Homework 2

Jaden Wang

Problem (1)**.** Since $G/Z(G)$ is cyclic, let $aZ(G)$ be its generator. Given $g, h \in G$, we know that $g = a^i x$ and $h = z^j y$ for some $i, j \in \mathbb{N}$ and $x, y \in Z(G)$. Hence,

$$gh = a^i x a^j y = a^i a^j xy = a^{i+j} yx = a^j y a^i x = hg.$$

Problem (2)**.**

(a) Define the set map $\phi_g : G/H \to G/H, g'H \mapsto gg'H$. We wish to show that $\Phi : G \to \mathrm{Aut}_{|G/H|} \cong S_{|G/H|}, g \mapsto \phi_g$ is a group homomorphism.

$$\begin{aligned}
\Phi(g_1 g_2)(g'H) &= \phi_{g_1 g_2}(g'H) \\
&= g_1 g_2 g' H \\
&= \phi_{g_1}(g_2 g' H) \\
&= \phi_{g_1} \phi_{g_2}(g'H) \\
&= \Phi(g_1)\Phi(g_2)(g'H)
\end{aligned}$$

Hence $\Phi(g_1 g_2) = \Phi(g_1)\Phi(g_2)$.

(b) Given $g_1 H$ and $g_2 H$, we see that $g_2 H = g_2 g_1^{-1} g_1 H = \Phi(g_2 g_1^{-1})(g_1 H)$ so the action is transitive. Moreover, $\mathrm{Stab}_G(H) = \{g \in G : gH = H\} = \{g \in H\} = H$.

(c) Clearly $K = \bigcap_{g' \in G} \mathrm{Stab}_G(g'H) \subseteq \mathrm{Stab}_G(H) = H$. Since $K = \ker \Phi$, it is a normal subgroup of G.

(d) Consider the cosets G/H which has order 4. Then the kernel K of the action $\Phi : G \to S_4$ is the largest normal subgroup contained in H by part c. Since $K \trianglelefteq H$, by order consideration $|K| = 1, 5, 7$ or 35 so $|G/K| = 140, 28, 20$ or 4. Since $\operatorname{im} \Phi \leq S_4$, $|\operatorname{im} \Phi| | 24$ so it is $1, 2, 3, 4, 6, 12$ or 24. By the first isomorphism theorem, $|G/K| = \operatorname{im} \Phi$ so they must equal 4. But this implies that $|K| = |H|$ so $K = H$. It follows that $H \trianglelefteq G$.

Problem (3)**.**

(a) Given $a, b \in A$, since the action is transitive, there exists a $g \in G$ s.t. $b = g.a$. I claim that $H_b = gH_ag^{-1}$. Given $h \in H_b$, then

$$\begin{aligned} h.b &= b \\ h.(g.a) &= g.a \\ (g^{-1}hg).a &= a \end{aligned}$$

Since $H \trianglelefteq G$, $g^{-1}hg \in H$. So $g^{-1}hg \in H_a$ and $h = gg^{-1}hgg^{-1}$. Given $gh'g^{-1} \in gH_ag^{-1}$, we know since H is normal, $gh'g^{-1} \in H$.

$$\begin{aligned} h'.a &= a \\ (g^{-1}gh'g^{-1}g).a &= a \\ (gh'g^{-1}).(g.a) &= g.a \\ (gh'g^{-1}).b &= b \end{aligned}$$

So $gh'g^{-1} \in H_b$ and the equality follows. Since action of g by conjugation on G is an automorphism of G, the action restricted to H_a is still a bijection so $|H_b| = |gH_ag^{-1}|$. Since a, b are arbitrary, we show that all stablizers of element in A have the same cardinality. By the Orbit-Stablizer Theorem, the orbits also have the same cardinality $|\mathcal{O}| = |H : H_a|$.

(b) It is easy to see that $H \cap G_a \subseteq H_a$. Given $h \in H_a$, clearly $h \in H$ and since $h.a = a$, $h \in G_a$. So $h \in H \cap G_a$ and therefore $H_a = H \cap G_a$. It follows that $|\mathcal{O}| = |H : H_a| = |H : H \cap G_a|$.

(c) Suppose the number of orbits of H on A is n. Since $|A|$ is finite, and the orbits partition A, n is finite and $|H : H \cap G_a|$ is finite. Thus $|HG_a : G_a| = |H : H \cap G_a|$ is also finite. But since $|HG_a| \leq |H||G_a|$ we have

$$\begin{aligned} n &= \frac{|A|}{|\mathcal{O}|} \\ &= \frac{|A|}{|H : H \cap G_a|} \\ &= \frac{|G.a|}{|H : H \cap G_a|} \\ &= \frac{|G : G_a|}{|H : H \cap G_a|} \end{aligned}$$

$$
\begin{aligned}
&= \frac{|G : G_a|}{|HG_a : G_a|} \\
&= |G : HG_a| && \text{4th iso for cosets}
\end{aligned}
$$

ALTER (using HW1.8 lemma):

$$
\begin{aligned}
\frac{|G : G_a|}{|H : H \cap G_a|} &= \frac{|G : HG_a||HG_a : G_a|}{|H : H \cap G_a|} \\
&= |G : HG_a| && \text{2nd iso}
\end{aligned}
$$

Problem (4)**.**

(a) We know that $\gcd(|N|, |G : N|) = 1$. Now suppose there exists a $H \leq G$ s.t. $|H| = |N|$. Since $N \trianglelefteq G$, $HN \leq G$.

$$
\begin{aligned}
|N| &= \frac{|G|}{|G : N|} \\
&= \frac{|G : HN||HN|}{|G : N|} \\
&= \frac{|G : HN||H||N|}{|G : N||H \cap N|} \\
&= \frac{|G : HN|}{|G : N|} \frac{|N|^2}{|H \cap N|}
\end{aligned}
$$

Since $|N|$ is an integer, all denominators in the expression must vanish. Since $|G : N|$ and $|N|$ are coprime, this implies that $|G : N| \mid |G : HN|$. But we also have $|G : N| = |G : HN||HN : N|$ so $|G : HN| \mid |G : N|$. Since these are positive integers, $|G : N| = |G : HN|$ which forces $HN = N$. It follows that $H \leq N$ and therefore $H = N$.

Alternatively (collab with Ari), we know that since $NH \leq G$, $|NH| \mid |G|$. Hence

$$
\begin{gathered}
\frac{|NH|}{|N|} \bigg| \frac{|G|}{|N|} \\
\frac{|H|}{|H \cap N|} \bigg| |G : N| \\
\frac{|N|}{|H \cap N|} \bigg| |G : N|
\end{gathered}
$$

Since $\frac{|N|}{|H \cap N|} = |N : H \cap N|$ also divides $|N|$ by Lagrange, $\frac{|N|}{|H \cap N|}$ divides $\gcd(|N|, |G : N|) = 1$. It must be that $\frac{|N|}{|H \cap N|} = 1$ so $|N| = |H \cap N|$ which implies $N = H \cap N$. Hence $H \leq N$ and thus $H = N$.

(b) We have $\gcd(|H|, |G : H|) = 1$ and $N \trianglelefteq G$. By the second isomorphism theorem, $|N : H \cap N| = |NH : H|$. Since $|G : H| = |G : NH||NH : H|$, and $|H \cap N|$ divides $|H|$ by Lagrange, $\gcd(|H \cap N|, |N : H \cap N|)$ must divide $\gcd(|H|, |G : H|) = 1$ which forces it to be 1 as well. Hence $H \cap N$ is a Hall subgroup of N.

By the third isomorphism theorem, $|G/N : NH/N| = |G : NH|$ which divides $|G : H|$. Also $|NH/N| = |NH : N|$. And again by the third isomorphism theorem, $|NH : N| = |H : H \cap N|$ which divides $|H|$. So again we have $\gcd(|NH/N|, |G : NH|)$ dividing $\gcd(|H|, |G : H|) = 1$ which yields that NH/N is a Hall subgroup of G/N.

Problem (5)**.**

(a) We know that S_n is generated by successively increasing transpositions (Exercise 3.5.3). So it suffices to show that $(1, 2)$ and $(1, 2, 3, \dots, n)$ generate all such transpositions. We know that conjugating $(1, 2)$ by $(1, 2, \dots, n)$ just becomes $(2, 3)$. Then conjugating $(2, 3)$ by $(1, 2, \dots, n)$ yields $(3, 4)$. Repeat until we get $(n - 1, n)$ and that's all the generators we need for S_n.

(b) It suffices to show that we can obtain $(1, 2)$ from any transposition (i, j) with $1 \leq i < j \leq p$ and $(1, 2, \dots, p)$. Since p is prime, powers ($< p$) of the p-cycle remains a p-cycle. Moreover, each power permutes the last letter in the cycle so we can always obtain some power (in fact, $(1 - i) \bmod p$) that looks like $(1, \dots, i)$. Conjugating (i, j) by this yields $(1, j)$. Moreover, $(1, 2, \dots, p)^{(2-j) \bmod p}$ should put 2 immediately after j. Conjugating $(1, j)$ by this yields $(1, 2)$.

(c) No. We see that in S_4, $(1, 4)$ cannot be generated by $(2, 4)$ and $(1, 2, 3, 4)$.

Problem (6)**.** Given $k \in K$, we know that $|K| = |S_n : \mathrm{Stab}_{S_n}(\{k\})|$ by Orbit-Stablizer Theorem. We also know from 3b that $\mathrm{Stab}_{A_n}(\{k\}) = H \cap \mathrm{Stab}_{S_n}(\{k\})$. Let the conjugacy class of k acted by A_n be K'. $|K'| = |A_n : \mathrm{Stab}_{A_n}(\{k\})| = |A_n : A_n \cap \mathrm{Stab}_{S_n}(\{k\})|$. Recall that $A_n \trianglelefteq S_n$ so $A_n \mathrm{Stab}_{S_n}(\{k\})$ is a subgroup of S_n containing A_n. Since A_n is maximal, $A_n \mathrm{Stab}_{S_n}(\{k\})$ either equals A_n or S_n. If it is A_n, then by the second isomorphism theorem, $|K'| = |A_n : A_n \cap \mathrm{Stab}_{S_n}(\{k\})| = |A_n \mathrm{Stab}_{S_n}(\{k\}) : \mathrm{Stab}_{S_n}(\{k\})| = |S_n : \mathrm{Stab}_{S_n}(\{k\})|/|S_n : A_n| = |K|/2$. Since k is arbitrary, picking another element not in K' yields another orbit of size $|K|/2$ and that is all of K. So we have two orbits of equal size in this case. If $A_n \operatorname{Stab}_{S_n}(\{k\}) = S_n$, then following the computation above, we obtain that $|K'| = |K|$ so there is only one orbit.

Problem (7)**.** Every group has the identity conjugacy class $\{e\}$. Let g be the representative of the other conjugacy class. By the class equation, $|G| = 1 + |G : C_G(g)|$. Since $|G : C_G(g)|$ divides $|G|$, we have that $n(|G| - 1) = |G|$ for some $n \in \mathbb{N}$. That is,

$$\begin{aligned} n|G| - n &= |G| \\ (n-1)|G| &= n \\ |G| &= \frac{n}{n-1} = 1 + \frac{1}{n-1} \end{aligned}$$

Since $|G| \in \mathbb{N}$, it's easy to see that $n = 2$ is the unique solution. Therefore, $|G| = 2$ so $G \cong \mathbb{Z}_2$.

Problem (8)**.** Let $S = \{(a_1, \ldots, a_p) : a_i \in G, a_1 \cdots a_p = e\}$. Consider the set map $\phi : S \to G^{p-1}, (a_1, \ldots, a_p) \mapsto (a_1, \ldots, a_{p-1})$ by dropping the last entry. Surjectivity is clear. If $\phi(a_1, \ldots, a_p) = (a_1, \ldots, a_{p-1}) = (b_1, \ldots, b_{p-1}) = \phi(b_1, \ldots, b_p)$, then $a_i = b_i$ for all $1 \leq i < p$, and $a_p = b_p = (a_1 \cdots a_{p-1})^{-1}$. So ϕ is injective. Hence $|S| = |G|^{p-1}$. Let Z be the set of fixed points of S from $\mathbb{Z}/p\mathbb{Z}$ action (by shifting indices). It's easy to see that $Z = \{(a, \ldots, a) : a \in G, a^p = e\}$. But since there are exactly n elements of order p in G, together with e we have exactly $n + 1$ elements in Z. Since $\mathbb{Z}/p\mathbb{Z}$ is a p-group, by the lemma from class,

$$|S| \equiv |Z| \bmod p.$$

But since order of any element divides the order of group, $p||G|$ so $p||G|^{p-1} = |S|$. Therefore, p must also divide $|Z| = n + 1$.