611 HW3 Solutions.

1. Recall the class equation of S_4 (HW2Q2)

$$\begin{array}{ccccccccccc} 24 & = & 1 & + & 6 & + & 8 & + & 6 & + & 3 \quad \dagger \\ & & e & & (12) & & (123) & & (1234) & & (12)(34) \end{array}$$

A normal subgroup H of a group G is a union of conjugacy classes, & $|H| \mid |G|$ (Lagrange's theorem). Also $e \in H$ of course.

So, for $H \lhd S_4$, $|H|$ must be a sum of terms from RHS of class equation $\dagger$, including 1, which divides $|G| = 24$.

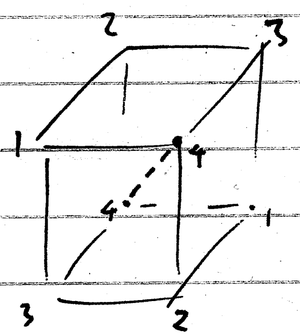
Cases: $4 = 1+3 \Rightarrow H = \{e, (12)(34), (13)(24), (14)(23)\}$

$12 = 1+8+3 \Rightarrow H = A_4$

NB. Check H is a subgroup!

(and trivial cases $H = \{e\}$, $H = S_4$)

2.



$$H = \langle (123) \rangle \leq S_4$$

$$N(H) = S_3 \leq S_4$$

$$= \langle (123), (12) \rangle$$

$$\cong D_3$$

Realizing S_4 as group of rotations of cube (label pairs of opposite vertices 1,2,3,4), H is identified with the subgroup of rotations about the axis L joining the vertices labelled 4,

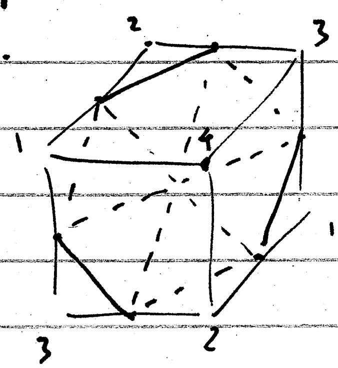
& $N(H)$ is the subgroup of rotations preserving this axis

– these are the rotations w/ axis L (the elements of H)

& the rotations about axes M orthogonal to L through angle π

In fact, if we slice the cube by the plane through its center of

mass with normal direction L, we get a regular hexagon, and the possible axes M are the diagonals of this hexagon.
Finally, inscribing an equilateral triangle in this hexagon, $N(H)$ is identified with the dihedral group of isometries of this triangle.



3. If h is a rotation about a point $p \in \mathbb{R}^2$ through angle θ ccw, then ghg^{-1} for g an isometry of $\mathbb{R}^2$ is a rotation about $g(p) \in \mathbb{R}^2$ through angle $\pm\theta$ ccw, where the sign is +/- if g is orientation preserving / reversing.

It follows that $N(H) = \{g \in G \mid g(0) = 0\}$.

$\cong O(2)$ the group of all orthogonal 2×2 matrices

(and $H \triangleleft N(H)$ corresponds to $SO(2)$, the orthogonal matrices of determinant 1).
$N(H)$ consists of rotations about 0 (the elements of H) & reflections in lines thru 0.
If $g \in N(H)$ is a rotation, $ghg^{-1} = h \quad \forall h \in H$ (H is abelian!)
If $g \in N(H)$ is a reflection, $ghg^{-1} = h^{-1} \quad \forall h \in H$.

(this can be checked by choosing coordinates such that the reflection is in the x-axis, & computing explicitly with 2x2 matrices, compare HW1 Q7a.)

4\. a. $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix} \quad \dagger$

So, these two matrices commute iff $az = xc$.

$\therefore \; Z(G) = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{Z}/p\mathbb{Z} \right\}$

b. Define a map

$$\varphi : G \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2$$

$$\varphi \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = (a, c)$$

This is a group hom. by $\dagger$

$\ker \varphi = Z(G)$, φ surjective $\Rightarrow$ $\bar{\varphi} : G/Z(G) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^2$

(First isom. thm.)

5\. a. We have $(AB)^T = B^T A^T$

& $(AB)^{-1} = B^{-1} A^{-1}$

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

Thus θ is an automorphism (note θ is clearly bijective).

b. Using the hint, if $A = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ is diagonal,

$\theta(A) = \begin{pmatrix} \lambda_1^{-1} & & 0 \\ & \ddots & \\ 0 & & \lambda_n^{-1} \end{pmatrix}$, trace $\theta(A) = \lambda_1^{-1} + \dots + \lambda_n^{-1} \neq \lambda_1 + \dots + \lambda_n = \text{trace } A$

for general $\lambda_1, \dots, \lambda_n \in \mathbb{R}^\times$. So $\theta(A) \neq BAB^{-1}$ for any $B \in GL_n(\mathbb{R})$.

6\. $H = \langle (1 2 3 \cdots p) \rangle \leq S_p$, p prime.

a. $\#$ p-cycles $= \dfrac{p\cdot(p-1)\cdots 2\cdot 1}{p} = (p-1)!$

$\therefore$ $\#$ conjugate subgroups of $H = \dfrac{(p-1)!}{p-1} = (p-2)!$

(each containing $(p-1)$ p-cycles, which are generators of the group)

$\therefore$ $|N(H)| = |G| \Big/ \#\text{ conj. subgroups} = |S_p| \Big/ (p-2)! = p\cdot(p-1)$

b. $g(12\cdots p)g^{-1} = (g(1)g(2)\cdots g(p))$

Thus $g \in G = S_p$ commutes w/ every element of H

iff $(g(1)g(2)\cdots g(p)) = (12\cdots p)$,

$\iff$ $g(1), g(2), \ldots, g(p)$ is a cyclic permutation of $1, 2, \ldots, p$,

i.e. $g \in H$.

So $\ker\varphi = H$.

Now since $|N(H)| = p(p-1)$ & $|H| = p$

we have $|\varphi(H)| = p-1 \overset{\dagger}{=} |\mathrm{Aut}(H)|$, so φ is surjective.

($\dagger$: Note $H \simeq \mathbb{Z}/p\mathbb{Z} \Rightarrow \mathrm{Aut}\,H \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, $|\mathrm{Aut}\,H| = p-1$)

c $\mathrm{Aut}\,H \simeq \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq (\mathbb{Z}/(p-1)\mathbb{Z})$

Thm. stated in class.

and $\varphi: N(H) \to \mathrm{Aut}(H)$ is surjective by b.

Let $a \in H$ be a generator of H (e.g. $a = (12\cdots p)$)

and $b \in N(H)$ an element mapping to a generator g of

$\mathrm{Aut}(H) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ under φ.

Then $N(H) = \langle a, b\rangle$

(Proof: if $x \in N(H)$, write $\varphi(x) = g^i$ then $xb^{-i} \in \ker\varphi$

so $xb^{-i} = a^j$, $x = a^j b^i$

Explicitly for $p=5$.

$(\mathbb{Z}/5\mathbb{Z})^\times$ is generated by 2 $(2, 2^2=4, 2^3=3, 2^4=1)$

So $g: H \to H$, $g(12345) = (12345)^2 = (13524)$

is a generator of $\mathrm{Aut}(H)$.

Then $g = \varphi(\sigma)$ where $(\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5)) = (13524)$,

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

i.e. $\sigma = (2354)$.

(Note that $\sigma \in N(H)$ because $H = \langle(12345)\rangle$

& $\sigma(12345)\sigma^{-1} = (13524) \in H$ by construction,

so $\sigma H \sigma^{-1} \subset H$, $\sigma H \sigma^{-1} = H$).

So $N(H) = \langle (12345), (2354) \rangle$

7. Let $a \in G$ be an element s.t. $\bar{a} \in G/Z(G)$

is a generator of the cyclic group $G/Z(G)$

(Here I am writing $\bar{a}$ for the image $q(a)$ of a under

the quotient hom $G \to G/Z(G)$)

Now, given $x, y \in G$, write $\bar{x} = \bar{a}^n$, $\bar{y} = \bar{a}^m$, $n, m \in \mathbb{Z}$,

then $x = a^n \cdot z_1$, $y = a^m \cdot z_2$, where $z_1, z_2 \in Z(G)$.

Now compute $x \cdot y = a^n \cdot z_1 \cdot a^m \cdot z_2 \overset{z_1 \in Z(G)}{=} a^n \cdot a^m \cdot z_1 \cdot z_2$

$= a^{n+m} \cdot z_1 \cdot z_2$

$y \cdot x = a^m \cdot z_2 \cdot a^n \cdot z_1 = a^m \cdot a^n \cdot z_2 \cdot z_1 = a^{n+m} z_1 \cdot z_2$

$z_2 \in Z(G)$

So G is abelian.

8. a Recall the counting formula.

$|G| = |N(H)| \cdot \#$ conjugate subgroups.

So $\left| \bigcup_{g \in G} gHg^{-1} \right| \leq |G| / |N(H)| \cdot (|H|-1) + 1$

(Here use each conjugate subgroup contains $e \in G$)

$\leq |G| / |H| \cdot (|H|-1) + 1$

$< |G|$

$\therefore \bigcup_{g \in G} gHg^{-1} \neq G$.

b Pick $x \in G \setminus \bigcup_{g \in G} gHg^{-1}$

Then $C(x) \cap H = \emptyset$.

$(gxg^{-1} \in H \iff x \in g^{-1}Hg$ $\#$ $)$

9. Consider the hom $\varphi : G \longrightarrow Aut(H)$

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

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

$\implies \gcd(|G|, |Aut(H)|) = 1$

$\implies \varphi$ is trivial hom, i.e. $\varphi(g) = e \in Aut(H)$ $\forall g \in G$

i.e. $ghg^{-1} = h$ $\forall$ $g \in G, h \in H$

So $H \leq Z(G)$.

10. $|G| = p^n$, $H \underset{\neq}{<} G$. Claim $H \underset{\neq}{\leq} N(H)$

Proof: By (strong) induction on n.

$n=1$: G abelian ($G \cong \mathbb{Z}/p\mathbb{Z}$) $\Rightarrow N(H) = G \Rightarrow$ ✓.

True for $m < n \Rightarrow$ true for n:

Recall $|G| = p^n \Rightarrow Z(G) \neq \{e\}$.

If $Z(G) \not\leq H$ then $H \lneq N(H)$

(because $Z(G) \leq N(H)$).

Otherwise, consider $\overline{H} = H/Z(G) \lneq \overline{G} = G/Z(G)$

$|\overline{G}| = p^m$, $m < n$.

Now by inductive hypothesis $\overline{H} \lneq N(\overline{H})$.

But it's easy to see that $N(\overline{H}) = N(H)/Z(G)$

So we get $H \lneq N(H)$ | i.e. $\overline{g}\,\overline{H}\,\overline{g}^{-1} = \overline{H} \iff gHg^{-1} = H$

This completes the proof by induction. $\square$