Subgroups

Notation: When it's obvious that the group operation is addition (for example when $G = \mathbb{Z}$) we may write $a + b$ instead of $a * b$. Otherwise, we'll write ab instead of $a * b$.

We will also write:

$$a^n = (a)(a)(a) \dots (a) \qquad n \text{ times}$$

$$a^{-1} = \text{inverse of } a$$

$$a^{-n} = (a^{-1})(a^{-1}) \dots (a^{-1}) \quad n \text{ times}$$

$$a^0 = e.$$

Notice that $a^m \cdot a^n = a^{m+n}; \quad m, n \in \mathbb{Z}$.

Ex. $a^{-2}a^4 = (a^{-1})(a^{-1})(a)(a)(a)(a)$

$$= (a^{-1})(a^{-1}a)(a)(a)(a)$$

$$= (a^{-1})(e)(a)(a)(a)$$

$$= (a^{-1}e)(a)(a)(a)$$

$$= (a^{-1})(a)(a)(a)$$

$$= (a^{-1}a)(a)(a)$$

$$= e(a)(a)$$

$$= a^2.$$

Def. If G is a group, then the **order** of G, written $|G|$, is the number of elements in G.

Def. If a subset H of a group G is closed under the binary operation of G and if H is a group with that binary operation, then H is a **subgroup** of G. We will write $H \leq G$ or $G \geq H$ in that case.

$H < G$ or $G > H$ will mean $H \leq G$ but $H \neq G$

Ex. $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$, in fact $(\mathbb{Z}, +) < (\mathbb{R}, +)$,

since $\mathbb{Z} \subsetneq \mathbb{R}$ and $\mathbb{Z}$ and $\mathbb{R}$ are both groups under $+$.

Ex. $(\mathbb{Q}^+, +)$ is not a subgroup of $(\mathbb{R}, +)$ even though $\mathbb{Q}^+ \subseteq \mathbb{R}$.

This is because $\mathbb{Q}^+$ is a group under $\cdot$ not $+$ (under $+$, $\mathbb{Q}^+$doesn't contain inverses for all of its elements).

Def. If G is a group, then the subgroup consisting of G itself is called the

improper subgroup of G. All the other subgroups are **proper subgroups**.

The subgroup $\{e\}$ is called the **trivial subgroup of G**. All other subgroups are

called **nontrivial**.

Ex. Let $G = \mathbb{R}^n$ with vector addition as the binary operation. This is a group under $+$. Let H be the set of vectors in $\mathbb{R}^n$ having 0 as the entry in the first component. Show H is a subgroup of G.

0) H is closed under $+$:

$$< 0, a_2, a_3, \dots, a_n > + < 0, b_2, b_3, \dots, b_n >$$
$$= < 0, a_2 + b_2, \dots, a_n + b_n > \in H.$$

1) $+$ is associative on H because vector addition is associative.

2) $< 0, 0, \ldots, 0 > = e \in H$.

3) If $a = < 0, a_1, a_2, \ldots, a_n > \in H$
Then $-a = < 0, -a_1, -a_2, \ldots, -a_n > \in H$
and $a + (-a) = e$.
$H \subsetneq G$ so H is a proper subgroup of G.

Ex. $(\mathbb{Q}^+, \ \cdot)$ is a proper subgroup of $(\mathbb{R}^+, \ \cdot)$. We saw earlier that both $(\mathbb{Q}^+, \ \cdot)$ and $(\mathbb{R}^+, \ \cdot)$ are groups under multiplication and $\mathbb{Q}^+ \subsetneq \mathbb{R}^+$.

Ex. The roots of the equation $x^4 = 1$ (called the 4th roots of unity) form an abelian subgroup of $\mathbb{C}^*$ under multiplication.

The roots of $x^4 = 1$ are $H = \{1, i, -1, -i\}$, where $i^2 = -1$.

Let's check that $(H, \ \cdot)$ is a group.

0) If $a, b \in H$ then clearly $ab \in H$.

1) Multiplication of complex numbers is associative and commutative.

2) 1 is the identity element.

3)

<u>element</u>	<u>inverse</u>	<u>product</u>
1	1	1·1 = 1
$\boldsymbol{i}$	- i	$i \cdot (-i) = -i^2 = 1$
-1	-1	(-1)·(-1) = 1
- $\boldsymbol{i}$	i	$(-i)(i) = -i^2 = 1$

It's actually the case that the n^{th} roots of unity, $n \in \mathbb{Z}^+$, form an abelian subgroup of order n of $(\mathbb{C}^*, \ \cdot)$. This group is sometimes called $\boldsymbol{U_n}$.

Ex. Another (abelian) group, V, of order 4 is called the Klein 4-Group

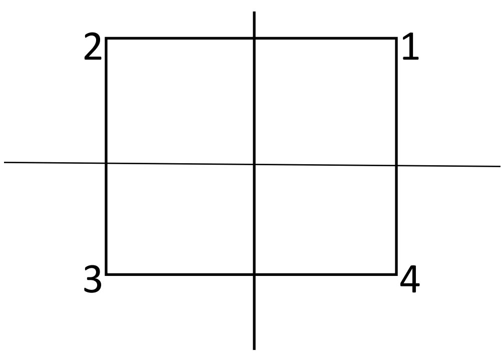
$V = \{e, a, b, c\}$, and the multiplication is given by:

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

V is a group.

0) The table shows that V is closed under multiplication.
1) One can check that the multiplication is associative by checking all the possible elements in $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2) e is the identity element shown by the table.
3) By the table we can see $a^{-1} = a,\ b^{-1} = b$ and $c^{-1} = c$.

V can be thought of as reflections of the vertices of a square along the x-axis, y-axis, and the origin.



a = reflection over x-axis

b = reflection over y-axis

c = reflection about the origin.

a: $1 \leftrightarrow 4$ and $2 \leftrightarrow 3$

b: $1 \leftrightarrow 2$ and $3 \leftrightarrow 4$

c: $1 \leftrightarrow 3$ and $2 \leftrightarrow 4$.

Multiplication is just the composition of these functions:

a: $1 \leftrightarrow 4$ $\quad$ b: $1 \leftrightarrow 2$

$2 \leftrightarrow 3$ $\quad$ $2 \leftrightarrow 1$

$3 \leftrightarrow 2$ $\quad$ $3 \leftrightarrow 4$

$4 \leftrightarrow 1$ $\quad$ $4 \leftrightarrow 3$

$b \cdot a$: $1 \rightarrow 4 \rightarrow 3$ which is $1 \rightarrow 3$ the same as c.

$2 \rightarrow 3 \rightarrow 4$ $\quad$ $2 \rightarrow 4$

$3 \rightarrow 2 \rightarrow 1$ $\quad$ $3 \rightarrow 1$

$4 \rightarrow 1 \rightarrow 2$ $\quad$ $4 \rightarrow 2$

Ex. Let's put the tables of $(\mathbb{Z}_4, +)$ and $(V, \ \cdot)$ next to each other:

$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

V

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

What subgroups of $(\mathbb{Z}_4, +)$ exist other than $\mathbb{Z}_4$ and $\{0\}$?

Notice that $H = \{0,2\}$ is a subgroup of $\mathbb{Z}_4$

0) $0 + 0 = 0, \ \ 0 + 2 = 2, \ \ 2 + 0 = 2, \ \ 2 + 2 = 4$ mod $2 = 0$.
   So, H is closed under $+$.
1) $+$ is associative.
2) 0 is the identity element .
3) 2 is its own inverse so if $a \in H$, then $a^{-1} \in H$.

Notice that:

$\{0,1\}, \{0,3\}, \{1,2\},\{1,3\}, \{2,3\}, \{0, 1, 2\}, \{0, 2, 3\}, \{1, 2, 3\}$

are not subgroups of $\mathbb{Z}_4$ because in each case the sets are not closed under addition.

For example:

$\{0,3\}$, $3 + 3 = 6$ mod 4 $= 2 \notin \{0,3\}$

$\{1,2\}$ $1 + 2 = 3 \notin \{1, 2\}$ etc.

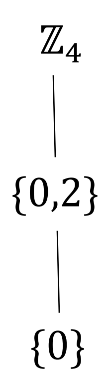
What subgroups of V exist other than V and $\{e\}$?

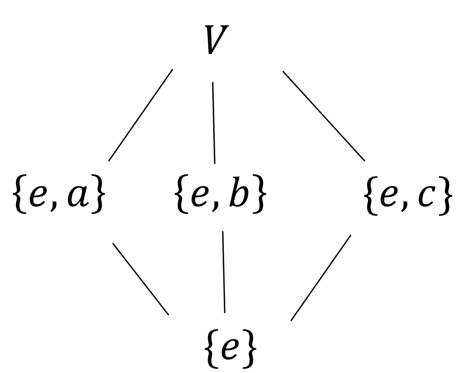
$H_1 = \{e, a\}$, $H_2 = \{e, b\}$, $H_3 = \{e, c\}$ are also subgroups.

The multiplication table for V shows that for each set H_i, $i = 1, 2, 3$

0) H_i is closed under $\cdot$.
1) $\cdot$ is associative.
2) e is the identity element.
3) H_i contains all of its inverses.

We can diagram $\mathbb{Z}_4$ and its subgroups and V and its subgroups by:





Theorem: A nonempty subset H of a group G is a subgroup of G if and only if

1. H is closed under the binary operation of G.
2. For all $a \in H, a^{-1} \in H$.

Proof: If $H \leq G$ then $1, 2$ hold by the definition of a group.

If $1, 2$ hold we just need to know that the multiplication is associative in H and that $e \in H$.

For any $a, b, c \in H, a, b, c$ are also in G so, $(ab)c = a(bc)$.

Since H is nonempty, closed under multiplication, and for all $a \in H, a^{-1} \in H$, then $aa^{-1} = e \in H$.

Hence $H \leq G$.

Ex. Let F be the group of real valued functions whose domain is $\mathbb{R}$ under addition. The subset H consisting of differentiable (or continuous) functions is a subgroup of F.

1. The sum of differentiable functions is differentiable.
2. $-f(x)$, the inverse of $f(x)$, is differentiable.

Ex. Let $G = GL(n, \mathbb{R})$ of invertible $n \times n$ matrices (which means

if $A \in GL(n, \mathbb{R})$, $\det(A) \neq 0$) with matrix multiplication.

Let $H =$ subset of G where $A \in H$ if $\det(A) = 1$. Show $H \leq G$.

1. $A, B \in H$ then $\det(AB) = (\det A)(\det B) = (1)(1) = 1$

   so H is closed under matrix multiplication.

2. If $A \in H$ then $\det(A^{-1}) = \frac{1}{\det A} = \frac{1}{1} = 1$. So $A^{-1} \in H$.

Ex. Let $G = \mathbb{Z}, +$. Let $H = 5\mathbb{Z} = \{x = 5n |\, n \in \mathbb{Z}\}$.

Show that H is a subgroup of $G = \mathbb{Z}$.

1. $a, b \in H \Rightarrow a = 5n, \;\; b = 5m, \;\; n, m \in \mathbb{Z}$.
   $a + b = 5n + 5m = 5(n + m), \; n + m \in \mathbb{Z}$
   So H is closed under $+$.

2. $a \in H \Rightarrow a = 5n, n \in \mathbb{Z}$. $-a = 5(-n), -n \in \mathbb{Z}$ so $-a \in H$.
   Thus H contains all of its inverses.

Cyclic Subgroups

What's the smallest subgroup H of $\mathbb{Z}_{12}, +$ that contains 3?

For H to be a subgroup of $\mathbb{Z}_{12}$ it needs to contain 0, the identity element of $\mathbb{Z}_{12}$. It also needs to be closed under addition so,

$3 + 3 = 6 \in H$

$3 + 6 = 9 \in H$

and $9 + 3 = 0 \in H$.

Notice the inverse of 6 is 6 (i.e. $6 + 6 = 0$ mod 12)

and the inverse of 9 is 3 (i.e. $9 + 3 = 0$ mod 12),

So $\{0, 3, 6, 9\}$ is the smallest subgroup of $\mathbb{Z}_{12}$ that contains 3.

In general, if a subgroup $H \leq G$ contains an element a then it must contain $\{a^n, n \in \mathbb{Z}\}$.

Theorem: Let G be a group and let $a \in G$. Then $H = \{a^n |\ n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G that contains a.

Proof:

1. Since $a^r \cdot a^s = a^{r+s}$ for $r, s \in \mathbb{Z}$, H is closed under multiplication.

2. If $a^r \in H$ then $a^{-r} \in H$ and $a^r \cdot a^{-r} = e$. So H contains inverses.

   Hence H is a subgroup of G.

Notice that any subgroup of G that contains a must also contain all powers of a and thus must contain H. Thus H is the smallest subgroup of G containing a.

Def. Let G be a group and $a \in G$. Then the subgroup $H = \{a^n |\ n \in \mathbb{Z}\}$ of G is called the **cyclic subgroup of G generated by a**, and denoted by $< a >$.

Def. An element a of a group G **generates** G and is a **generator for G** if $< a > = G$. A group G is **cyclic** if there is some a in G that generates G.

Ex. $\mathbb{Z}$ is a cyclic group under $+$ and 1 and -1 are both generators of $\mathbb{Z}$.

Ex. $\mathbb{Z}_4, +$ is cyclic and both 1 and 3 are generators, i.e. $< 1 > = < 3 >= \mathbb{Z}_4$.

If $a = 1$ then

$a^1 = 1$

$a^2 = 1 + 1 = 2$

$a^3 = 1 + 1 + 1 = 3$

$a^4 = 1 + 1 + 1 + 1 = 4(mod\ 4) = 0$

If $a = 3$ then

$a^1 = 3$

$a^2 = (3 + 3)\ (mod\ 4) = 2$

$a^3 = (3 + 3 + 3)(mod\ 4) = 1$

$a^4 = (3 + 3 + 3 + 3)(mod\ 4) = 0.$

Ex. $V =$ Klein 4-group is not cyclic because

$a^2 = e,\ b^2 = e,\ c^2 = e$ so $< a >, < b >, < c >$ generate subgroups of V of order 2 and $|V| = 4$.

Ex. $\mathbb{Z}_n$ is a cyclic group and 1 and $n - 1$ are generators. There could be other generators depending on what n is. For example, if $n = 8$, then $1, 3, 5,$ and 7 are generators (any number relatively prime to n, i.e. a number with no common factors with n will be a generator).

Ex. If $a = 3$, find $< a >$ in $\mathbb{Z}, +$.

$a^1 = 3$	$a^0 = 0$
$a^2 = 3 + 3 = 6$	$a^{-1} = -3$
$a^3 = 3 + 3 + 3 = 9$	$a^{-2} = -3 + (-3) = -6$
$\vdots$	$\vdots$
$a^n = 3 + 3 + \cdots + 3 = 3n$	$a^{-n} = -3 + (-3) + \cdots + (-3) = -3n.$

So $< a > = < 3 > = 3\mathbb{Z} = \{n \mid n = 3m,\ m \in \mathbb{Z}\}$.

Ex. Find all elements in the cyclic subgroup H of $GL(2,\mathbb{R})$ (with matrix multiplication) generated by $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

$\vdots$

$$A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

If $A \in GL(2,\mathbb{R})$, $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

Then $A^{-1} = \frac{1}{detA}\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}$ so,

$$A^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

$$A^{-2} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$$

$\vdots$

$$A^{-n} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$$

and $A^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

So $H = \{A \in GL(2,\mathbb{R}) \mid A = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}, n \in \mathbb{Z}\}$.