Basic Properties of Groups

Groups can be finite or infinite

Let G be a group write $|G|$ = # of elements in G (order of 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

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

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

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

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:

$$abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e = \underbrace{b^{-1}a^{-1}}ab$$

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

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

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

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

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

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

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

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: $n \in \mathbb{N}$

$$g^0 = e$$

$$g^n = \overbrace{g \cdot g \cdots g}^{n \text{ times}}$$

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

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* $(gh)^n = g^n h^n$.

$$\overset{\shortparallel}{((gh)^{-1})^{-n}}$$

$(gh)^n \neq g^n h^n$ if G is not abelian.

Subgroups

$\uparrow$ smaller Group inside another group

Ex] $\swarrow$ Even integers

$2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\}$ is a group under addition.

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

Formally a <u>Subgroup</u> of a group G is a subset H of G

s.t. H is also a Group under the operation of G

- $H = \{e\}$ is a subgroup of every group, called the <u>trivial subgroup</u>
- $G, \{e\}$ are always subgroups of G
- H Proper subgroup $\Leftrightarrow$ H is a proper subset and a subgroup.

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

$H = \{1, -1, i, -i\}$ is a subgroup under mult.

Ex]

$$SL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \underset{\substack{\| \\ ad-bc}}{\det(A)} = 1 \right\}$$ is a subgroup of

$GL_2(\mathbb{R})$ $\leftarrow$ invertible 2×2 Real matrices under matrix mult.

- closed since $\det(A) \cdot \det(B) = \det(AB)$
- Has inverses since $\det(A^{-1}) = \dfrac{1}{\det(A)}$ $\Rightarrow$ $A^{-1} \in SL_2(\mathbb{R})$ if $A \in SL_2(\mathbb{R})$
- $I \in SL_2(\mathbb{R})$

Ex) group of 2x2 matrices

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

$GL_2(\mathbb{R})$ is a subset, but Not a subgroup under addition

Since it is not closed i.e. $a \neq 0$

$$\underbrace{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}}_{\in GL_2(\mathbb{R})} + \underbrace{\begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix}}_{\in} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin GL_2(\mathbb{R})$$

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 $h_1 h_2 \in H$.*
3. *If $h \in H$, then $h^{-1} \in H$.*

Proof:

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

identity in G

H is a group $\therefore$ has an identity $e_H \in H$, show $e_H = e$

$e_H e_H = e_H$ and $e e_H = e_H e = e_H$

$e e_H = e_H e_H$

$e = e_H \quad \therefore$ 1 holds

H is a group $\therefore$ 2 holds

we know (since H is a group)

$\exists\, h' \in H$ s.t. $h h' = h' h = e$

Since inverses in G are unique then $h' = h^{-1}$

Conversly if 1,2,3 hold then H is group by def using the associative binary op. of G.

Prop 3.31

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

Proof:

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

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

Now suppose $H \subset G$, $H \neq \phi$ 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 arbitray set $g = e, h = a$, 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 $h_1 \cdot h_2 \in H$, we know $h_2^{-1} \in H$

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

$$h_1 h_2 \in H$$

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

Mond