Group Theory

Daniel Mao

Contents

1

Group Basics

1.1 Definitions

Definition (Binary Operation) Let G be a set. We define a ***binary operation*** on G to be the function $*$ from $G \times G$ to G.

Definition (Group)**.** *Let G be a set. Let $*$ be a binary operation. We say that the ordered pair $(G, *)$ is a **group** if it satisfies all of the conditions listed below.*

(1) (Closure) For any two elements a and b in G, $a * b \in G$.

(2) (Associativity) For any elements a, b, and c in G, $a * (b * c) = (a * b) * c$.

(3) (Identity) There exists an element id in G such that for any element a in G, $a * id = id * a = a$.

(4) (Invertibility) For any element a in G, there exists an element a^{-1} also in G such that $a * a^{-1} = id$.

Definition (Commutative Group)**.** *We say a group is **commutative** if the binary operation on the group is also commutative.*

Definition (Finite Group)**.** *We say a group is **finite** if the set is a finite set.*

1.2 Properties

Proposition 1.2.1 (Uniqueness of identity)**.** *Let $(G, *)$ be a group. Then the identity element id of $(G, *)$ is unique.*

Proposition 1.2.2 (Uniqueness of Inverse)**.** *Let $(G, *)$ be a group. Then for any element a in G, a^{-1} is unique.*

Proposition 1.2.3 (Arithmetic Properties). *(1) Let $(G, *)$ be a group. For any element a in G,*

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

(2) Let $(G, *)$ be a group. For any elements a and b in G,

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

1.3 Sufficient Conditions

Proposition 1.3.1. *The intersection of a collection of subgroups is also a subgroup.*

Proof.
Let $(G, *)$ be a group.
Let $\mathcal{H}$ be a collection of subgroups of G.
Say $\mathcal{H} = \{H_\lambda\}_{\lambda \in \Lambda}$ where Λ is an index set and H_λ is a subgroup of $(G, *)$ for any $\lambda \in \Lambda$.
Let H denote the intersection of all subgroups in $\mathcal{H}$.
Let H_λ be an arbitrary subgroup in $\mathcal{H}$.
Since H_λ is a group, $id \in H_\lambda$.
Since $id \in H_\lambda$ for any $\lambda \in \Lambda$, $id \in H$.
Let h_1 and h_2 be arbitrary elements in H.
Since $h_1, h_2 \in H$ and $H \subseteq H_\lambda$, $h_1, h_2 \in H_\lambda$.
Since $h_1, h_2 \in H_\lambda$ and H_λ is a group, $h_1 h_2 \in H_\lambda$.
Since $h_1 h_2 \in H_\lambda$ for any $\lambda \in \Lambda$, $h_1 h_2 \in H$.
Since $h_1 h_2 \in H$ for any elements h_1 and h_2 in H, H is closed under product.
Let h be an arbitrary element in H.
Since $h \in H$ and $H \subseteq H_\lambda$, $h \in H_\lambda$.
Since $h \in H_\lambda$ and H_λ is a group, $h^{-1} \in H_\lambda$.
Since $h^{-1} \in H_\lambda$ for any $\lambda \in \Lambda$, $h^{-1} \in H$.
Since $h^{-1} \in H$ for any element h in H, H is closed under inverse.
Since $id \in H$ and H is closed under product and inverse, H is a subgroup.

■

Proposition 1.3.2. *Let $(G, *)$ be a group. Let S and T be subgroups of G. Then the product ST is a group if and only if the two subgroups permute. i.e., if $ST = TS$.*

Proof.
[ST ***is a group*** $\implies$ $ST = TS$]
For one direction, assume that ST is a group.
We are to prove that $ST = TS$.
Let x be an arbitrary element in ST.

Since ST is a group, by definition of group, any element in ST has an inverse in ST.
Since $x \in ST$ and any element in ST has an inverse in ST, in particular, x has an inverse ST. i.e., x^{-1} exists and $x^{-1} \in ST$.
Since $x \in ST$, $x = st$ for some $s \in S$ and $t \in T$.
Since $x^{-1} \in ST$, $x^{-1} = s't'$ for some $s' \in S$ and $t' \in T$.
Since $x^{-1} = s't'$, $x = (x^{-1})^{-1} = (s't')^{-1} = t'^{-1}s'^{-1}$.
Since T is a group, by definition, any element in T has an inverse in T.
Since $t' \in T$ and any element in T has an inverse in T, in particular, t' has an inverse in T. i.e., t^{-1} exists and $t'^{-1} \in T$.
Since S is a group, by definition, any element in S has an inverse in S.
Since $s' \in S$ and any element in S has an inverse in S, in particular, s' has an inverse in S. i.e., s^{-1} exists and $s'^{-1} \in S$.
Since $x = t'^{-1}s'^{-1}$ and $t'^{-1} \in T$ and $s'^{-1}) \in S$, $x \in TS$.
Since for any $x \in ST$, $x \in TS$, $ST \subseteq TS$.
[$ST = TS \implies ST$ ***is a group***]
For the reverse direction, assume that $ST = TS$.
We are to prove that $(ST, *)$ is a subgroup of $(G, *)$.
Part 0. $ST \subseteq G$.
Part 1. Closure.
Let x_1 and x_2 be two arbitrary elements in ST.
Since $x_1 \in ST$, $x_1 = s_1t_1$ for some $s_1 \in S$ and some $t_1 \in T$.
Since $x_2 \in ST$, $x_2 = s_2t_2$ for some $s_2 \in S$ and some $t_2 \in T$.
Since $x_1 = s_1t_1$ and $x_2 = s_2t_2$, $x_1x_2 = s_1t_1s_2t_2$.
Since $t_1 \in T$ and $s_2 \in S$, $t_1s_2 \in TS$.
Since $t_1s_2 \in TS$ and $ST = TS$, $t_1s_2 \in ST$.
Since $t_1s_2 \in ST$, $t_1s_2 = s't'$ for some $s' \in S$ and $t' \in T$.
Since $x_2x_2 = s_1t_1s_2t_2$ and $t_1s_2 = s't'$, $x_2x_2 = s_1s't't_2$.
Since $(S, *)$ is a group, it is closed under $*$.
Since $(S, *)$ is closed under $*$ and $s_1, s' \in S$, in particular, $s_1s' \in S$.
Since $(T, *)$ is a group, it is closed under $*$.
Since $(T, *)$ is closed under $*$ and $t', t_2 \in T$, in particular, $t't_2 \in T$.
Since $x_2x_2 = s_1s't't_2$ and $s_1s' \in S$ and $t't_2 \in T$, $x_1x_2 \in ST$.
Since $x_1x_2 \in ST$ for any $x_1, x_2 \in ST$, $(ST, *)$ is closed under $*$.
Part 2. Associativity.
Follows directly from the associativity of $*$ on G.
Part 3. Identity.
Let id be the identity element in $(G, *)$.
Since $(S, *)$ is a subgroup of $(G, *)$, $id \in S$.

Since $(T, *)$ is a subgroup of $(G, *)$, $id \in T$.
Since $id \in S, T$, $id \in ST$.
Since id is the identity element in $(G, *)$ and $ST \subseteq G$, id is the identity element in $(ST, *)$.
Part 4. Invertibility.
Let x be an arbitrary element in ST.
Since $x \in ST$, $x = st$ for some element s in S and some element t in T.
Since S is a group, any element in T has an inverse in T.
Since $s \in S$ and any element in S has an inverse in S, in particular, s has an inverse in S. i.e., s^{-1} exists and $s^{-1} \in S$.
Since T is a group, any element in T has an inverse in T.
Since $t \in T$ and any element in T has an inverse in T, in particular, t has an inverse in T. i.e., t^{-1} exists and $t^{-1} \in T$.
Define $x' := t^{-1}s^{-1}$.
Since $t^{-1} \in T$ and $s^{-1} \in S$ and $x' = t^{-1}s^{-1}$, $x' \in TS$.
Since $ST = TS$ and $x' \in TS$, $x' \in ST$.
Since $x = st$ and $x' = t^{-1}s^{-1}$,

$$\begin{aligned} xx' &= stt^{-1}s^{-1} \\ &= s * (t * t^{-1}) * s^{-1} \\ &= s * id * s^{-1} \\ &= s * s^{-1} \\ &= id. \end{aligned}$$

Since $x = st$ and $x' = t^{-1}s^{-1}$,

$$\begin{aligned} x'x &= t^{-1}s^{-1}st \\ &= t^{-1} * (s^{-1} * s) * t \\ &= t^{-1} * id * t \\ &= t^{-1} * t \\ &= id. \end{aligned}$$

Since $x' \in ST$ and $xx' = id$ and $x'x = id$, by definition of inverse, x' is the inverse of x in $(ST, *)$.

■

2

Normal Subgroups

2.1 Definitions and Equivalent Conditions

Definition (Normal Subgroup)**.** *Let $(G, *)$ be a group. Let $(N, *)$ be a subgroup of $(G, *)$. We say that $(N, *)$ is a **normal subgroup** of $(G, *)$ if $(N, *)$ is invariant under conjugation. i.e., if $gng^{-1} \in N$ for any $g \in G$ and any $n \in N$. Or equivalently, if $gNg^{-1} \subseteq N$ for any $g \in G$.*

Definition (Normal Subgroup)**.** *Let $(G, *)$ be a group. Let $(N, *)$ be a subgroup of $(G, *)$. We say that $(N, *)$ is a **normal subgroup** of $(G, *)$ if the left and right cosets of N for any element in G coincide.*

Proposition 2.1.1. *The two definitions of normal subgroup are equivalent.*

Proof.

■

2.2 Properties

Proposition 2.2.1. *The product of a normal subgroup with any other subgroup is a subgroup.*

Proof.
Let $(G, *)$ be a group.
Let $(N, *)$ be a normal subgroup of $(G, *)$.
Let $(H, *)$ be an arbitrary subgroup of $(G, *)$.
We are to prove that $HN = NH$.
[***Forward Direction.*** $HN \subseteq NH$]

For one direction, let x be an arbitrary element in HN.
Since $x \in HN$, $x = hn$ for some $h \in H$ and some $n \in N$.
Since $(H, *)$ is a group, by definition of group, any element in H has an inverse in H.
Since $h \in H$ and any element in H has an inverse, in particular, h has an inverse in H. i.e., h^{-1} exists and $h^{-1} \in H$.
Define $n' := hnh^{-1}$.
Since $n' = hnh^{-1}$, $x = hn = hnh^{-1}h = n'h$.
Since $(H, *)$ is a subgroup of $(G, *)$, $H \subseteq G$.
Since $h \in H$ and $H \subseteq G$, $h \in G$.
Since $(N, *)$ is a normal subgroup of $(G, *)$, by definition of normality, $gng^{-1} \in N$ for any $g \in G$ and any $n \in N$.
Since $h \in G$ and $n \in N$ and $n' = hnh^{-1}$ and $gng^{-1} \in N$ for any $g \in G$ and any $n \in N$, in particular, $n' \in N$.
Since $n' \in N$ and $h \in H$ and $x = n'h$, $x \in NH$.
Since $x \in NH$ for any $x \in HN$, $NH \subseteq HN$.
[***Backward Direction.*** $HN \subseteq NH$]
For the reverse direction, let x be an arbitrary element in NH.
Since $x \in NH$, $x = nh$ for some $n \in N$ and some $h \in H$.
Since $(H, *)$ is a group, by definition of group, any element in H has an inverse in H.
Since $h \in H$ and any element in H has an inverse, in particular, h has an inverse in H. i.e., h^{-1} exists and $h^{-1} \in H$.
Define $n' := h^{-1}nh$.
Since $n' = h^{-1}nh$, $x = nh = hh^{-1}nh = hn'$.
Since $(H, *)$ is a subgroup of $(G, *)$, $H \subseteq G$.
Since $h \in H$ and $H \subseteq G$, $h \in G$.
Since $(N, *)$ is a normal subgroup of $(G, *)$, by definition of normality, $g^{-1}ng \in N$ for any $g \in G$ and any $n \in N$.
Since $h \in G$ and $n \in N$ and $n' = h^{-1}nh$ and $g^{-1}ng \in N$ for any $g \in G$ and any $n \in N$, in particular, $n' \in N$.
Since $n' \in N$ and $h \in H$ and $x = hn'$, $x \in HN$.
Since $x \in HN$ for any $x \in NH$, $HN \subseteq HN$.
[***Summary.***]
Since $(H, *)$ and $(N, *)$ are subgroups of $(G, *)$ and $HN = NH$, $(HN, *)$ and $(NH, *)$ are subgroups of $(G, *)$.

■

Proposition 2.2.2. *The product of two normal subgroups is also a normal subgroup.*

Proof.

Let $(G, *)$ be a group.
Let $(N, *)$ and $K, *)$ be two arbitrary normal subgroups of $(G, *)$.
We are to prove that NK is a normal subgroup of $(G, *)$.
Since $(N, *)$ and $(K, *)$ are both normal, $(NK, *)$ is a subgroup of $(G, *)$.
Let x be an arbitrary element in NK.
Since $x \in NK$, $x = nk$ for some $n \in N$ and some $k \in K$.
Let g be an arbitrary element in G.
Since $(G, *)$ is a group and $g \in G$, g^{-1} exists and $g^{-1} \in G$.
Since $(N, *)$ is a normal subgroup of $(G, *)$, $gng^{-1} \in N$.
Since $(K, *)$ is a normal subgroup of $(G, *)$, $gkg^{-1} \in K$.
Since $gng^{-1} \in N$ and $gkg^{-1} \in K$, $gng^{-1}gkg^{-1} \in NK$.
Since $gxg^{-1} = gnkg^{-1} = gng^{-1}gkg^{-1}$ and $gng^{-1}gkg^{-1} \in NK$, $gxg^{-1} \in NK$.
Since $gxg^{-1} \in NK$ for any $x \in NK$ and any $g \in G$, by definition of normal subgroup, $(NK, *)$ is a normal subgroup of $(G, *)$.

■

3

Cosets

3.1 Definitions

Definition (Left Coset)**.** *Let $(G, *)$ be a group. Let $(H, *)$ be a subgroup of $(G, *)$. Let g be an element in G. We define the* ***left*** *coset of H determined by g, denoted by gH, to be the set given by*

$$gH := \{gh : h \in H\}.$$

Definition (Right Coset)**.** *Let $(G, *)$ be a group. Let $(H, *)$ be a subgroup of $(G, *)$. Let g be an element in G. We define the* ***right*** *coset of H determined by g, denoted by Hg, to be the set given by*

$$Hg := \{hg : h \in H\}.$$

3.2 Properties

Proposition 3.2.1. *All cosets have the same cardinality.*