20240926 MATH3301 NOTE 4[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

In linear algebra, we tend to define determinant as:

$$\det\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} = \sum_{\{j_1,j_2,\cdots,j_m\}=\{1,2,\cdots,m\}} \tau a_{1j_1}a_{2j_2}\cdots a_{mj_m}$$

Here, τ is the sign of the following permutation:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_{1j_1} & a_{2j_2} & \cdots & a_{mj_m} \end{pmatrix}$$

Clearly, we need to define τ before we define determinant. In order to show τ is well-defined, we shall not rely on determinant, otherwise, there is a vicious circle. Hence, this note proposes a construction to solve this problem.

2 Preliminaries

Definition 2.1. (**Group**)
Let G be a set, and $\circ : (g_1, g_2) \mapsto g_1g_2$ be a binary operation on G. If:
(1) $\forall g_1, g_2, g_3 \in G, (g_1g_2)g_3 = g_1(g_2g_3) \in G$;
(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 $h_2 \in H \implies h_1h_2 \in H$;
(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. □

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 $g, g' \in G$:

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

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

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

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

$$gH_1H_2 = H_1gH_2 = H_1H_2g$$

Hence, $H_1, H_2 \trianglelefteqslant G$. Quod. Erat. Demonstrandum. □

Remark: *This can be generalized to:*

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

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 Construction of S_m

Definition 3.1. (**The Symmetric Group** S_m)
Let S_m be the set of all bijective functions on $\{1, 2, \cdots, m\}$. Observe that:
(1) Composition $\circ$ is a well-defined operation on S_m;
(2) S_m is a group under $\circ$.
Hence, define this group as the symmetric group S_m.

Proof. Let's prove the two observations above.
(1) For all bijective functions f_1, f_2 on $\{1, 2, \cdots, m\}$,
$f_1 f_2$ is a bijective function on $\{1, 2, \cdots, m\}$.
Hence, $\circ$ is a well-defined operation on S_m.
(2) We may divide our proof into three parts.
Part 1: Composition $\circ$ is associative in general, so it is associative in S_m.
Part 2: The identity function e is an identity in S_m.
Part 3: For all $f \in S_m$, its inverse function f^{-1} is an inverse of f in S_m.
Combine the three parts above, we've proven that S_m is a group under $\circ$.
Quod. Erat. Demonstrandum. □

4 Construction of A_m

Definition 4.1. (**The Alternating Group** A_m)
Define the alternating group A_m as the largest proper normal subgroup of S_m.

Remark: *The word "largest" here means the maximal element of subset relation. We need to show that such maximal element exists and is unique.*

5 Transposition

Definition 5.1. (**Transposition**)
Let k_1, k_2 be two distinct elements of $\{1, 2, \cdots, m\}$. Define:

$$(k_1, k_2) \in S_m, (k_1, k_2)(k) = \begin{cases} k_2 & \text{if} \quad k = k_1; \\ k_1 & \text{if} \quad k = k_2; \\ k & \text{if} \quad k \neq k_1, k_2; \end{cases}$$

as a transposition.

Lemma 5.2. When $m \geq 2$, each $f \in S_m$ is a product of transpositions.

Proof. We may divide our proof into two cases.
Case 1: If $f = e$, then $e = (1, 2)(1, 2)$ is a product of transpositions.

Case 2: If $f \neq e$, then find the smallest $1 \leq k \leq m$ such that $f(k) \neq k$.
Consider the product $(k, f(k))f$.
Situation 2.1: If $(k, f(k))f = e$, then $f = (k, f(k))$ is a transposition.
Situation 2.2: If $(k, f(k))f \neq e$, then define $g = (k, f(k))f$ and repeat the process.
This process will eventually end because there are finitely many element to permute.
Hence, $f = (k, f(k))g$ is a product of transpositions.
Quod. Erat. Demonstrandum. □

Lemma 5.3. Let H be a normal subgroup of S_m.
If H contains some transposition, then H contains all transposition.

Proof. Assume that H contains some transposition (k_1, k_2).
For all transposition (k_3, k_4), define f by:

$$f(k) = \begin{cases} k_3 & \text{if} \quad k = k_1; \\ k_4 & \text{if} \quad k = k_2; \\ k_1 & \text{if} \quad k = k_3; \\ k_2 & \text{if} \quad k = k_4; \\ k & \text{if} \quad k \neq k_1, k_2, k_3, k_4; \end{cases}$$

As $k_1 \neq k_2$ and $k_3 \neq k_4$, f is a well-defined bijection on $\{1, 2, \cdots, m\}$, so:

$$(k_3, k_4) = f(k_1, k_2)f^{-1} \in fHf^{-1} = H$$

Quod. Erat. Demonstrandum. □

Remark: *This implies no $H \lhd G$ contains any transposition.*

Theorem 5.4. When $m \geq 2$, there exists a unique A_m.

Proof. We may divide our proof into two parts.
Part 1: In this part, we prove the existence of A_m.
Define $\text{Spec}(S_m) = \{H\}_{H \lhd S_m}$.
We want to find a maximal element $A_m \in \text{Spec}(S_m)$ of $\text{Spec}(S_m)$.
Assume to the contrary that such element fails to exist.
There exists a sequence of normal subgroups $(H_n)_{n \in \mathbb{N}}$ of S_m, such that:

$$\forall n \in \mathbb{N}, H_n \subset H_{n+1}$$

But S_m is finite, it cannot have infinitely many $H_n \in \text{Spec}(S_m)$, a contradiction.
Hence, there exists $A_m \in \text{Spec}(S_m)$, such that for all $H \in \text{Spec}(S_m)$:

$$A_m \subseteq H \implies A_m = H$$

Part 2: In this part, we prove the uniqueness of A_m.

For all transposition (k_1, k_2), as A_m is maximal,
the smallest normal subgroup of S_m containing $A_m \cup \{(k_1, k_2)\}$ is S_m.
Hence, $S_m = A_m \sqcup (k_1, k_2)A_m$.
For all transpositions $(k_1, k_2), (k_1', k_2')$:

$$(k_1, k_2)A_m = (k_1', k_2')A_m = S_m \backslash A_m \implies (k_1, k_2)(k_1', k_2') \in A_m$$

This implies:
(1) All even product of transpositions is contained in A_m.
(2) All odd product of transpositions is contained in $S_m \backslash A_m$.
As the two types of products partition S_m, A_m is unique.
Quod. Erat. Demonstrandum. □

References

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