21-610 HW #1

Wilson Pan

January 20, 2026

Problem 1

Since $G/Z(G)$ is cyclic then there exist some generator xH where $H := Z(G)$ such that $\langle xH \rangle = Z/Z(G)$. For any $g \in G$, g must be in one of the cosets in $Z/Z(G)$ since the cosets partition G. So take any $g, g' \in G$ then suppose $g \in x^n H$ and $g' \in x^m H$. We can write

$$g = x^n h \text{ and } g' = x^m h' \text{ for some } h, h' \in H.$$

Then

$$g \cdot g' = x^n h x^m h' = h' x^n x^m h = h' x^{n+m} h = h' x^m x^n h = x^m h' x^n h = g' \cdot g.$$

Such manipulation is possible as $h, h' \in H = Z(G)$. Thus, G is abelian.

A counter example to $G/Z(G)$ abelian but G not is D_8 as $|Z(D_8)| = 2$ as $Z(G) = \{e, r^2\}$. So by Lagrange's Theorem, $|D_8/Z(D_8)| = 4$ and by problem 2A is abelian but D_8 is not.

Problem 2

Lemma 0.1. *For a prime p, groups of order p^n have non-trivial centers.*

Proof. Let our group be G with $|G| = p^n$. Consider the conjugacy actions then the orbits under conjugacy partition G so

$$|G| = \sum_{x \in G} |\mathcal{C}_x| = \sum_{x \in Z(G)} |\mathcal{C}_x| + \sum_{x \notin Z(G)} |\mathcal{C}_x| = |Z(G)| + \sum_{x \notin Z(G)} |\mathcal{C}_x|.$$

The last equality is true by if $x \in Z(G)$ then $\forall g \in G$, $gx = xg \iff gxg^{-1} = x$ so $|\mathcal{C}_x| = 1$. Since conjugacy classes are subgroups of G, by lagrange's theorem, for $x \notin Z(G)$ we have $|\mathcal{C}_x| \Bigm| |G|$. With $|\mathcal{C}_x| > 1$ otherwise we'll have $x \in Z(G)$, we have $|C_x| = p^m$ for some integer $m < n$. Consequently, since $p \Bigm| G|$ then

$$p \Bigm| |Z(G)| + \sum_{x \notin Z(G)} |\mathcal{C}_x|.$$

So $p \Bigm| |Z(G)|$ so $|Z(G)| > 1$ and is thus non-trivial □

Part A

To show all groups say G of order p^2 is abelian, consider the center $Z(G)$. Since $Z(G) \leq G$ then $|Z(G)| \Bigm| |G|$ so by Lagrange's Theorem $|Z(G)|$ can be potentially $1, p$ or p^2. However, by lemma 0.1 we have $|Z(G)| \neq 1$. If $|Z(G)| = p$ then by Lagrange's Theorem, $|G/Z(G)| = \frac{|G|}{|Z(G)|} = p$ and all groups of order p are cyclic so by the result in problem 1, G is abelian. In the case of $|Z(G)| = p^2$ then $G = Z(G)$ so G is abelian.

Part B

If G is a non-abelian group of order p^3, we want to show $|Z(G)| = p$. We know $|Z(G)| \Bigm| |G|$, so $|Z(G)|$ can potentially be $1, p, p^2, \text{or } p^3$.

By Lemma 0.1, $|Z(G)| \neq 1$. Additionally, $|Z(G)| \neq p^3$, otherwise $Z(G) = G$ and G would be abelian, a contradiction.
If $|Z(G)| = p^2$, then $|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^3}{p^2} = p$.
Since every group of prime order is cyclic, $G/Z(G)$ would be cyclic.
However, by the result in problem 1 (if $G/Z(G)$ is cyclic then G is abelian), this implies G is abelian, which is a contradiction. Thus, $|Z(G)| \neq p^2$.
Therefore, the only remaining possibility is $|Z(G)| = p$.
To show $G/Z(G)$ is abelian, observe that $|G/Z(G)| = \frac{p^3}{p} = p^2$. By the result proved in part A, any group of order p^2 is abelian. Thus, $G/Z(G)$ is abelian. Note that $G/Z(G)$ is not cyclic, as otherwise (by Problem 1 again) G would be abelian.

Problem 3

Let $\phi \in Z(Aut(G))$ then consider the automorphism defined by $c_g(x) = gxg^{-1}$ for some $g \in G$ then

$$\phi(g)\phi(x)\phi(g)^{-1} = \phi(gxg^{-1}) = \phi \circ c_g = c_g \circ \phi = c_g(\phi(x)) = g\phi(x)g^{-1}.$$

So we have

$$\phi(g)\phi(x)\phi(g)^{-1} = g\phi(x)g^{-1}.$$

Let $y = \phi(x)$ then

$$\phi(g)y\phi(g)^{-1} = gyg^{-1} \iff g^{-1}\phi(g)y = yg^{-1}\phi(g).$$

We can conclude $g^{-1}\phi(g) \in Z(G)$
Since $|Z(G)| = 1$ then $Z(G) = \{e\}$ so $g^{-1}\phi(g) = e$ and thus $\phi(g) = g$ and this holds for arbitrary $g \in G$ so $|Z(Aut(G))| = 1$ and is the identity automorphism.

Problem 4

Let $|a| = n$ and $|b| = m$ then as G is abelian

$$(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m (b^m)^n = e^m e^n = e.$$

So $|ab| \leq nm$.

To show this may fail when G is not abelian, consider $G = GL_2(\mathbb{R})$ and two matrices of order 2 namely

$$A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

We have

$$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

So $|A| = 2$ and

$$B^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

So $|B| = 2$.
Claim: $(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$
We'll show this by induction.
(Base Case) When $n = 1$, $AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, so it holds true for $n = 1$
(Induction Step) Assume it holds true for n then

$$(AB)^{n+1} = (AB)^n(AB) = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -(n+1) \\ 0 & 1 \end{pmatrix}.$$

So it holds true by induction. Consequently, $(AB)^{n+1} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as $-n \neq 0$ for $n \geq 1$.

Problem 5

Part A

Consider a matrix where the rows are group elements of G and columns are set elements of X. Then for any grid $(g, x) \in G \times X$, it is 1 if $g \cdot x = x$ and 0 otherwise. Then the LHS $\sum_{g \in G} |Fix(g)|$ goes along each row and counts the number of ones in each row. Similarly for $\sum_{x \in X} |G_x|$ counts the number of ones in each column. So they are equal as both counts the number of ones in the entire matrix.

Part B

We can rewrite with part A to get

$$\frac{\sum_{g\in G} |Fix(g)|}{|G|} = \frac{\sum_{x\in X} |G_x|}{|G|} = \frac{\sum_{x\in X} \frac{|G|}{|\mathcal{O}_x|}}{|G|} = \sum_{x\in X} \frac{1}{|\mathcal{O}_x|}.$$

Consider any orbit say θ and if $|\theta| = n$ then for each $x \in \theta$ it contributes $\frac{1}{n}$ to the sum but there are n elements so the total contribution of any orbit is 1.

$$\sum_{x\in X} \frac{1}{|\mathcal{O}_x|} = \# \text{ orbits}.$$

Problem 6

Let $G = D_{24}$ and $X = \{(c_1, ..., c_{12}) | c_i \in \{\text{red, green, blue}\}\}$. Then let G act on X where

$$r \cdot (c_1, ..., c_{12}) = (c_2, ..., c_{12}, c_1)$$
$$s \cdot (c_1, ..., c_{12}) = (c_{12}, ..., c_1)$$

For any $r^k \in D_{24}$, it'll break the beads into $\gcd(12, k)$ cycles and each cycle must be the same color since if a cycle c has length say $m + 1$ and $c = (c_i, c_{i+k}, ...c_{i+mk})$ then $c_i = c_{i+k}, c_{i+k} = c_{i+2k}, ..., c_{i+mk} = c_i$. So $c_i = c_{i+k} = \cdots = c_{i+mk}$.
For each of these cycles there are 3 possible ways to color them so $|Fix(r^k)| = 3^{\gcd(12,k)}$.
For the reflections, if the line of symmetry goes through two vertices then we fixed 2 vertices (vertices the line passed through) and there are 5 cycles. So there are $3^2 \cdot 3^5 = 3^7$ fixed elements in this case. Otherwise, if the line of symmetry does not go through vertices we have 6 cycles so 3^6. Each case has 6 cases so $6(3^7 + 3^6)$.
By Problem 5, we have

$$\#\text{Orbits} = \frac{\sum_{g \in G} |Fix(G)|}{|G|} = \frac{6(3^7 + 3^6) + \sum_{k=1}^{12} 3^{\gcd(12,k)}}{24} = \frac{6(3^7 + 3^6) + 532416}{24} = 22913.$$