Prop: Let G be a group, $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof:

$e = a\,b\,b^{-1}\,a^{-1} = b^{-1}\,a^{-1}\,a\,b = e$

$(ab)\cdot(b^{-1}a^{-1}) = e$

$(b^{-1}a^{-1})\,ab = e$

$\therefore$ by definition $(ab)^{-1} = b^{-1}a^{-1}$. ∎

Prop Let G be a group. For any $a \in G$ $(a^{-1})^{-1} = a$

Proof:

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

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

$(a^{-1})^{-1} = a$. ∎

Prop Let G be a group, $a, b \in G$. Then

$ax = b$ and $xa = b$ have unique solutions in G.

Proof: Show x exists

$a^{-1}\,ax = a^{-1}\,b$

$\therefore\ x = a^{-1}\,b$ $\therefore$ x exists

Show x is unique. Suppose $ax_1 = a\,x_2 = b$

$$a^{-1}a x_1 = a^{-1}a x_2 = a^{-1} b$$

$$x_1 = x_2 = a^{-1} b. \quad \blacksquare$$

Prop) If G is a group, $a, b, c \in G$ then

$ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$.

Exponents in Groups

$g \in G$ ← a group, e = identity in G

Define $g^0 = e$

$g^n = \underbrace{g \cdots g}_{n \text{ times}}$

$g^{-n} = \underbrace{g^{-1} \cdots g^{-1}}_{n \text{ times}}$

Th. For all $g, h \in G$ ← a group.

- $g^m g^n = g^{m+n}$ $\quad \forall m, n \in \mathbb{Z}$
- $(g^m)^n = g^{mn}$
- $(gh)^n = (h^{-1} g^{-1})^{-n}$

$$\| \quad (gh)^{-1})^{-n} = (gh)^n$$

Furth if G is abelian then $(gh)^n = g^n h^n$

BUT this is <u>not</u> true in general.

Subgroups ← smaller group inside another group

[Ex] $2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\}$ ← even integers, with addition

is a subgroup of $(\mathbb{Z}, +)$

A **subgroup** of a group G is a subset H of G s.t H is also a group under the same operation as G.

Ex)
- $H = \{e\}$ the identity e always forms a subgroup (sometimes called the trivial subgroup).
- G is always a subgroup of G

Def) H is a **proper** subgroup of G iff H is a proper subset and is a subgroup.

$H \subseteq G$ is a subgroup (sometimes written as $H < G$)

Ex] $\mathbb{C}^*$ = group of non-zero complex numbers with multiplication.

$H = \{1, -1, i, -i\}$

Ex] $SL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \det(A) = 1,\ a,b,c,d \in \mathbb{R} \right\}$

Recall $GL_2(\mathbb{R})$ = invertible 2×2 real matrices under mult.

- Closed: since $\det(A)\cdot\det(B) = \det(AB)$
- Has inverses: $\det(A^{-1}) = \frac{1}{\det(A)}$

$\therefore$ $A \in SL_2(\mathbb{R}) \Rightarrow A^{-1} \in SL_2(\mathbb{R})$.

- identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is in $SL_2(\mathbb{R})$

Ex]

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\} \text{ under addition.}$$

$$GL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R},\ \det(A) \neq 0 \right\}$$

is <u>Not</u> a subgroup under addition.

Since $GL_2(\mathbb{R})$ is <u>Not</u> closed under addition

(also no identity $= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$)

<u>Prop</u> A subset H is a subgroup iff the following hold:

1) The identity e of G is in H (and is the identity of H)

2) If $h_1, h_2 \in H$ then $h_1 h_2 \in H$

3) If $h \in H$, then $h^{-1} \in H$

<u>Proof:</u>

1) H is a group $\therefore$ has an identity $e_H \in H$

Show $e_H = e$ where e is the identity of G.

$e\, e_H = e_H\, e = e_H$ since e is the identity in G

and $e_H\, e_H = e_H$ since e_H is the identity in H

$e\, e_H = e_H\, e_H$ (working in G)

$\Rightarrow \quad e = e_H$ ∎

One step Subgroup test.

Prop Let H be a subset of a group G.

Then H is a subgroup of G iff $H \neq \emptyset$ and whenever $g, h \in H \Rightarrow gh^{-1} \in H$.

Proof:

$\Rightarrow$ First Assume H is a subgroup of G, $g, h \in H$.

$\Rightarrow \quad h^{-1} \in H$ and $gh^{-1} \in H$ (closure and inverses in H).

$\Leftarrow$ Now suppose $H \subset G$, $H \neq \emptyset$, and $gh^{-1} \in H$ whenever $g, h \in H$.

Consider $h = g$

$\Rightarrow \quad g g^{-1} \in H \Rightarrow e \in H$ (identity of G = identity of H)

Now let $a \in H$ be arbitrary, set $g = e$, $h = a$

$\Rightarrow \quad gh^{-1} \in H \Rightarrow \quad e \cdot a^{-1} = a^{-1} \in H.$

$\therefore$ identity and inverses are in H

Need to show closure

Suppose $h_1, h_2 \in H$, show $h_1 \cdot h_2 \in H$. we Know $h_2^{-1} \in H$

$\therefore \quad h_1, h_2^{-1} \in H$ take $g = h_1$, $h = h_2^{-1}$

$gh^{-1} \in H \Rightarrow \quad h_1 (h_2^{-1})^{-1} \in H$

$\Rightarrow h_1 h_2 \in H.$

$\therefore$ H is closed $\therefore$ H is a subgroup. ∎

Cyclic Subgroups ← subgroup generated by all powers of 1 element.

Ex] $3\mathbb{Z} = \{ \ldots, -3, 0, 3, 6, \ldots \}$ with addition

⇓ powers = repeated addition

Ex] $H = \{ 2^n \mid n \in \mathbb{Z} \}$ is a subgroup of

$\mathbb{Q}^*$ = non-zero rationals with multiplication

if $a = 2^n$, $b = 2^n \in H$

$$ab^{-1} = 2^m 2^{-n} = 2^{m-n} \in H$$

$\therefore$ H is a subgroup by 1 step Step subgroup test.

Thm. Let G be a group, $a \in G$. set

$$\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$$

cyclic subgroup generated by a.

is a subgroup of G. Furthermore $\langle a \rangle$ is the smallest subgroup of G which contains a.

Proof:

- $e \in \langle a \rangle$ since $a^0 = e \in \langle a \rangle$
- If $g, h \in \langle a \rangle \Rightarrow g = a^m$, $h = a^n$ / for some $m, n \in \mathbb{Z}$.

$$\Rightarrow g \cdot h = a^m \cdot a^n = a^{m+n} \in \langle a \rangle$$

- $g = a^n \in \langle a \rangle \Rightarrow g^{-1} = a^{-n} \in \langle a \rangle$ $\therefore \langle a \rangle$ is a subgroup

Any subgroup H of G containing a must contain all powers of a (by closure) $\therefore$ H contains $\langle a \rangle$

$\therefore$ $\langle a \rangle$ is the smallest subgroup of G containing a. ∎

Def) If $a \in G$ the order of a is the smallest positive $n \in \mathbb{N}$ s.t. $a^n = e$ $(n \neq 0)$

write this as $|a| = n$.

If there exists no such integer $\Rightarrow$ $|a| = \infty$.