20241008 MATH3301 NOTE 5[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Introduction

This note introduces some constructions of subgroups, including but limited to set-generated subgroup, centralizer subgroup, normalizer subgroup and commutator subgroup.

2 Preliminaries

Definition 2.1. (**Group**)
Let G be a set, and $\circ : (g_1, g_2) \mapsto g_1 g_2$ be a binary operation on G. If:
(1) $\forall g_1, g_2, g_3 \in G, (g_1 g_2) g_3 = g_1 (g_2 g_3) \in G$;
(2) $\exists e \in G, \forall g \in G, eg = ge = g$;
(3) $\forall g \in G, \exists h \in G, hg = gh = e$,
then G is a group under $\circ$.

Remark: *It is easy to show that:*
(1) e is unique in G;
(2) $\forall g \in G$, h is unique in G.
Hence, we may apply the notation g^{-1} for the inverse of g.

Definition 2.2. (**Subgroup**)
Let G be a group under $\circ$, and H be a subset of G. If:
(1) $e \in H$;
(2) $\forall h_1, h_2 \in G, h_1 \in H$ and $h_2 \in H \implies h_1 h_2 \in H$;
(3) $\forall h \in G, h \in H \implies h^{-1} \in H$,
then $H \leq G$, i.e., H is a subgroup of G.

Definition 2.3. (**Coset**)
Let G be a group under $\circ$, H be a subgroup of G, and g be an element of G.
Define $gH = \{gh\}_{h \in H}$ as the left $H-$coset of g;
Define $Hg = \{hg\}_{h \in H}$ as the right $H-$coset of g.

Remark: *One may expand a "word" as follows:*

$$uH^2vIJ = \{uh_1h_2vij \in G : h_1, h_2 \in H \text{ and } i \in I \text{ and } j \in J\}$$

Theorem 2.4. (**Lagrange's Theorem**)
Let G be a group under $\circ$, and H be a subgroup of G.
$G/H = \{gH\}_{g \in G}$ partitions G.

Proof. We may divide our proof into three parts.
Part 1: For all $gH \in G/H$, there exists $g = ge \in gH$, so $gH \neq \emptyset$.

Part 2: For all $g_1H, g_2H \in G/H$:

$$\begin{aligned} g_1H \cap g_2H \neq \emptyset &\implies \exists h_1, h_2 \in H, g_1h_1 = g_2h_2 \\ &\implies \exists h_2h_1^{-1} \in H, g_1 = g_2h_2h_1^{-1} \implies g_1H = g_2H \end{aligned}$$

Part 3: For all $g \in G$, there exists $gH \in G/H$, such that $g = ge \in gH$.
Hence, G/H partitions G. Quod. Erat. Demonstrandum. □

Remark: *It is easy to show that $H \to gH, h \mapsto gh$ is a bijection, so each coset gH have the same cardinality, which implies the order of H divides the order of G.*

Definition 2.5. (**Normal Subgroup**)
Let G be a group under $\circ$, and H be a subgroup of G.
If $\forall g \in G, gH = Hg$, then $H \trianglelefteq G$, i.e., H is normal in G.

Remark: *As a corollary, for all subgroups H, K of G, $H \trianglelefteq G \implies KH = HK$.*

Proposition 2.6. $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$

Proof. We may divide our proof into four parts.
Part 1: $e \in \{e\}$ and $e \in G$.
Part 2: $ee \in \{e\}$ and $\forall g_1, g_2 \in G, g_1g_2 \in G$.
Part 3: $e^{-1} = e \in \{e\}$ and $\forall g \in G, g^{-1} \in G$
Part 4: $\forall g \in G, g\{e\} = \{e\}g = \{g\}$ and $\forall g \in G, gG = Gg = G$.
Hence, $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$. Quod. Erat. Demonstrandum. □

Proposition 2.7. $H_1 \trianglelefteq G$ and $H_2 \trianglelefteq G \implies H_1 \cap H_2 \trianglelefteq G$

Proof. We may divide our proof into four parts.
Part 1: $e \in H_1$ and $e \in H_2 \implies e \in H_1 \cap H_2$.
Part 2: For all $g, g' \in G$:

$$\begin{aligned} g \in H_1 \cap H_2 \text{ and } g' \in H_1 \cap H_2 &\implies g \in H_1 \text{ and } g \in H_2 \text{ and } g' \in H_1 \text{ and } g' \in H_2 \\ &\implies gg' \in H_1 \text{ and } gg' \in H_2 \\ &\implies gg' \in H_1 \cap H_2 \end{aligned}$$

Part 3: For all $g \in G$:

$$\begin{aligned} g \in H_1 \cap H_2 &\implies g \in H_1 \text{ and } g \in H_2 \\ &\implies g^{-1} \in H_1 \text{ and } g^{-1} \in H_2 \\ &\implies g^{-1} \in H_1 \cap H_2 \end{aligned}$$

Part 4: For all $g \in G$:

$$g(H_1 \cap H_2) = (gH_1) \cap (gH_2) = (H_1 g) \cap (H_2 g) = (H_1 \cap H_2)g$$

Hence, $H_1 \cap H_2 \trianglelefteq G$. Quod. Erat. Demonstrandum. $\square$

Remark: *This can be generalized to:*

$$\text{Each } H_\lambda \trianglelefteq G \implies \bigcap_{\lambda \in I} H_\lambda \trianglelefteq G$$

Proposition 2.8. $H_1 \trianglelefteq G$ and $H_2 \trianglelefteq G \implies H_1 H_2 \trianglelefteq G$

Proof. We may divide our proof into four parts.
Part 1: $e \in H_1$ and $e \in H_2 \implies e = ee \in H_1 H_2$.
Part 2: For all $g, g' \in G$:

$$\begin{aligned} g \in H_1H_2 \text{ and } g' \in H_1H_2 &\implies \exists h_1, h_1' \in H_1 \text{ and } h_2, h_2' \in H_2, g = h_1h_2 \text{ and } g' = h_1'h_2' \\ &\implies \exists h_1'' \in H_1 \text{ and } h_2'' \in H_2, h_2h_1' = h_1''h_2'' \\ &\implies \exists h_1h_1'' \in H_1 \text{ and } h_2''h_2' \in H_2, gg' = h_1h_1''h_2''h_2' \\ &\implies gg' \in H_1H_2 \end{aligned}$$

Part 3: For all $g \in G$:

$$\begin{aligned} g \in H_1H_2 &\implies \exists h_1 \in H_1 \text{ and } h_2 \in H_2, g = h_1h_2 \\ &\implies \exists h_1' \in H_1 \text{ and } h_2' \in H_2, h_1h_2 = h_2'h_1' \\ &\implies \exists h_1'^{-1} \in H_1 \text{ and } h_2' \in H_2, g^{-1} = h_1'^{-1}h_2'^{-1} \\ &\implies g^{-1} \in H_1H_2 \end{aligned}$$

Part 4: For all $g \in G$:

$$gH_1H_2 = H_1gH_2 = H_1H_2g$$

Hence, $H_1, H_2 \trianglelefteq G$. Quod. Erat. Demonstrandum. $\square$

Remark: *This can be generalized to:*

$$\text{Each } H_k \trianglelefteq G \implies \prod_{k=1}^{m} H_k \trianglelefteq G$$

Definition 2.9. (**Quotient Group**)
Let G be a group under $\circ$, and H be a normal subgroup of G.
Define $\circ : (g_1H, g_2H) \mapsto g_1g_2H$. Observe that:
(1) $\circ$ is a well-defined binary operation on G/H;
(2) G/H is a group under $\circ$.
Hence, define this group as the quotient group of G by H.

Proof. Let's prove the two observations above.
(1) For all $(g_1H, g_2H), (g_1'H, g_2'H) \in G/H \times G/H$:

$$\begin{aligned}
(g_1H, g_2H) = (g_1'H, g_2'H) &\implies g_1H = g_1'H \text{ and } g_2H = g_2'H \\
&\implies \exists h_1, h_2 \in H, g_1 = g_1'h_1 \text{ and } g_2 = g_2'h_2 \\
&\implies \exists h_1'' \in H, h_1g_2' = g_2'h_1'' \\
&\implies \exists h_3h_2 \in H, g_1g_2 = g_1'g_2'h_1''h_2 \\
&\implies g_1g_2H = g_1'g_2'H
\end{aligned}$$

Hence, $\circ$ is a well-defined operation on G/H.
(2) We may divide our proof into three parts.
Part 1: For all $g_1H, g_2H, g_3H \in G/H$:

$$\begin{aligned}
(g_1Hg_2H)g_3H &= g_1g_2Hg_3H = (g_1g_2)g_3H \\
&= g_1(g_2g_3)H = g_1Hg_2g_3H = g_1H(g_2Hg_3H)
\end{aligned}$$

Part 2: There exists $eH \in G/H$, such that for all $gH \in G/H$:

$$eHgH = egH = gH \text{ and } gHeH = geH = gH$$

Part 3: For all $gH \in G/H$, there exists $g^{-1}H \in G/H$, such that:

$$g^{-1}HgH = g^{-1}gH = eH \text{ and } gHg^{-1}H = gg^{-1}H = eH$$

Hence, G/H is a group under $\circ$. Quod. Erat. Demonstrandum. □

3 Set-generated Subgroup

Definition 3.1. (**Word**)
Let G be a group, and A be a subset of G.
If $g = e$ or $g = g_1g_2\cdots g_m$ is a finite product of elements in A,
then g is a word in A.

Definition 3.2. (**Set-generated Subgroup**)
Let G be a group, and A be a subset of G.
Define the subgroup of G generated by A as:

$$\langle A\rangle = \{g \in G : g \text{ is a word in } A \cup A^{-1}\}$$

Proposition 3.3. Let G be a group, and A be a subset of G.

$$\langle A\rangle \leq G$$

Proof. We may divide our proof into three parts.
Part 1: $e \in \langle A\rangle$.
Part 2: $\forall g = g_1 g_2 \cdots g_m, h = h_1 h_2 \cdots h_n \in \langle A\rangle, gh = g_1 g_2 \cdots g_m h_1 h_2 \cdots h_n \in \langle A\rangle$.
Part 3: $\forall g = g_1 g_2 \cdots g_m \in \langle A\rangle, g^{-1} = g_m^{-1} \cdots g_2^{-1} g_1^{-1} \in \langle A\rangle$.
Hence, $\langle A\rangle \leq G$. Quod. Erat. Demonstrandum. □

Proposition 3.4. Let $E_n(\mathbb{F})$ be the set of all elementary matrices in $GL_n(\mathbb{F})$.

$$GL_n(\mathbb{F}) = \langle E_n(\mathbb{F})\rangle$$

Definition 3.5. (**Cyclic Subgroup**)
Let G be a group, and g be an element of G.
Define the cyclic subgroup of G generated by g as:

$$\langle g\rangle = \langle\{g\}\rangle$$

Proposition 3.6. Let G be a group, and g be an element of G.
(1) If $|\langle g\rangle| = m$, then $\sigma : \langle g\rangle \to \mathbb{Z}_m, \sigma(g^k) = [k]_m$ is an isomorphism.
(2) If $|\langle g\rangle| = +\infty$, then $\sigma : \langle g\rangle \to \mathbb{Z}, \sigma(g^k) = k$ is an isomorphism.

Proof. We may divide our proof into three parts.
Part 1: We prove that the two functions are well-defined.
(1) $\forall g^k, g^{k'} \in \langle g\rangle, g^k = g^{k'} \implies k \equiv k' (\text{mod } m) \implies [k]_m = [k']_m$.
(2) $\forall g^k, g^{k'} \in \langle g\rangle, g^k = g^{k'} \implies k = k'$.
Part 2: We prove that the two functions are bijective.
(1) Every $[k]_m \in \mathbb{Z}_m$ has a unique preimage $g^k \in \langle g\rangle$.
(2) Every $k \in \mathbb{Z}$ has a unique preimage $g^k \in \langle g\rangle$.
Part 3: We prove that the two functions preserve commpositions.
(1) $\forall g^k, g^{k'} \in \langle g\rangle, \sigma(g^k g^{k'}) = \sigma(g^{k+k'}) = [k+k']_m = [k]_m + [k']_m = \sigma(g^k) + \sigma(g^{k'})$.
(2) $\forall g^k, g_{k'} \in \langle g\rangle, \sigma(g^k g^{k'}) = \sigma(g^{k+k'}) = k + k' = \sigma(g^k) + \sigma(g^{k'})$.
Hence, both maps are isomorphisms. Quod. Erat. Demonstrandum. □

4 Centralizer Subgroup

Definition 4.1. (**Centralizer Subgroup**)
Let G be a group, and H be a subgroup of G.
Define the centralizer subgroup of H in G as:

$$C(H) = \{g \in G : \forall h \in H, gh = hg\}$$

Proposition 4.2. Let G be a group, and H be a subgroup of G.

$$C(H) \leq G$$

Proof. We may divide our proof into three parts.
Part 1: $\forall h \in H, eh = he = h$, so $e \in C(H)$.
Part 2: For all $g, g' \in G$:

$$\begin{aligned} g, g' \in C(H) &\implies \forall h \in H, gh = hg \text{ and } g'h = hg' \\ &\implies \forall h \in H, gg'h = ghg' = hgg' \\ &\implies gg' \in C(H) \end{aligned}$$

Part 3: For all $g \in G$:

$$\begin{aligned} g \in C(H) &\implies \forall h \in H, gh = hg \\ &\implies \forall h \in H, g^{-1}h = (h^{-1}g)^{-1} = (gh^{-1})^{-1} = hg^{-1} \\ &\implies g^{-1} \in C(H) \end{aligned}$$

Hence, $C(H) \leq G$. Quod. Erat. Demonstrandum. $\square$

Remark: *Note that $H \not\leq C(H)$ and $C(H) \not\leq H$ in general.*

Proposition 4.3. Let $\tilde{I}$ be the set of all scalar matrices in $GL_n(\mathbb{F})$.

$$C(GL_n(\mathbb{F})) = \tilde{I}$$

5 Normalizer Subgroup

Definition 5.1. (**Normalizer Subgroup**)
Let G be a group, and H be a subgroup of G.
Define the normalizer subgroup of H in G as:

$$N(H) = \{g \in G : gH = Hg\}$$

Proposition 5.2. Let G be a group, and H be a subgroup of G.

$$N(H) \leq G$$

Proof. We may divide our proof into three parts.
Part 1: $eH = H = He$, so $e \in N(H)$.
Part 2: For all $g, g' \in G$:

$$\begin{aligned} g, g' \in N(H) &\implies gH = Hg \text{ and } g'H = Hg' \\ &\implies gg'H = gHg' = Hgg' \\ &\implies gg' \in N(H) \end{aligned}$$

Part 3: For all $g \in G$:

$$\begin{aligned} g \in N(H) &\implies gH = Hg \\ &\implies g^{-1}H = (Hg)^{-1} = (gH)^{-1} = Hg^{-1} \\ &\implies g^{-1} \in N(H) \end{aligned}$$

Hence, $N(H) \leq G$. Quod. Erat. Demonstrandum. □

Remark: *Note that* $H \trianglelefteq N(H)$.

Proposition 5.3. Let G be a group, and H be a subgroup of G.

$$C(H) \trianglelefteq N(H)$$

Proof. We may divide our proof into two parts.
Part 1: For all $g \in G$:

$$\begin{aligned} g \in C(H) &\implies \forall h \in H, gh = hg \\ &\implies gH = Hg \\ &\implies g \in N(H) \end{aligned}$$

Part 2: For all $c \in C(H)$ and $n \in N(H)$:

$$\forall h \in H, hncn^{-1} = nh'cn^{-1} = nch'n^{-1} = ncn^{-1}h \implies ncn^{-1} \in C(H)$$

Hence, $C(H) \trianglelefteq N(H)$. Quod. Erat. Demonstrandum. □

Remark: *ChatGPT helped me in formulating the proof.*

6 Commutator Subgroup

Definition 6.1. (**Commutator**)
Let G be a group, and g, g' be two elements of G.
Define the commutator of g, g' in G as:

$$[g, g'] = gg'g^{-1}g'^{-1}$$

Definition 6.2. (**Commutator Subgroup**)
Let G be a group, and H, H' be two subgroups of G. Define the commutator subgroup $[H, H']$ of H, H' in G as the subgroup of G generated by:

$$\{[h, h'] \in G : h \in H \text{ and } h' \in H'\}$$

Proposition 6.3. Let G be a group.

$$[G, G] \trianglelefteq G$$

Proof. For all $a, b, c \in G$:

$$\begin{aligned}
(cac^{-1})^{-1} &= (c^{-1})^{-1}a^{-1}c^{-1} = ca^{-1}c^{-1} \\
(cbc^{-1})^{-1} &= (c^{-1})^{-1}b^{-1}c^{-1} = cb^{-1}c^{-1} \\
[cac^{-1}, cbc^{-1}] &= cac^{-1}cbc^{-1}ca^{-1}c^{-1}cb^{-1}c^{-1} \\
&= caba^{-1}b^{-1}c^{-1} = c[a, b]c^{-1}
\end{aligned}$$

Hence, $[G, G]$ is closed under conjugation, which implies $[G, G] \trianglelefteq G$.
Quod. Erat. Demonstrandum. $\square$

References

[1] H. Ren, "Template for math notes," 2021.