MATH 611 HW3 SOLUTIONS.

Sunday 10/20/19.

3. a. $\theta(AB) = ((AB)^{-1})^T = (B^{-1}A^{-1})^T = (A^{-1})^T \cdot (B^{-1})^T = \theta(A)\cdot\theta(B)$.

since $(XY)^T = Y^T X^T$.

θ is bijective : in fact $\theta^2 = id$:-

$$\theta(\theta(A)) = (((A^{-1})^T)^{-1})^T = (((A^{-1})^{-1})^T)^T = ((A)^T)^T = A.$$

since $(X^T)^{-1} = (X^{-1})^T$.

So θ is an automorphism. $\square$.

b. $\det BAB^{-1} = \det A$

$\det (A^{-1})^T = \det A^{-1} = (\det A)^{-1}$.

So $BAB^{-1} \neq (A^{-1})^T$ if $\det A \neq (\det A)^{-1}$, i.e., $\det A \neq \pm 1$. $\square$.

4. Recall $D_n \cong \langle a, b \mid a^n = b^2 = e,\ ba = a^{-1}b \rangle$. (†) a = rotation by $2\pi/n$ ccw (about centre of mass)
b = reflection in axis of symmetry

In particular, since D_n is generated by a & b, an automorphism $\theta: D_n \to D_n$ is determined by $\theta(a)$ & $\theta(b)$.

$D_n = \{ \underbrace{e, a, \ldots, a^{n-1}}_{\text{rotations}}, \underbrace{b, ab, \ldots, a^{n-1}b}_{\text{reflections, order 2.}} \}$

order of $a^i = n/\gcd(i,n)$

Thus $\theta(a) = a^c$, some $c \in \mathbb{Z}/n\mathbb{Z}$, $\gcd(c,n)=1$ (because $\theta(a)$ has the same order as a)

Also $\theta(b) = a^d \cdot b$, some $d \in \mathbb{Z}/n\mathbb{Z}$, ($\theta(b) \notin \langle a \rangle$ otherwise θ not surjective ※)

Conversely, given $c, d \in \mathbb{Z}/n\mathbb{Z}$, c s.t. $\gcd(c,n)=1$,

then $\theta(a) = a^c$ & $\theta(b) = a^d \cdot b$ defines an automorphism $\theta: D_n \xrightarrow{\sim} D_n$:-

First, to check θ defines a hom., sufficient to check that $\theta(a)$ & $\theta(b)$ satisfy the defining relations $(\dagger)$ of D_n, i.e. $(a^c)^n = e$, $(a^d b)^2 = e$, $(a^d b)\cdot a^c = a^{-c}\cdot(a^d b)$.

$$\therefore \quad (a^c)^n = a^{cn} = (a^n)^c = e. \checkmark$$

$$(a^d b)^2 = a^d b a^d b \underset{ba = a^{-1}b}{=} a^d \cdot a^{-d} \cdot b \cdot b = b^2 = e. \checkmark$$

$$(a^d b)\cdot a^c \underset{ba = a^{-1}b}{=} a^d \cdot a^{-c} \cdot b = a^{d-c}\cdot b.$$

$$a^{-c}\cdot(a^d b) = a^{d-c} b \quad \checkmark.$$

Second, given two such homs θ, θ' corresponding to (c,d), (c',d') compute composite $\theta'\circ\theta$:

$$\theta'\circ\theta(a) = \theta'(a^c) = (a^{c'})^c = a^{c'c}$$

$$\theta'\circ\theta(b) = \theta'(a^d b) = (a^{c'})^d \cdot (a^{d'} b) = a^{c'd+d'}\cdot b.$$

Compare w/ composition in the group G of $f(x) = cx+d$ & $f'(x) = c'x+d'$:

$$f'\circ f(x) = c'(cx+d) + d' = c'c\cdot x + (c'd+d').$$

Since G has inverses (G is a group), see θ is invertible

& $\quad \mathrm{Aut}\, D_n \longrightarrow G \quad$ is an isom. of groups $\square$

$$\begin{array}{ccc} \theta & \longmapsto & f(x) = cx+d \\ \theta(a) = a^c & & \\ \theta(b) = a^d . b. & & \end{array}$$

5a. $\quad H = \langle (12\cdots p) \rangle \leq S_p.$

a) $gHg^{-1} = \langle (g(1)\, g(2) \cdots g(p)) \rangle \leq S_p.$

Each conjugate subgroup contains $(p-1)$ p-cycles, any of which generates the subgroup.

$$\therefore \# \text{ conj. subgps} = \frac{\#\ p\text{-cycles}}{p-1} = \frac{p!/p}{(p-1)} = (p-2)!$$

Now, by OST, $p! = |S_p| = (p-2)! \cdot |N(H)| \Rightarrow |N(H)| = p \cdot (p-1)$. $\square$.

b) $$\varphi : N(H) \longrightarrow \mathrm{Aut}(H)$$
$$g \longmapsto (h \mapsto ghg^{-1})$$

$$\mathrm{Aut}(H) \simeq \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^* \left(\simeq \mathbb{Z}/(p-1)\mathbb{Z}.\right)$$

$\Rightarrow |\mathrm{Aut}(H)| = p-1.$

$$\ker \varphi = \{ g \in S_p \mid \underset{\substack{\shortparallel \\ (g(1)g(2)\cdots g(p))}}{g(12\cdots p)g^{-1}} = (12\cdots p) \} = \langle (12\cdots p) \rangle = H.$$

So $N(H)/H \xrightarrow[\text{1.I.T.}]{\simeq} \varphi(N(H))$, $|\varphi(N(H))| = \dfrac{p \cdot (p-1)}{p} = p-1 = |\mathrm{Aut}\ H|$

$\Rightarrow \varphi$ surj.

c). Let $\theta \in \mathrm{Aut}\,H$ be a generator. (recall $\mathrm{Aut}\,H \simeq \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic)

Let $\sigma \in N(H)$ be a lift of θ under φ (i.e. $\varphi(\sigma) = \theta$).

Then $N(H) \simeq \langle (12\cdots p), \sigma \rangle$

$(\tau \in N(H) \Rightarrow \varphi(\tau) = \theta^k = \varphi(\sigma^k) \Rightarrow \tau\sigma^{-k} \in \ker\varphi = H = \langle (12\cdots p) \rangle$
$\Rightarrow \tau \in \langle (12\cdots p), \sigma \rangle$. $\square$).

If $p=5$, $(\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/4\mathbb{Z}$
$$2 \leftarrow\!\shortmid\ 1$$

So, want σ s.t. $$\underset{\substack{\shortparallel \\ (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))}}{\sigma(12\cdots 5)\sigma^{-1}} = (12\cdots 5)^2 = (13524)$$

e.g. $\sigma(1)=1$, $\sigma(2)=3$, $\sigma(3)=5$, $\sigma(4)=2$, $\sigma(5)=4$, i.e. $\sigma = (2354)$.

$N(H) = \langle (12\cdots 5), (2354) \rangle$. $\square$.

6. $H \trianglelefteq G \Rightarrow \varphi : G \longrightarrow \operatorname{Aut} H$ hom.

$$g \longmapsto (h \mapsto ghg^{-1})$$

$|H| = p \Rightarrow H \simeq \mathbb{Z}/p\mathbb{Z} \Rightarrow \operatorname{Aut} H \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$

p the smallest prime dividing $|G|$ $\Rightarrow \gcd(|G|, |\operatorname{Aut} H|) = 1$

$\Rightarrow \varphi(G) = \{e\} = \{id_H\}$

$\Rightarrow ghg^{-1} = h \ \forall\, g \in G, h \in H$, equiv $gh = hg \ \forall\, g \in G, h \in H$.

$\Rightarrow H \leq Z(G)$. $\square$.

7. Let $H = SL_n(F) = \ker(\det : GL_n(F) \longrightarrow F^*)$.

$K = Z(GL_n(F)) = \{\lambda \cdot I \mid \lambda \in F^*\} \simeq F^*$.

Note $\det : K \longrightarrow F^*$ is identified with $\theta : F^* \longrightarrow F^*$, $\lambda \longmapsto \lambda^n$, i.e., $\det(\lambda I) = \lambda^n$.

Now, $H \trianglelefteq GL_n(F)$ (H is a kernel)

$K \trianglelefteq GL_n(F)$ (K is the center)

$H \cap K = \{e\} \iff \theta$ is injective

$HK = GL_n(F) \iff \theta$ is surjective.

& recall criterion:
$H, K \trianglelefteq G$, $H \cap K = \{e\}$, $HK = G$
$\Rightarrow H \times K \xrightarrow{\sim} G$
$(h, k) \longmapsto hk$.

(If $g = h \cdot k$, $h \in H, k \in K$, ~~$\theta(g)$~~ $\det g = \det h \cdot \det k = 1 \cdot \theta(\lambda)$, where $k = \lambda \cdot I$.

Now $\det : GL_n(F) \to F^*$ is surj. (e.g. $\begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \mapsto \lambda$), so $G = HK \Rightarrow \theta$ surj.

Conversely, if θ is surj, given $g \in G$ let $\det(g) = \theta(\lambda)$, then

$g = h \cdot (\lambda \cdot I)$, where $h = g \cdot (\lambda \cdot I)^{-1} \in SL_n(F)$. So $G = HK$).

Now, for $F = \mathbb{R}$, θ is bijective $\iff n$ odd.

For $F = \mathbb{Z}/p\mathbb{Z}$, $F^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, so θ bij. $\iff \gcd(n, p-1) = 1$. $\square$.

8a. $|D_{60}| = 2\cdot 60 = 2^3\cdot 3\cdot 5$

$\exists\ H \leq D_{60}$, $|H| = 2^3 = 8$, $H \simeq D_4$ obtained by inscribing a square in the regular 60-gon (w/ vertices 15, 30, 45, 60 in cyclic order)

$\#$ Sylow 2-subgroups of $D_{60} \underset{S.T.2}{=} \#$ conjugates of H $=$ $\#$ inscribed squares

$= 15$ (inscribed square has vertices $i+15j$, $j = 0,1,2,3$, some fixed i, $0 \leq i < 15$.)

b. $|S_6| = 720 = 2^4\cdot 3^2\cdot 5$

$\exists\ H = \langle (123), (456) \rangle \leq S_6$, $|H| = 3^2 = 9$.

$\#$ Sylow 3-subgps of S_6 $=$ $\#$ conjugates of H $= \dfrac{\binom{6}{3}\cdot\binom{3}{3}}{2} = 10.$

c. $|GL_3(\mathbb{Z}/5\mathbb{Z})| = (5^3-1)\cdot(5^3-5)\cdot(5^3-5^2) = 5^3\cdot(5^3-1)(5^2-1)(5-1)$

$\exists\ H \leq GL_3(\mathbb{Z}/5\mathbb{Z})$, $H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle|\ a,b,c \in \mathbb{Z}/5\mathbb{Z} \right\}$, $|H| = 5^3$.

$\#$ Sylow 5-subgps of $GL_3(\mathbb{Z}/5\mathbb{Z})$ $=$ $\#$ conjugates of H

$\underset{OST}{=} |GL_3(\mathbb{Z}/5\mathbb{Z})| \big/ |N(H)| = \dfrac{124}{4}\cdot\dfrac{24}{4}\cdot\dfrac{4}{4} = 31\cdot 6 = 186.$ $\square$.

(recall $|N(H)| = |B| = 5^3\cdot 4^3$

$N(H) = B = \left\{ \begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix} \middle|\ \begin{matrix} a,b,c \in \mathbb{Z}/5\mathbb{Z} \\ d_1,d_2,d_3 \in (\mathbb{Z}/5\mathbb{Z})^\times \end{matrix} \right\}$)

9. $|G| = 50. = 2\cdot 5^2$

$s :=$ $\#$ Sylow 5-subgroups; $s \equiv 1 \bmod 5$, $s \mid 2$ $\Rightarrow$ $s = 1$.

All elements of order 5 are contained in a Sylow 5-subgp. (by S.T.2)

$H \leq G$, $|H| = 5^2 = 25$ $\Rightarrow$ $H \simeq \mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$\Rightarrow$ $\#$ elements of order 5 $= 4$ or 24.

Both cases occur (e.g. can take G abelian, $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$.) $\square$.

10. $K := \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\} \leq G$ is a Sylow p-subgroup of $G = GL_n(\mathbb{Z}/p\mathbb{Z})$:-

upper triangular matrices w/ 1's on the diagonal

$$|G| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$$

$$= p^{0+1+\cdots+(n-1)} \cdot m, \quad p \nmid m$$

$$= p^{\frac{1}{2}(n-1)n} \cdot m$$

$$|K| = p^{1/2(n-1)n}.$$

Now by S.T.2, given $H \leq G$, $|H| = p^k$,

$\exists\ g \in G$ s.t. $gHg^{-1} \leq K$. $\square$.

11. $|G| = 57 = 3 \cdot 19 = p \cdot q$ $\quad q = 19 \equiv 1 \bmod (p=3)$

So, $\exists!$ isomorphism type of non abelian group G : $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$.

$$\psi(1) = (x \mapsto lx) \in \mathrm{Aut}\,\mathbb{Z}/q\mathbb{Z},$$

where $l \in (\mathbb{Z}/q\mathbb{Z})^*$ has order p.

Our case : $2^{18} \equiv 1 \bmod 19$.

$(2^6)^3 \equiv 1 \bmod 19$.

$2^6 = 64 \equiv 7 \bmod 19$, $\not\equiv 1 \bmod 19$.

So $l = 7 \in (\mathbb{Z}/19\mathbb{Z})^*$ has order 3.

In terms of generators & relations, $G \cong \langle a, b \mid a^q = b^p = e,\ bab^{-1} = a^l \rangle$. $\square$.