

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

$$-7 * x = (-7) + x + 7 = x$$

$$\text{and } x * (-7) = x + (-7) + 7 = x$$

for all $x \in \mathbb{R}$.

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

$$(-x - 14) * x = (-x - 14) + x + 7 = -7$$

$$x * (-x - 14) = x + (-x - 14) + 7 = -7$$

for all $x \in \mathbb{R}$.

So $-x - 14$ 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 $n \geq 2$.

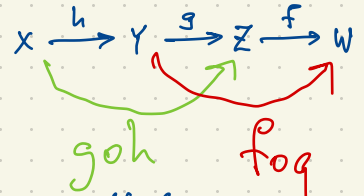
$GL_1(\mathbb{R})$ is commutative.

$(G, *)$ 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

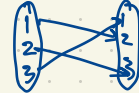
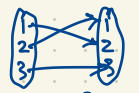
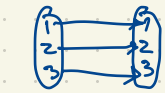
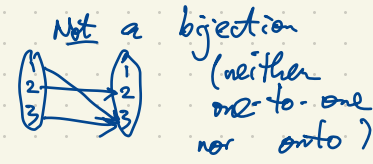
$$G = \text{Sym } X = \{ \text{bijections } X \rightarrow X \} = \{ \text{permutations of } X \}$$

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.

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 3 & 3 \end{pmatrix}$
(1)

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 3 & 3 \end{pmatrix}$
(12)

$\begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 1 \end{pmatrix}$
(123)

$\begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 1 \end{pmatrix}$
(23)

$\begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 1 \end{pmatrix}$
(132)

$\begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 3 \end{pmatrix}$
(13)

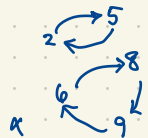
In S_3 ,

$$(12)(13) = (132)$$

$$(13)(12) = (123)$$

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



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

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

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

$$(3) = (1)$$

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

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

If α, β 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 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.** $|S_n| = n!$, $|[n]| = n$.

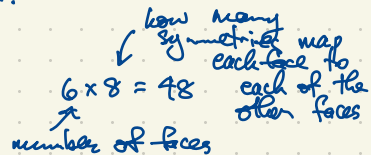
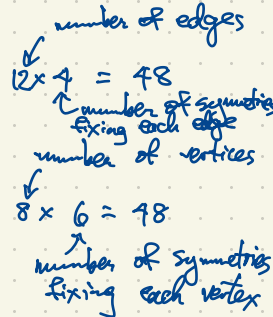
Typically, groups act on things (generically called points).

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.



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

$$\underbrace{g * g * \dots * g}_n = e$$

$n \geq 1$

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 $\alpha = (1, 2, 3, \dots, n)$ then $\alpha^n = ()$ but $\alpha^k \neq ()$ for $k = 1, 2, \dots, n-1$.

S_4 has $\frac{1}{9}$ elements of order 1, i.e. $()$
 $\frac{6}{8}$ elements of order 2, i.e. $(12), \dots, (13)(24), \dots$ (six 2-cycles (ij) ; three permutations $(ij)(kl)$ having the same cycle structure as $(13)(24)$)
 $\frac{8}{6}$ elements of order 3, i.e. $(123), \dots$ (eight 3-cycles (ijk) , the same \dots \dots \dots (123))
 $\frac{6}{6}$ elements of order 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: $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$

$$= \frac{m!}{n!(m-n)!} = \frac{m(m-1)(m-2)\dots(m-n+1)}{n(n-1)(n-2)\dots \cdot 1}$$

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

$S_5 = \{\text{permutations of } [5] = \{1, 2, 3, 4, 5\}\}$ 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?

1 element of order 1: (1)

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

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

or: $10 \times 3 \div 2 = 15$

how many choices of 2-cycle $(i\ j)$ \times how many 2-cycles $(k\ l)$ disjoint from $(i\ j)$

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

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

20 elements of order 3: 3-cycles $(i\ j\ k)$

$\binom{5}{3} \times 2 = 10 \times 2 = 20$

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

24 elements of order 5: 5-cycles $(1\ *\ *\ *\ *)$
 $2, 3, 4, 5$

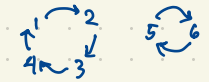
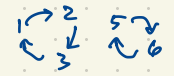
$\binom{5}{4} \times 3! = 5 \times 6 = 30$

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

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

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

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

1 has order 1;

-1 " " 2; $(-1)^2 = 1$

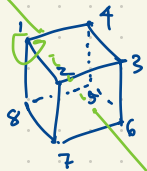
every other element of \mathbb{R}^* has infinite order.

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

we also write the order of $a \in G$ as $|a|$ e.g.

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

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



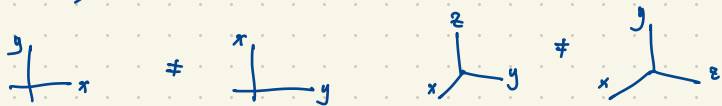
$90^\circ \curvearrowright$

$$G = \{ (1), \underbrace{(1234)(5876)}_{\substack{\uparrow \\ \text{identity}}}, \underbrace{(1854)(2763)}_{\substack{90^\circ \text{ rotation} \\ \text{about green} \\ \text{axis of symmetry}}}, \underbrace{(18)(27)(36)(45)}_{\substack{\text{reflection in} \\ \text{horizontal plane} \\ \text{of symmetry}}}, (173)(486), \dots \}$$

$$(1854)(2763)(1234)(5876) = (173)(2)(486)(5) = (173)(486) \text{ is a } 180^\circ \text{ rotation about the axis joining the pair of antipodal vertices } 2,5$$

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

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



$U \neq U$

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.

Y 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).

The symmetry group of Y is $\{I, R, R^2, T, TR, TR^2\} = \langle T, R \rangle$ where R is a counter-clockwise 120° rotation about center, T is reflection about vertical axis of symmetry. $RT = TR^2$ so the group is nonabelian.

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

 O has the same symmetry group as $E \equiv$ (abelian of order 4).

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

$TT' \neq T'T$
 $\underbrace{10^\circ \text{ rotation clockwise}}_{\text{(i.e., } 320^\circ \text{ counter-clockwise rotation about center)}} \quad \underbrace{40^\circ \text{ rotation counterclockwise}}_{\text{about center}}$

A symmetry of X is a bijection $X \rightarrow X$ (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.

... .. 0 then X 4



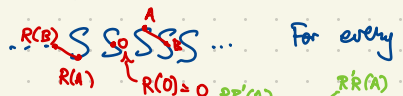
The letter R has trivial symmetry group (only the identity).

... .. S has symmetry group of order 2.

Note: The symmetry group of X is a subgroup of $\text{Sym } X = \{\text{all permutations of } X\}$.

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.

$$RR' \neq R'R$$

$$RR'(A)$$

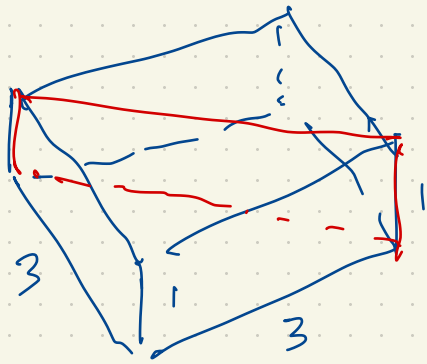
$$\neq$$

$$R'R(A)$$

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

R is a half turn about this center
 R' is a half turn about this center

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. $(R'R)^{-1} = RR'$

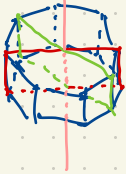


$1 \times 3 \times 3$ block

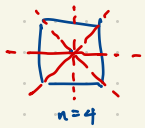
has 16 symmetries.

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).



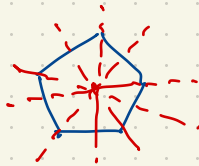
A regular n -gon ($n \geq 3$) has a symmetry group of order $2n$ (n rotational symmetries and n reflective symmetries).
Dihedral groups



$n=4$



$n=3$



$n=5$

In \mathbb{R}^* , the multiplicative group of nonzero real numbers,

$$\langle 3 \rangle = \left\{ \dots, \frac{1}{27}, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, 27, 81, 243, \dots \right\} = \{3^k : k \in \mathbb{Z}\}$$

$$\langle 2, 3 \rangle = \{2^k 3^l : k, l \in \mathbb{Z}\} \text{ so } \frac{2}{9} \in \langle 2, 3 \rangle, 5 \notin \langle 2, 3 \rangle, 25 \notin \langle 2, 3 \rangle \text{ (non-cyclic but it is abelian)}$$

$$\langle -1 \rangle = \{1, -1\}$$

$$\langle 1 \rangle = \{1\}$$

Theorem Let G be a group ^{with identity 1} and let $g \in G$. Then $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ has order $|\langle g \rangle| = |g|$.

(The order of each element is the order of the subgroup that it generates.)

A subgroup that is generated by a single element (i.e. a subgroup of the form $\langle g \rangle$ for some $g \in G$) is called cyclic. Cyclic groups (i.e. groups that are generated by a single element) are always abelian since in $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ we have $g^i g^j = g^{i+j} = g^{j+i} = g^j g^i$.

In the subgroup $\langle 3 \rangle < \mathbb{R}^*$ has two generators $3, \frac{1}{3}$ since $\langle 3 \rangle = \langle \frac{1}{3} \rangle$.

\mathbb{R}^* is not finitely generated: there is no finite list of elements $a_1, \dots, a_k \in \mathbb{R}^*$ such that

$\langle a_1, \dots, a_k \rangle = \mathbb{R}^*$. For every finite list $a_1, \dots, a_k \in \mathbb{R}^*$, the subgroup $\langle a_1, \dots, a_k \rangle < \mathbb{R}^*$ is a proper subgroup

(i.e. a subgroup which is a proper subset). $H \leq G$ means H is a subgroup of G ; $H < G$ means H is a proper subgroup of G .

Proof of the Theorem (about orders)

First suppose $g \in G$ has infinite order i.e. $g^k \neq 1$ for $k = 1, 2, 3, \dots$. We must show that $|\langle g \rangle| = \infty$ where $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$.

We will prove that all the powers g^k ($k \in \mathbb{Z}$) are distinct in this case. If not, then $g^k = g^l$ for some $k, l \in \mathbb{Z}$ with $k \neq l$, then without loss of generality $k < l$ and $1 = g^0 = g^{-k} g^k = g^{-k} g^l = g^{l-k}$, a contradiction.

So $|\langle g \rangle| = \infty$ in this case.

Next suppose $|g| = n$ is finite i.e. n is a positive integer and $g^k \neq 1$ for $k=1, 2, 3, \dots, n-1$ but $g^n = 1$.

We will show that $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ where these n elements are distinct. The same argument as above shows that $1, g, g^2, \dots, g^{n-1}$ are distinct (otherwise $g^k = g^l$ with $1 \leq k < l \leq n-1$ and then $g^{l-k} = 1$ where $l-k \in \{1, 2, \dots, n-1\}$, contrary to the assumption $|g| = n$). It remains to show that $g^k \in \{1, g, g^2, \dots, g^{n-1}\}$ for every $k \in \mathbb{Z}$. For this we use the Division Algorithm: $k = qn + r$ where $q, r \in \mathbb{Z}$, $r \in \{0, 1, 2, \dots, n-1\}$.

Then $g^k = g^{qn+r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r \in \{1, g, g^2, \dots, g^{n-1}\}$. \square