Basic Properties of Groups

Groups can be finite or infinite

Let $G$ be a group write $|G| = n$ of elements in $G$

$|\mathbb{Z}_5| = 5$, $|\mathbb{Z}| = \infty$

Proposition 3.17. The identity element in a group $G$ is unique; that is, there exists only one element $e \in G$ such that $eg = ge = g$ for all $g \in G$.

Inverses are also unique

If $g'$, $g''$ are inverses of $g$

$$g' \cdot g = e \quad \text{and} \quad g \cdot g'' = g'' \cdot g = e$$

$$g' = g' \cdot e = g' \cdot (g \cdot g'') = (g' \cdot g) \cdot g'' = e \cdot g'' = g''$$

$\therefore \quad g' = g''$

Proposition 3.18. If $g$ is any element in a group $G$, then the inverse of $g$, denoted by $g^{-1}$, is unique.

Proposition 3.19. Let $G$ be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof:

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

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

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

$\therefore \quad \text{by definition} \quad (ab)^{-1} = b^{-1}a^{-1}$$
Prop 1. Let $G$ be a group. For any $a \in G$, $(a^{-1})^{-1} = a$.

Proof: $a^{-1} \cdot (a^{-1})^{-1} = e$

$= a^{-1} \cdot e = a$

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

Proposition 3.21. Let $G$ be a group and $a$ and $b$ be any two elements in $G$. Then the equations $ax = b$ and $xa = b$ have unique solutions in $G$.

Right and left cancellation laws hold in groups:

Proposition 3.22. If $G$ is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

Exponents in Groups

Define: $g^0 = e$, $g^n = g \cdot \ldots \cdot g$ $n$ times, $g^{-n} = g^{-1} \cdot \ldots \cdot g^{-1}$.

Theorem 3.23. In a group, the usual laws of exponents hold; that is, for all $g, h \in G$,

1. $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$;
2. $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$;
3. $(gh)^n = (h^{-1} g^{-1})^{-n}$ for all $n \in \mathbb{Z}$. Furthermore, if $G$ is abelian, then $(gh)^n = g^n h^n$.

If $G$ is not abelian.
Subgroups

A smaller group inside another group

Example

Even integers

\[ \mathbb{Z} = \{ \ldots, -2, 0, 2, 4, \ldots \} \text{ is a group under addition, and is a subgroup of } (\mathbb{Z}, +) \]

Formally, a subgroup of a group \( G \) is a subset \( H \) of \( G \) such that \( H \) is also a group under the operation of \( G \):

1. \( H = \{ e \} \) is a subgroup of every group, called the trivial subgroup.
2. \( G \), \( \{ e \} \) are always subgroups of \( G \).
3. \( H \), proper subgroup \( \implies \) \( H \) is a proper subset and a subgroup.

Example

\( \mathbb{C}^* = \) group of non-zero complex numbers under mutl.

\( H = \{ 1, -1, i, -i \} \) is a subgroup under mutl.

Example

\( \text{SL}_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \det(A) = 1 \right\} \) is a subgroup of \( \text{GL}_2(\mathbb{R}) \), the invertible \( 2 \times 2 \) real matrices under matrix mutl.

- Closed since \( \det(A) \cdot \det(B) = \det(AB) \)
- Has inverses since \( \det(A^{-1}) = \frac{1}{\det(A)} \implies A^{-1} \in \text{SL}_2(\mathbb{R}) \) if \( A \in \text{SL}_2(\mathbb{R}) \)
- \( I \in \text{SL}_2(\mathbb{R}) \)
Ex

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

\( \text{GL}_2(\mathbb{R}) \) is a subset, but not a subgroup under addition.

Since it is not closed i.e. \( a \circ 0 \)

\[ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -a & 0 \\ 0 & -c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin \text{GL}_2(\mathbb{R}) \]

Proposition 3.30. A subset \( H \) of \( G \) is a subgroup if and only if it satisfies the following conditions:

1. The identity \( e \) of \( G \) is in \( H \).
2. If \( h_1, h_2 \in H \), then \( h_1h_2 \in H \).
3. If \( h \in H \), then \( h^{-1} \in H \).

Proof:

First suppose \( H \) is a subgroup of \( G \), show 1, 2, 3 hold.

\( H \) is a group \( \Rightarrow \) has an identity \( e_H \in H \), show \( e_H = e \).

\( e_H e_H = e_H \) and \( e e_H = e_H e = e_H \)

\( e e_H = e_H e_H \)

\( e = e_H \Rightarrow 1 \) holds

Since \( H \) is a group, we know (since \( H \) is a group)

\( \exists h' \in H \) s.t. \( hh' = h' h = e \)

Since inverses in \( G \) are unique then \( h' = h^{-1} \)

Conversely, if 1, 2, 3 hold then \( H \) is a group by def using the associative binary op. of \( G \).
Prop 3.3.1

Let $H$ be a subset of a group $G$. Then $H$ is a subgroup of $G$ if and only if $H \neq \emptyset$ and whenever $g, h \in H \Rightarrow gh^{-1} \in H$.

Proof:
First assume $H$ is a subgroup, and $g, h \in H$

$\Rightarrow h^{-1} \in H$ and $gh^{-1} \in H$

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

Consider $h=g$

$gg^{-1} \in H \Rightarrow e \in H$

Now $a \in H$ be arbitrary set $g=a$, then

$e \cdot a^{-1} = a^{-1} \in H$

$\therefore$ identity and inverses are in $H$

Need to show closure:
Suppose $h_1, h_2 \in H$ show $h_1h_2 \in H$, we know $h_2^{-1} \in H$

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

$h_1h_2 \in H$

$\therefore$ $H$ is closed, thus $H$ is a subgroup of $G$.

\[ \square \]

\textit{Remark}