20240924 MATH3301 Assignment 2 Part 2:

1.(a) Solution:

If G is the general linear group $GL_2(\mathbb{R})$,

H is the special linear group $SL_2(\mathbb{R})=\{A\in GL_2(\mathbb{R}): \det(A)=1\}$,

$x=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\in GL_2(\mathbb{R})$ and $h=\begin{pmatrix}1&1\\0&1\end{pmatrix}\in SL_2(\mathbb{R})$,

then $xhx^{-1}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}^{-1}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}$

$=\begin{pmatrix}0&-1\\1&1\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}1&0\\-1&1\end{pmatrix}\neq\begin{pmatrix}1&1\\0&1\end{pmatrix}=h$

and $\forall x'\in GL_2(\mathbb{R}), \forall h\in GL_2(\mathbb{R})$:

$h\in x'Hx'^{-1}\Rightarrow\exists h'\in H, h=x'h'x'^{-1}$

$\Rightarrow\det(x'h'x'^{-1})=\det(x')\det(h')\det(x'^{-1})=\det(x')1\det(x')^{-1}=1$

$\Rightarrow h=x'h'x'^{-1}\in H$

$h\in H\Rightarrow\det(h)=1\Rightarrow\det(x'^{-1}hx')=\det(x'^{-1})\det(h)\det(x')$

$=\det(x')^{-1}1\det(x')=1\Rightarrow x'^{-1}hx'\in H\Rightarrow h=x'(x'^{-1}hx')x'^{-1}\in x'Hx'^{-1}$

This implies $x'Hx'^{-1}=H$, so $H=SL_2(\mathbb{R})$ is normal in $G=GL_2(\mathbb{R})$.

(b) Proof: We may divide our proof into two parts.

Part 1: Assume that H is normal in G, i.e., $\forall x\in G, xHx^{-1}=H$.

For all $x\in G$, for all $h\in G$:

$h\in xH\Rightarrow\exists h'\in H, h=xh'\Rightarrow\exists xh'x^{-1}\in xHx^{-1}=H, h=(xh'x^{-1})x$

$\Rightarrow h\in Hx$

$h\in Hx\Rightarrow\exists h'\in H, h=h'x\Rightarrow\exists x^{-1}h'(x^{-1})^{-1}\in x^{-1}H(x^{-1})^{-1}=H, h=x[x^{-1}h'(x^{-1})^{-1}]$

$\Rightarrow h\in xH$.

Hence, $xH=Hx$.

Part 2: Assume that $\forall x \in G, xH = Hx$.

For all $x \in G$, for all $h \in G$:

$$\left.\begin{array}{l} h \in xHx^{-1} \Rightarrow \exists h' \in H, h = xh'x^{-1} \\ xH = Hx \Rightarrow \exists h'' \in H, xh' = h''x \end{array}\right\} \Rightarrow h = xh'x^{-1} = h''xx^{-1} = h''e = h'' \in H$$

$$h \in H \Rightarrow x^{-1}h \in x^{-1}H = Hx^{-1} \Rightarrow \exists h' \in H, x^{-1}h = h'x^{-1} \Rightarrow h = xh'x^{-1} \in xHx^{-1}$$

Hence, $xHx^{-1} = H$, so H is normal in G.

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

(c) Proof: Assume that $H \leq G$ and $\forall x \in G, xHx^{-1} \subseteq H$.

For all $x \in G$, as $xHx^{-1} \subseteq H$ is provided, it remains to show $xHx^{-1} \supseteq H$.

For all $h \in G$,

$$h \in H \Rightarrow x^{-1}h(x^{-1})^{-1} \in x^{-1}H(x^{-1})^{-1} \subseteq H \Rightarrow x^{-1}h(x^{-1})^{-1} \in H$$

$$\Rightarrow h = x[x^{-1}h(x^{-1})^{-1}]x^{-1} \in xHx^{-1}$$

Hence, $xHx^{-1} = H$, so H is normal in G.

(d) Proof: Assume that $H \leq G$ and $[G:H] = 2$.

On one hand, $[G:H]=2$ implies $\{eH, x_1H\}$ partitions G for some $x_1 \in G \setminus H$;

On the other hand, $[G:H]=2$ implies $\{He, Hx_2\}$ partitions G for some $x_2 \in G \setminus H$;

For all $x \in G$:

If $x \in H$, then $xH = H = Hx$;

If $x \in G \setminus H$, then $xH = G \setminus H = Hx$.

In both cases, $xH = Hx$, so H is a normal subgroup of G.

(e) Proof: In Tutorial 4, we've proven that:

$$\phi \in Hom(G,G') \text{ and } H' \leq G' \Rightarrow \phi^{-1}(H') \leq G$$

It remains to prove $\phi^{-1}(H')$ is normal in G, i.e., $\forall x \in G, x\phi^{-1}(H')x^{-1} \subseteq \phi^{-1}(H')$.

For all $x \in G$, for all $h \in G$:

$$h \in x\phi^{-1}(H')x^{-1} \Rightarrow \exists h' \in \phi^{-1}(H'), h = xh'x^{-1}$$

$$\Rightarrow \phi(h) = \phi(xh'x^{-1}) = \phi(x)\phi(h')\phi(x^{-1}) = \overset{\substack{G'\\ \Downarrow}}{\phi(x)}\overset{\substack{H'\\ \Downarrow}}{\phi(h')}\overset{\substack{G'\\ \Downarrow}}{\phi(x)}^{-1} \in H'$$

$$\Rightarrow h \in \phi^{-1}(H')$$

Hence, $x\phi^{-1}(H')x^{-1} \subseteq \phi^{-1}(H')$, which implies $\phi^{-1}(H')$ is normal in G.

(f) Proof: In Tutorial 4, we've proven that:

$$\phi \in Hom(G,G') \text{ and } H \leq G \Rightarrow \phi(H) \leq G' \text{ (we can do better, } \leq \phi(G))$$

It remains to prove $\phi(H)$ is normal in $\phi(G)$, i.e., $\forall x' \in \phi(G), x'\phi(H)x'^{-1} \subseteq \phi(H)$.

For all $x' \in \phi(G)$, for all $h' \in x'\phi(H)x'^{-1}$:

$$\left.\begin{array}{l} x' \in \phi(G) \Rightarrow \exists x \in G, x' = \phi(x) \\ h' \in x'\phi(H)x'^{-1} \Rightarrow \exists h \in H, h' = x'\phi(h)x'^{-1} \end{array}\right\}$$

$$\Rightarrow h' = x'\phi(h)x'^{-1} = \phi(x)\phi(h)\phi(x)^{-1} = \phi(x)\phi(h)\phi(x^{-1})$$

$$= \phi(x\underset{\substack{\cap\\ xHx^{-1}\\ \cap\\ H}}{h}x^{-1}) \in \phi(H)$$

Hence, $x'\phi(H)x'^{-1} \subseteq \phi(H)$, which implies $\phi(H)$ is normal in $\phi(G)$.

2. Solution: $|S_3|=6$, and we may list all its elements with corresponding orders.

$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $ord(e)=1$; $r=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $ord(r)=3$; $r^2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $ord(r^2)=3$;

$\sigma=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $ord(\sigma)=2$; $r\sigma=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $ord(r\sigma)=2$; $r^2\sigma=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $ord(r^2\sigma)=2$;

As all isomorphism $\phi: S_3\to S_3$ preserves the order of each element in S_3, we may pick $\phi(r)$ from $\{r, r^2\}$ and pick $\phi(\sigma)$ from $\{\sigma, r\sigma, r^2\sigma\}$ to construct ϕ.

Case 1: $\phi(r)=r$ and $\phi(\sigma)=\sigma$.

$\phi(e)=e$, $\phi(r)=r$, $\phi(r^2)=\phi(r)^2=r^2$, $\phi(\sigma)=\sigma$, $\phi(r\sigma)=\phi(r)\phi(\sigma)=r\sigma$, $\phi(r^2\sigma)=\phi(r)^2\phi(\sigma)=r^2\sigma$;

This gives a unique isomorphism $\phi_e: S_3\to S_3$, $x\mapsto exe^{-1}$;

Case 2: $\phi(r)=r^2$ and $\phi(\sigma)=\sigma$.

$\phi(e)=e$, $\phi(r)=r^2$, $\phi(r^2)=\phi(r)^2=r^4=r$, $\phi(\sigma)=\sigma$, $\phi(r\sigma)=\phi(r)\phi(\sigma)=r^2\sigma$, $\phi(r^2\sigma)=\phi(r)^2\phi(\sigma)=r^4\sigma=r\sigma$

This gives a unique isomorphism $\phi_\sigma: S_3\to S_3$, $x\mapsto \sigma x\sigma^{-1}$;

Case 3: $\phi(r)=r$ and $\phi(\sigma)=r\sigma$.

$\phi(e)=e$, $\phi(r)=r$, $\phi(r^2)=\phi(r)^2=r^2$, $\phi(\sigma)=r\sigma$, $\phi(r\sigma)=\phi(r)\phi(\sigma)=r^2\sigma$, $\phi(r^2\sigma)=\phi(r)^2\phi(\sigma)=r^3\sigma=\sigma$

This gives a unique isomorphism $\phi_{r^2}: S_3\to S_3$, $x\mapsto r^2x(r^2)^{-1}$;

Case 4: $\phi(r)=r^2$ and $\phi(\sigma)=r\sigma$

$\phi(e)=e$, $\phi(r)=r^2$, $\phi(r^2)=\phi(r)^2=r^4=r$, $\phi(\sigma)=r\sigma$, $\phi(r\sigma)=\phi(r)\phi(\sigma)=r^3\sigma=\sigma$, $\phi(r^2\sigma)=\phi(r)^2\phi(\sigma)=r^5\sigma=r^2\sigma$

This gives a unique isomorphism $\phi_{r\sigma}: S_3\to S_3$, $x\mapsto r^2\sigma x(r^2\sigma)^{-1}$;

Case 5: $\phi(r)=r$ and $\phi(\sigma)=r^2\sigma$

$\phi(e)=e$, $\phi(r)=r$, $\phi(r^2)=\phi(r)^2=r^2$, $\phi(\sigma)=r^2\sigma$, $\phi(r\sigma)=\phi(r)\phi(\sigma)=r^3\sigma=\sigma$, $\phi(r^2\sigma)=\phi(r)^2\phi(\sigma)=r^4\sigma=r\sigma$

This gives a unique isomorphism $\phi_r: S_3\to S_3$, $x\mapsto rxr^{-1}$;

Case 6: $\phi(r)=r^2$ and $\phi(\sigma)=r^2\sigma$

$\phi(e)=e$, $\phi(r)=r^2$, $\phi(r^2)=\phi(r)^2=r^4=r$, $\phi(\sigma)=r^2\sigma$, $\phi(r\sigma)=\phi(r)\phi(\sigma)=r^4\sigma=r\sigma$, $\phi(r^2\sigma)=\phi(r)^2\phi(\sigma)=r^6\sigma=\sigma$

This gives a unique isomorphism $\phi_{r\sigma}: S_3\to S_3$, $x\mapsto r\sigma x(r\sigma)^{-1}$;

Collect all isomorphisms above in the following set:

$$X = \mathrm{Aut}(S_3) = \{\phi_e, \phi_r, \phi_{r^2}, \phi_\sigma, \phi_{r\sigma}, \phi_{r^2\sigma}\}$$

If we equip this set with $\circ$, then $\forall x, y \in S_3$, $\phi_{xy} = \phi_x \phi_y$.

This implies the bijective function $\psi: S_3 \to \mathrm{Aut}(S_3)$, $\psi(x) = \phi_x$ is an isomorphism.

That is, $\mathrm{Aut}(S_3)$ is not only a group under multiplication, it is isomorphic to S_3.

3\. Proof: Without loss of generality, assume that $\alpha: \{1,\cdots,n\} \to \{1,\cdots,n\}$ $\alpha(m) = \begin{cases} m+1, & \text{if } 1 \le m < k; \\ 1, & \text{if } m = k; \\ m, & \text{if } k < m \le n; \end{cases}$

For all $\sigma \in S_n$, for all $1 \le m \le n$:

Case 1: If $1 \le m < k$, then $\sigma\alpha\sigma^{-1}(\sigma(m)) = \sigma\alpha(\sigma^{-1}\sigma(m)) = \sigma\alpha(m) = \sigma(m+1)$;

Case 2: If $m = k$, then $\sigma\alpha\sigma^{-1}(\sigma(k)) = \sigma\alpha(\sigma^{-1}\sigma(k)) = \sigma\alpha(k) = \sigma(1)$;

Case 3: If $k < m \le n$, then $\sigma\alpha\sigma^{-1}(\sigma(k)) = \sigma\alpha(\sigma^{-1}\sigma(k)) = \sigma\alpha(k) = \sigma(k)$.

Combine the three cases above, we've proven that $\sigma\alpha\sigma^{-1} = (\sigma(1), \sigma(2), \cdots, \sigma(k))$.

4\. Proof: We may divide our proof into two parts:

"if" direction: Assume that $\sigma = (x_1, x_2, \cdots, x_k)$, $\tau = (y_1, y_2, \cdots, y_k)$ have the same length k.

Construct $\alpha \in S_n$, such that $\alpha(y) = \begin{cases} x_m, & \text{if } y = y_m \text{ for some } 1 \le m \le k; \\ \text{arbitrary}, & \text{if } y \ne y_m \text{ for all } 1 \le m \le k; \end{cases}$ and α is bijective.

Notice that $\sigma = \alpha\tau\alpha^{-1}$, so σ is conjugate to τ.

"only if" direction: Assume that σ is conjugate to τ, i.e., $\exists \alpha \in S_n$, $\sigma = \alpha\tau\alpha^{-1}$.

As $|S_n| < +\infty$, both $\mathrm{ord}\,\sigma$ and $\mathrm{ord}\,\tau$ exists.

For all $m \in \mathbb{Z}$, $\mathrm{ord}\,\sigma \mid m \Rightarrow \sigma^m = e \Rightarrow \tau^m = (\alpha^{-1}\sigma\alpha)^m = \alpha^{-1}\sigma^m\alpha = \alpha^{-1}e\alpha = e \Rightarrow \mathrm{ord}\,\tau \mid m$

$\mathrm{ord}\,\tau \mid m \Rightarrow \tau^m = e \Rightarrow \sigma^m = (\alpha\tau\alpha^{-1})^m = \alpha\tau^m\alpha^{-1} = \alpha e\alpha^{-1} = e \Rightarrow \mathrm{ord}\,\sigma \mid m$

Hence, the two positive integers $\mathrm{ord}\,\sigma$, $\mathrm{ord}\,\tau$ are equal, which implies σ, τ have the same length.

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

5. (a) (i) e 1

(ii) $(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)$ 6

(iii) $(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)$ 3

(iv) $(1,2,3),(3,2,1),(1,2,4),(4,2,1),(1,3,4),(4,3,1),(2,3,4),(4,3,2)$ 8

(v) $(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2)$ 6

We get $1+6+3+8+6=24=4!$ distinct elements in total.

(b) Proof: We may divide our proof into four parts.

Part 1: In this part, we prove that V contains the identity of S_4.

$$e\in V=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$$

Part 2: In this part, we prove that V is closed under the group operation of S_4

$x \circ y$	e	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
e	e	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
$(1,2)(3,4)$	$(1,2)(3,4)$	e	$(1,4)(2,3)$	$(1,3)(2,4)$
$(1,3)(2,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$	e	$(1,2)(3,4)$
$(1,4)(2,3)$	$(1,4)(2,3)$	$(1,3)(2,4)$	$(1,2)(3,4)$	e

Part 3: In this part, we prove that V is closed under the group inversion of S_4

$$e^{-1}=e\in V;\ [(1,3)(2,4)]^{-1}=(1,3)(2,4)\in V$$

$$[(1,2)(3,4)]^{-1}=(1,2)(3,4)\in V;\ [(1,4)(2,3)]^{-1}=(1,4)(2,3)\in V$$

Part 4: In this part, we prove that V is Abelian.

As its Cayley Table is symmetric about the main diagonal, V is Abelian.

Combine the four parts above, we've proven that V is an Abelian subgroup of S_4.

(c) Solution:

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

$(1,2)V=\{(1,2),(3,4),(1,3,2,4),(1,4,2,3)\}$

$(1,3)V=\{(1,3),(1,2,3,4),(2,4),(1,4,3,2)\}$

$(1,4)V=\{(1,4),(1,2,4,3),(1,3,4,2),(2,3)\}$

$(1,2,3)V=\{(1,2,3),(1,3,4),(4,3,2),(4,2,1)\}$

$(3,2,1)V=\{(3,2,1),(2,3,4),(1,2,4),(4,3,1)\}$

$Ve=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}=eV$

$V(1,2)=\{(1,2),(3,4),(1,4,2,3),(1,3,2,4)\}=(1,2)V$

$V(1,3)=\{(1,3),(1,4,3,2),(2,4),(1,2,3,4)\}=(1,3)V$

$V(1,4)=\{(1,4),(1,3,4,2),(1,2,4,3),(2,3)\}=(1,4)V$

$V(1,2,3)=\{(1,2,3),(4,3,2),(4,2,1),(1,3,4)\}=(1,2,3)V$

$V(3,2,1)=\{(3,2,1),(4,3,1),(2,3,4),(1,2,4)\}=(3,2,1)V$

As $\forall \alpha\in S_4$, $\alpha V=V\alpha$, V is an abelian normal subgroup of S_4.

Date / /