements of order 4 : 4-cycles $(i\ j\ k\ l)$ e.g. $(1\,2\,3\,4)$, $(1\,3\,4\,2)$, $(2\,5\,3\,4)$, ...

$\underline{24}$ elements of order 5 : 5-cycles $(1\underbrace{* * * *}_{2,3,4,5})$ $\binom{5}{4} \times 3! = 5 \times 6 = 30$

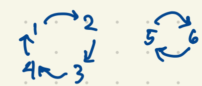
how many ways to choose i, j, k, l

$\underline{20}$ elements of order 6 : $(i\ j\ k)(l\ m)$

$(1\ 2\ 3)(4\ 5) \in S_5$ has order 6



$(1\ 2\ 3\ 4)(5\ 6) \in S_6$ has order 4



$120 = |S_5|$

If $\alpha \in S_n$ is written as a product of disjoint cycles, then its order is the least common multiple of the lengths of its cycles.

$(1\ 2\ 3)(4\ 5\ 6\ 7\ 8)$ has order 15

$(1\ 2\ 3)(4\ 5\ 6\ 7\ 8\ 9)$ $\cdots\cdots$ 6

In $\mathbb{R}^\times = \{$nonzero real numbers$\}$ under multiplication,

1 has order 1;

-1 " " 2; $(-1 \cdot -1 = 1)$

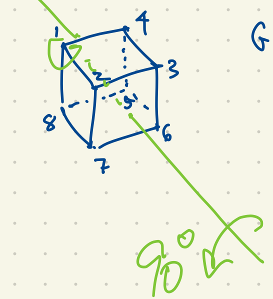
every other element of $\mathbb{R}^\times$ has infinite order.

If $a \in \mathbb{R}^*$, $\operatorname{ord}(a) = \begin{cases} 1, & \text{if } a = 1; \\ 2, & \text{if } a = -1; \\ \infty, & \text{otherwise.} \end{cases}$

We also write the order of $a \in G$ as $|a|$ e.g. $|(1\ 2\ 3)(4\ 5\ 6\ 7\ 8)| = 15$

$\operatorname{ord}((1\ 2\ 3)(4\ 5\ 6\ 7\ 8)) = 15$

The symmetry group of a cube is a group G of order 48 ie. $|G| = 48$.
It is useful to think of G as a subgroup of S_8 :



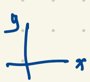
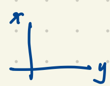
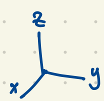
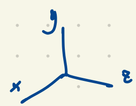
$$G = \{ (\,) , \underbrace{(1234)(5876)}_{\text{90° rotation about the vertical axis of symmetry}} , \underbrace{(1854)(2763)}_{\text{90° rotation about green axis of symmetry}} , \underbrace{(18)(27)(36)(45)}_{\text{reflection in horizontal plane of symmetry}} , (173)(486) , \ldots \}$$

$(\,)$ ↑ identity

$(1854)(2763)(1234)(5876) = (173)(2)(486)(5) = (173)(486)$ is a $120°$ rotation about the axis joining the pair of antipodal vertices 2,5

If G is any group and $g_1, \ldots, g_k \in G$ then $\langle g_1, g_2, \ldots, g_k \rangle$ = the subgroup of G generated by $g_1, \ldots, g_k$ ie. the smallest subgroup of G containing $g_1, \ldots, g_k$.

The letter S has a rotational symmetry about its centre (rotate 180° about S). The symmetry group in this case is $\{I, R\}$ where R is the 180° rotation, $R^2 = I$. Both symmetries of S preserve orientation. S ≠ S

 ≠ 
 ≠ 

U ≠ U

U has symmetry group of order 2 $\{I, T\}$ where T is a reflection in the vertical axis of symmetry, $T^2 = I$

Reflections reverse orientation; rotations preserve orientation.

Y has symmetry group of order 2

Y has symmetry group of order 1.

 has symmetry group of order 6. (3 rotational symmetries, 3 reflective symmetries).

For any object $X \subset \mathbb{R}^n$, either all symmetries of X preserve orientation or exactly half of the symmetries preserve orientation (so the other half reverse orientation).

reflection about vertical axis of symmetry

" " axis

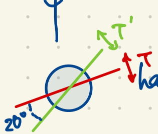
The symmetry group of Y is $\{\underbrace{I, R}, R^2, T, TR, TR^2\} = \langle T, R \rangle$ $RT = TR^2$ so the group is nonabelian.

(counter-clockwise 120° rotation about center)

E ≠ E

The figure EƎ has a symmetry group of order 4 $\{I, R, T, RT\}$ where I = identity, R = 180° rotation about the center, T = reflection in horizontal axis of symmetry, $RT = TR$ = reflection in the vertical axis of symmetry. This group is abelian.

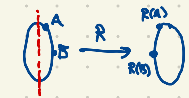
 has the same symmetry group as EƎ (abelian of order 4).



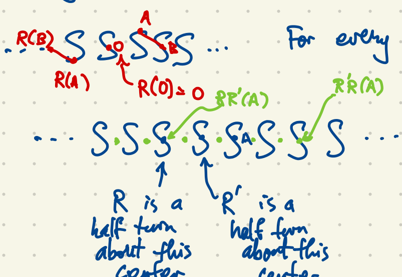
has infinitely many symmetries. The symmetry group is infinite nonabelian.

$$\underbrace{TT'}_{\substack{40^\circ\text{ rotation}\\ \text{clockwise}\\ \text{(i.e. }320^\circ\text{ counterclockwise}\\ \text{rotation about center)}}} \neq \underbrace{T'T}_{\substack{40^\circ\text{ rotation}\\ \text{counterclockwise}\\ \text{about center}}}$$

A symmetry of X is a bijection $X \to X$ (permutation of the points of X) which preserves distances and angles i.e. the shape of X. Here typically $X \subseteq \mathbb{R}^2$ or $X \subseteq \mathbb{R}^3$.
eg. if $X = \mathbb{R}^2$ then the symmetries (isometries) of $X = \mathbb{R}^2$ includes infinitely many transformations (rotations, reflections, translations, etc.).



If X is a circle then X has infinitely many symmetries.
If X is the pattern E then X has exactly 2 symmetries.
" " " " " " O then X " " 4 " .
The letter R has trivial symmetry group (only the identity).
" " S has symmetry group of order 2.
Note: The symmetry group of X is a subgroup of $\mathrm{Sym}\,X = \{\text{all permutations of } X\}$.
Eg. the pattern …SSSSS… in $\mathbb{R}^2$ is different from its mirror images so all its symmetries are orientation-preserving (in particular it has no reflective symmetries).
Some symmetries of the pattern:

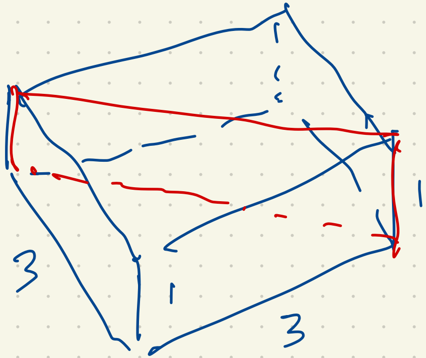


For every point at the center of some S, rotate 180° about that point.
Also we have translational symmetries found by translating an integer distance horizontally.
Also, half turns about any point midway between the centers of two adjacent S's.

$RR' \neq R'R$

$RR'(A) \neq R'R(A)$ so $RR' \neq R'A$ so the symmetry group is nonabelian.

In fact RR' is a translation two units to the left where a 'unit' is the distance between the centers of two adjacent S's. And $R'R$ is the translation two units to the right. $(R'R)^{-1} = RR'$

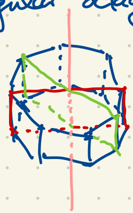


$1 \times 3 \times 3$ block

has 16 symmetries.

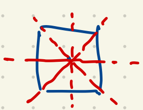
Compare: A square has only 8 symmetries.

A regular octagonal prism has symmetry group of order 32. This group is nonabelian.

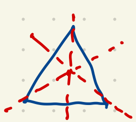


(16 rotational symmetries and 16 other symmetries which reverse orientation).

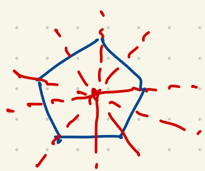
A regular n-gon ($n \geq 3$) has a symmetry group of order $2n$ (n rotational symmetries and n reflective symmetries).



$n=4$



$n=3$



$n=5$