20240929 MATH3301 Tutorial 5

1. Solution:

When $G=S_3$, $H=\{e,(1,2)\}$, $K=\{e,(1,3)\}$,

$HK=\{e,(1,2),(1,3),(1,3,2)\}$ is not closed under inverse.

To be specific, there exists $(1,3,2)\in HK$, such that $(1,3,2)^{-1}=(1,2,3)\notin HK$.

Hence, HK is not a subgroup.

We may prove "HK is a subgroup of G if and only if $HK=KH$" in two parts.

Part 1: Assume that HK is a subgroup of G.

For all $hk\in HK$, as HK is closed under inverse, $k^{-1}h^{-1}=(hk)^{-1}\in HK$.

This implies for some $h'\in H$ and $k'\in K$, $k^{-1}h^{-1}=h'k'$, so $hk=(h'k')^{-1}=k'^{-1}h'^{-1}\in KH$.

For all $kh\in KH$, $h^{-1}k^{-1}\in HK$. As HK is closed under inverse,

$kh=(h^{-1}k^{-1})^{-1}\in HK$. Hence, $HK=KH$.

Part 2: Assume that $HK=KH$.

First, $e\in H$ and $e\in K$ implies $e=ee\in HK$.

Second, for all $h_1k_1, h_2k_2\in HK$, $k_1h_2\in KH=HK$, so $k_1h_2=h_3k_3$ for some

$h_3\in H$ and $k_3\in K$. As H,K are closed under composition, $h_1k_1h_2k_2=h_1h_3k_3k_2\in HK$.

Third, for all $hk\in HK=KH$, there exist $h'\in H$ and $k'\in K$, such that

$hk=k'h'$. As H,K are closed under inverse, $(hk)^{-1}=h'^{-1}k'^{-1}\in HK$.

Hence, HK is a subgroup of G.

Combine the two parts above, we've proven the biconditional.

(i) Take $G=\mathbb{Z}_6$, $H=2\mathbb{Z}_6=\{0,2,4\}$, $K=3\mathbb{Z}_6=\{0,3\}$. Now $H+K=\mathbb{Z}_6\cong\mathbb{Z}_2\times\mathbb{Z}_3=H\times K$;

(ii) Take $G=\mathbb{Z}_6$, $H=2\mathbb{Z}_6=\{0,2,4\}$, $K=\mathbb{Z}_6=\{0,1,2,3,4,5,6\}$. Now $H+K=\underbrace{\mathbb{Z}_6}_{\text{cardinality } 6}\ncong\underbrace{\mathbb{Z}_2\times\mathbb{Z}_6}_{\text{cardinality } 12}=H\times K$;

2. Solution:

We may prove "$[H,H]$ is a subgroup of $[G,G]$" in four parts.

Part 1: H is a subset of G, so $[H,H]=\langle xyx^{-1}y^{-1}\rangle_{(x,y)\in H\times H}$ is a subset of $[G,G]=\langle xyx^{-1}y^{-1}\rangle_{(x,y)\in G\times G}$.

Part 2: $e\in H$, so $e=eee^{-1}e^{-1}\in[H,H]$;

Part 3: For all $x_1y_1x_1^{-1}y_1^{-1}x_2y_2x_2^{-1}y_2^{-1}\cdots x_{n-1}y_{n-1}x_{n-1}^{-1}y_{n-1}^{-1}x_ny_nx_n^{-1}y_n^{-1}$,

$x_1'y_1'x_1'^{-1}y_1'^{-1}x_2'y_2'x_2'^{-1}y_2'^{-1}\cdots x_{n'-1}'y_{n'-1}'x_{n'-1}'^{-1}y_{n'-1}'^{-1}x_{n'}'y_{n'}'x_{n'}'^{-1}y_{n'}'^{-1}\in[H,H]$,

their product:

$x_1y_1x_1^{-1}y_1^{-1}x_2y_2x_2^{-1}y_2^{-1}\cdots x_{n-1}y_{n-1}x_{n-1}^{-1}y_{n-1}^{-1}x_ny_nx_n^{-1}y_n^{-1}x_1'y_1'x_1'^{-1}y_1'^{-1}x_2'y_2'x_2'^{-1}y_2'^{-1}\cdots x_{n'-1}'y_{n'-1}'x_{n'-1}'^{-1}y_{n'-1}'^{-1}x_{n'}'y_{n'}'x_{n'}'^{-1}y_{n'}'^{-1}$

$\in[H,H]$.

Part 4: For all $x_1y_1x_1^{-1}y_1^{-1}x_2y_2x_2^{-1}y_2^{-1}\cdots x_{n-1}y_{n-1}x_{n-1}^{-1}y_{n-1}^{-1}x_ny_nx_n^{-1}y_n^{-1}\in[H,H]$,

its inverse $y_nx_ny_n^{-1}x_n^{-1}y_{n-1}x_{n-1}y_{n-1}^{-1}x_{n-1}^{-1}\cdots y_2x_2y_2^{-1}x_2^{-1}y_1x_1y_1^{-1}x_1^{-1}\in[H,H]$.

Combine the four parts above, we've proven that $[H,H]$ is a subgroup of $[G,G]$.

To save our labor, construct a homomorphism $\sigma:\overbrace{S_3}^{\text{nonAbelian}}\to\overbrace{\{+1,-1\}^\times}^{\text{Abelian}}$,

where $\sigma(f)$ is the sign of permutation.

For all $xyx^{-1}y^{-1}\in S_3'$, $\sigma(xyx^{-1}y^{-1})=\sigma(x)\sigma(y)\sigma(x^{-1})\sigma(y^{-1})$

$=\sigma(x)\sigma(x^{-1})\sigma(y)\sigma(y^{-1})=\sigma(xx^{-1}yy^{-1})=\sigma(e)=1$, so S_3' is a subgroup of A_3.

For $e\in A_3$, it certainly lies in S_3';

For $(1,2,3)\in A_3$, there exist $(1,2),(1,3)\in S_3$, such that $(1,2,3)=(1,2)(1,3)(1,2)^{-1}(1,3)^{-1}\in S_3'$

For $(1,3,2)\in A_3$, there exist $(1,3),(1,2)\in S_3$, such that $(1,3,2)=(1,3)(1,2)(1,3)^{-1}(1,2)^{-1}\in S_3'$

This implies $S_3'=A_3$, which is an Abelian group, so $S_3''=\{e\}$.

Date / /

3. Solution:

We may prove "G is a group under matrix multiplication" in four parts

Part 1: For all $\begin{pmatrix}1&y_1&z_1\\0&1&x_1\\0&0&1\end{pmatrix},\begin{pmatrix}1&y_2&z_2\\0&1&x_2\\0&0&1\end{pmatrix}\in G$,

there exists a unique $\begin{pmatrix}1&y_1&z_1\\0&1&x_1\\0&0&1\end{pmatrix}\begin{pmatrix}1&y_2&z_2\\0&1&x_2\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y_1+y_2&z_1+z_2+x_2y_1\\0&1&x_1+x_2\\0&0&1\end{pmatrix}\in G$

so matrix multiplication is a well-defined operation on G.

Part 2: Matrix Multiplication is associative in general, so it is associative on G.

Part 3: There exists $\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\in G$, such that for all $\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}\in G$,

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}$$

Part 4: For all $\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}\in G$, there exists $\begin{pmatrix}1&-y&-z+xy\\0&1&-x\\0&0&1\end{pmatrix}\in G$, such that:

$$\begin{pmatrix}1&-y&-z+xy\\0&1&-x\\0&0&1\end{pmatrix}\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}\begin{pmatrix}1&-y&-z+xy\\0&1&-x\\0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

Hence, G is a group under matrix multiplication.

We may prove $Z(G)=[G,G]$ in two parts.

Part 1: For all $\begin{pmatrix}1&0&z_1\\0&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}1&y_2&z_2\\0&1&x_2\\0&0&1\end{pmatrix}\in G$, $\begin{pmatrix}1&0&z_1\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&y_2&z_2\\0&1&x_2\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y_2&z_2\\0&1&x_2\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&z_1\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y_2&z_1+z_2\\0&1&x_2\\0&0&1\end{pmatrix}$,

For all $\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}\in G$, $\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}$ commutes with every $\begin{pmatrix}1&y'&z'\\0&1&x'\\0&0&1\end{pmatrix}$ implies

$$\begin{pmatrix}1&y+1&z\\0&1&x\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y+1&x+z\\0&1&x\\0&0&1\end{pmatrix}$$

and $\begin{pmatrix}1&y&y+z\\0&1&x+1\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}=\begin{pmatrix}1&y&z\\0&1&x+1\\0&0&1\end{pmatrix}$,

so $\begin{pmatrix}1&y&z\\0&1&x\\0&0&1\end{pmatrix}$ must be $\begin{pmatrix}1&0&z\\0&1&0\\0&0&1\end{pmatrix}$. Hence, $Z(G)=\left\{\begin{pmatrix}1&0&z\\0&1&0\\0&0&1\end{pmatrix}\right\}_{z\in\mathbb{R}}$

Part 2: For all $\begin{pmatrix}1&y_1&z_1\\0&1&x_1\\0&0&1\end{pmatrix},\begin{pmatrix}1&y_2&z_2\\0&1&x_2\\0&0&1\end{pmatrix}\in G$,

$$\begin{pmatrix}1&y_1&z_1\\0&1&x_1\\0&0&1\end{pmatrix}\begin{pmatrix}1&y_2&z_2\\0&1&x_2\\0&0&1\end{pmatrix}\begin{pmatrix}1&y_1&z_1\\0&1&x_1\\0&0&1\end{pmatrix}^{-1}\begin{pmatrix}1&y_2&z_2\\0&1&x_2\\0&0&1\end{pmatrix}^{-1}=\begin{pmatrix}1&0&-x_1y_2+x_2y_1\\0&1&0\\0&0&1\end{pmatrix}$$

so $[G,G]=\left\{\begin{pmatrix}1&0&z\\0&1&0\\0&0&1\end{pmatrix}\right\}_{z\in\mathbb{R}}=Z(G)$

If we define:

$$*: \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3, \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} * \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = \begin{bmatrix} x_1+x_2 \\ y_1+y_2 \\ z_1+z_2+x_2y_1 \end{bmatrix}$$

then $\mathbb{R}^3$ forms a group under $*$, and:

$$\sigma: G \to \mathbb{R}^3, \ \sigma\left(\begin{pmatrix} 1 & y & z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}\right) = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

is a group isomorphism.

~~4. Solution:~~ $\sigma(i_1, i_2, \cdots, i_k)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \cdots, \sigma(i_k))$

(i) $C(\alpha) = \{g \in S_4 : g\alpha g^{-1} = \alpha\} = \{g \in S_4 : (g(1), g(3)) = (1,3)\}$

$$= \left\{\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 1&4&3&2 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 3&2&1&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 3&4&1&2 \end{pmatrix}\right\}$$

(ii) $C(\beta) = \{g \in S_4 : g\beta g^{-1} = \beta\} = \{g \in S_4 : g(1,3)g^{-1}g(2,4)g^{-1} = (1,3)(2,4)\}$

Remark: $\{(g(1), g(3)), (g(2), g(4))\} = \{(1,3),(2,4)\}$

$$= \{g \in S_4 : (g(1), g(3))(g(2), g(4)) = (1,3)(2,4)\}$$

$$= \left\{\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 1&4&3&2 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 2&1&4&3 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 2&3&4&1 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 3&2&1&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 3&4&1&2 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 4&1&2&3 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 4&3&2&1 \end{pmatrix}\right\}$$

(iii) $C(\gamma) = \{g \in S_4 : g\gamma g^{-1} = \gamma\} = \{g \in S_4 : (g(1), g(2), g(3)) = (1,2,3)\}$

$$= \left\{\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 2&3&1&4 \end{pmatrix}, \begin{pmatrix} 1&2&3&4 \\ 3&1&2&4 \end{pmatrix}\right\}$$

(iv) $\left\{\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}\right\} \subseteq Z(S_4) \subseteq C(\alpha) \cap C(\beta) \cap C(\gamma) = \left\{\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}\right\}$

Hence, $Z(S_4) = \left\{\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}\right\}$.

5\. Solution: $Aut(G)$ is the set of all isomorphism on G

(i) $Aut(\mathbb{Z}_4) \leq S_4$ (Here we are permuting $\overset{ord=1}{0}, \underset{ord=4}{1}, \overset{ord=2}{2}, \underset{ord=4}{3}$)

$$Aut(\mathbb{Z}_4) = \left\{ \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 2 & 1 \end{pmatrix} \right\}$$

As $|Aut(\mathbb{Z}_4)| = |\mathbb{Z}_2| = |\mathbb{Z}_4^\times| = 2$ is prime, $Aut(\mathbb{Z}_4) \cong \mathbb{Z}_2 \cong \mathbb{Z}_4^\times$.

(ii) $Aut(\mathbb{Z}_8) \leq S_8$ (Here we are permuting $\overset{ord=1}{0}, \underset{ord=8}{1}, \overset{ord=4}{2}, \underset{ord=8}{3}, \overset{ord=2}{4}, \underset{ord=8}{5}, \overset{ord=4}{6}, \underset{ord=8}{7}$)

$$Aut(\mathbb{Z}_8) = \left\{ \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 5 & 2 & 7 & 4 & 1 & 6 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \right\}$$

As $|Aut(\mathbb{Z}_8)| = |\mathbb{Z}_2 \times \mathbb{Z}_2| = |\mathbb{Z}_8^\times| = 4$, and $Aut(\mathbb{Z}_8)$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8^\times$ are not cyclic, $Aut(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_8^\times$.

6\. Solution:

(a) Assume that $H \trianglelefteq G$ and $K \leq G$ and $H \subseteq K$, we prove that $H \trianglelefteq K$.

First, $H \subseteq K$;

Second, $H \trianglelefteq G$ implies H is closed under the multiplication in K.

Third, $H \trianglelefteq G$ implies H is closed under the inverse in K.

Fourth, $H \trianglelefteq G$ implies $gH = Hg$ forall $g \in K$

Hence, $H \trianglelefteq K$.

(b)(c) Consider $G = S_4$. Notice that $K = K_4 \trianglelefteq G = S_4$ (Done in Assignment 2, 5(c)),

and $H = \{e, (1,2)(3,4)\} \trianglelefteq K = K_4$ (As $|H| = 2 = \frac{1}{2}|K|$),

but $(1,3)\{e, (1,2)(3,4)\} = \{(1,3), (1,2,3,4)\} \neq \{(1,3), (4,3,2,1)\} = \{e, (1,2)(3,4)\}(1,3)$

so $H = \{e, (1,2)(3,4)\} \ntrianglelefteq G = S_4$