MATH 3311, FALL 2025: HOMEWORK 5

(1) Decide if the following are true or false:
   (a) There is no non-trivial homomorphism $\mathbb{Z}/9\mathbb{Z} \to (\mathbb{Z}/25\mathbb{Z})^{\times}$.

   True: $|(\mathbb{Z}/25\mathbb{Z})^{\times}| = \phi(25) = 25 \cdot \frac{4}{5} = 20$. Therefore, $|g| \mid 20$. There is a bijection between $\mathrm{Hom}(\mathbb{Z}/9\mathbb{Z}, (\mathbb{Z}/25\mathbb{Z})^{\times}) \to \{g \in (\mathbb{Z}/25\mathbb{Z})^{\times} : |g| \mid 9\}$. For $|g|$ to divide both 20 and 9, it must be 1, meaning $g = e$. So, the latter set in our only consists of e. Therefore, the only homomorphism in the former set is given by $\psi(a) = e^a = e$, which is the trivial homomorphism.

   (b) If G is a group of order 1024, then $Z(G) \neq \{e\}$.

   True: $|G| = 1024 = 2^{10}$, so G is a p-group. According to HW#4 problem 8, $Z(G) \neq \{e\}$ is nontrivial.

   (c) There is a subgroup of $\mathbb{Z}$ with exactly 2024 cosets.

   True: Take $2024\mathbb{Z}$. Then, the number of $a + 2024\mathbb{Z}$ is the same as the number of equivalence classes modulo 2024, which is exactly 2024. (i.e. $|\mathbb{Z}/2024\mathbb{Z}| = 2024$)

   (d) If D_{10} acts on a set X with 8 elements, and there are no fixed points, then every orbit must have exactly 2 elements.

   True: $\forall x \in X, |\mathcal{O}(x)| \mid 10$. So orbits have possible sizes of 1, 2, and 5. Since there are no fixed, possible sizes are 2 and 5. If an orbit was size 5, there would be 3 elements left, which cannot be split into sizes of 2 or 5. So each orbit must have exactly two elements.

   (e) Every subgroup of an abelian group is *normal*. [1]

   True: Take an abelian group G and an arbitrary subgroup $H \leq G$. Then, $gHg^{-1} = \{ghg^{-1} : h \in H\} = \{gg^{-1}h : h \in H\} = \{h : h \in H\} = H$.

(2) Suppose that G is a finite group acting on a finite set X. For each $g \in G$, set $X^g = \{x \in X : g \cdot x = x\}$, and let X/G be the set of *orbits* for the action of G on X. Prove *Burnside's lemma*:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} X^g.$$

Hint: Count the size of the set $\{(g,x) \in G \times X : g \cdot x = x\}$ in two different ways.

Let $P = \{(g,x) \in G \times X : g \cdot x = x\}$. $|P| = \sum_{g \in G} |X^g|$ $|P| = \sum_{x \in X} |G_x| = \sum_{x \in X} |G|/|\mathcal{O}(x)| = |G| \sum_{x \in X} \frac{1}{\mathcal{O}(x)} = |G||X/G|$. The last equality is true because for each orbit, there are $|\mathcal{O}(x)|$ elements that contribute to the sum of $\frac{1}{|\mathcal{O}(x)|}$, yielding 1 for each orbit. Therefore, the summation is same as the number of orbits.

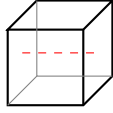Therefore, $|G||X/G| = \sum_{g \in G} X^g$, meaning $|X/G| = \frac{1}{|G|} \sum_{g \in G} X^g$.

(3) Use Burnside's lemma to count the possible colorings of the faces of a cube using 3 colors. Here, two colorings are considered the same if one can be rotated to match the other.

   This is the same as counting the number of orbits X/G if G is the group of rotations acting on X, which is the set of colorings of each face. Recall $|G| = 24$.

---

[1]See definition from Homework 4.

Case 0: $e \in G$. $\forall x \in X, e \cdot x = x$. So $|X^e| = |X| = 3^6$.

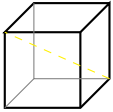Case 1: $g \in G$ is a 90° rotation (either direction) across an axis that starts from the middle of one face to an opposite face. There are 3 such axes with 2 elements each, giving 6 such elements.
Notice that after rotation, the faces with the axis going through does not change color. So these could be anything. However, the other faces will always change color, so these need to be the same color. Therefore, we have $3 \times 3 \times 3 = 3^3$ things in X^g.

Case 2: $h \in G$ is a 180° rotation across the same such axes. Then, there are 3 such elements. Again, the faces with the axis going through does not change color. For the other faces, the opposing ones "swap" position, so colorings will stay the same if opposing sides have same color. We have $3 \times 3 \times 3 \times 3 = 3^4$ things in X^h.
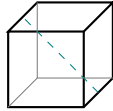
Case 3: $k \in G$ is a 120° rotation (either direction) across axes from one vertex to the opposite vertex. There are 4 such axes with 2 elements each, giving 8 such elements.
Every color gets sent to an adjacent one within the corner. Therefore faces sharing one corner of the axis have the same color, there are $3 \times 3 = 9$ colorings in X^k.

Case 4: $l \in G$ is a 180° rotation across axes from the middle of one edge to the middle of the opposing edge. There are 6 such axes with 1 element each, giving 6 such elements.
Here, at least from the image, the top face gets sent to the left face, bottom face to the right face, and the front face to the back face. Therefore, we only need that the colors on the corresponding faces are the same. There are $3 \times 3 \times 3 = 3^3$ things in X^l.

Now, $|X/G| = \frac{1}{|G|} \sum_{g \in G} G^x = \frac{1}{24}(1 \cdot 3^6 + 6 \cdot 3^3 + 3 \cdot 3^4 + 8 \cdot 3^2 + 6 \cdot 3^3) = 57$.
There are 57 possible colorings of the faces of a cube using 3 colors.

(4) Suppose that $H \leq G$ is a subgroup of index 2. Show that H is automatically normal.

Lemma 1. $\forall g \in G, gH = Hg \implies H$ *is normal*

Proof. Assume $\forall g \in G, gH = Hg$. $\forall h \in H, gh = \tilde{h}g$ for some $\tilde{h} \in H$. Then, $ghg^{-1} = \tilde{h} \in H$. ☐
Now, $Hg = g^{-1}H$ because these two have the same size, and $\forall h \in H, (hg)^{-1} \in Hg$.

Elements in the cosets here are closed under taking inverses. If the element was in H, by property of subgroups, the inverse is in H. If the element was in a different coset, the inverse must also be. Else, if the inverse is in H, the inverse of inverse, which is itself, is also in H.

So Hg is also a coset of H. Now, $g \in Hg$ and $g \in gH$ because $g = eg = ge$. Since Hg and gH are left cosets with a common element, they must be the same. Therefore, $Hg = gH$. By our lemma, H is a normal subgroup.

The **conjugacy class** of an element $h \in G$ is its orbit under the conjugation action.

(5) Compute the conjugacy classes in the group D_{2n} for $n \geq 3$.

The rotations are of form σ^i. Then, its elements of its orbits are of the form $\sigma^k \sigma^i \sigma^{-k}$ or of the form $\sigma^k \tau \sigma^i (\sigma^k \tau)^{-1}$.

The former is always equal to $\sigma^{k+n-k=\sigma^i}$. On the other hand, the latter is $\sigma^k \tau \sigma^i (\sigma^k \tau)^{-1} = \sigma^k \tau \sigma^i \sigma^k \tau = \tau \sigma^{-k} \sigma^i \sigma^k \tau = \tau \sigma^i \tau = \tau \tau \sigma^{-i} = \sigma^{-i}$.

Therefore, a conjugacy class of a rotation $\mathcal{O}(\sigma^k) = \{\sigma^k, \sigma^{-k}\} = \{\sigma^k, \sigma^{n-k}\}$.

The reflections are of the form $\sigma^i \tau$. The elements of its orbits are of the form $\sigma^k \sigma^i \tau \sigma^{-k} = \sigma^k \sigma^i \sigma^k \tau = \sigma^{n+2k} \tau$ or of the form $\sigma^k \tau \sigma^i \tau (\sigma^k \tau)^{-1} = \sigma^k \tau \sigma^i \tau \tau^{-1} \sigma^{-k} = \sigma^k \tau \sigma^i \sigma^{-k} = \tau \sigma^{-k} \sigma^i \sigma^{-k} = \tau \sigma^{n-2k}$.

Therefore, a conjugacy class of a reflection $\mathcal{O}(\sigma^i) = \{\sigma^{n+2k} \tau \ k \in \mathbb{Z}\}$. Basically, observe that if the power of the rotation part of a reflection has the same parity, they are in each other's orbits. So when n is even, there are two separate conjugacy classes of the reflections, namely $\{\sigma^{1+2k} \tau : k \in \mathbb{Z}\}$ and $\{\sigma^{2k} \tau : k \in \mathbb{Z}\}$. It is clear that they span the whole set of rotations. They are also distinct because if $\sigma^{2k+1} \tau = \sigma^{2j} \tau$, then, $\sigma^{2(k-j)+1} = e \implies |\sigma| \mid 2(k-j) + 1$. However, $|\sigma| = n$ is even.

On the other hand, if n is odd, the orbit of reflections would be the whole set of reflections. This is because $\sigma^{2k} \tau = \sigma^n \sigma^{2k} \tau = \sigma^{2k+n} \tau$, and $2k$ is even while $2k + n$ is odd. So every reflection with an even power of σ is that of an odd power of σ (and vice versa).

Therefore, the set conjugacy classes of D_{2n} is $\{\{\sigma^k, \sigma^{n-k}\} : k \in \{0, 1, ..., \frac{n}{2} - 1\}\} \cup \{\{\sigma^{1+2k} \tau : k \in \mathbb{Z}\}, \{\sigma^{2k} \tau : k \in \mathbb{Z}\}\}$ if n is even. It is $\{\{\sigma^k, \sigma^{n-k}\} : k \in \{0, 1, ..., \frac{n}{2} - 1\}\} \cup \{\{\sigma^k \tau : k \in \mathbb{Z}\}\}$ if n is odd.

It is worth mentioning that if n is even, there is a fixed point besides $\{\mathrm{Id}\}$, namely $\{\sigma^{\frac{n}{2}}\}$, as $\sigma^{n-\frac{n}{2}} = \sigma^{\frac{n}{2}}$.

A group action $G \curvearrowright X$ is **transitive** if X has a *single* orbit.

The **kernel** $\ker f$ of a group homomorphism $f : G \to G'$ is the subset

$$\ker f = \{g \in G : \ f(g) = e\}.$$

(6) Suppose that $H \leq G$ is a subgroup.
  (a) Show that there is a *transitive* action of G on G/H given by:

$$G \times G/H \xrightarrow{(g_1, g_2 H) \mapsto g_1 g_2 H} G/H.$$

First, this is a group action.

Well-defined ness: $\forall g', \tilde{g} \in G, g'H = \tilde{g}H \iff \tilde{g}^{-1} g' \in H \iff (g\tilde{g})^{-1} gg' \in H \iff gg'H = g\tilde{g}H \iff g \cdot g'H = g \cdot \tilde{g}H$.

Identity: $\forall gH \in G/H, e \cdot gH = egH = gH$. "Associativity": $\forall g_1, g_2 \in G, \forall gH, g_1 \cdot (g_2 \cdot gH) = g_1 \cdot g_2 gH = g_1 g_2 gH = g_1 g_2 \cdot gH$.

We will find the orbit of eH. $\forall g \in G, g \cdot eH = gH$, so every possible coset is in the orbit of eH. Therefore, the given action is transitive.

  (b) Conclude that there is a natural homomorphism of groups

$$\rho : G \to \mathrm{Bij}(G/H).$$

Because have a group action of G on G/H, there is such a homomorphism of groups.

(c) Show that we have
$$\ker \rho = \bigcap_{g \in G} gHg^{-1}.$$

$\ker \rho = \{g \in G : \rho(g) = \mathrm{Id}\} = \{g \in G : \forall \tilde{g}H \in G/H, g\tilde{g}H = \tilde{g}H\}$

Now, $g\tilde{g}H = \tilde{g}H \implies \forall h \in H \exists \tilde{h} \in H : g\tilde{g}h = \tilde{g}\tilde{h} \implies g\tilde{g} = \tilde{g}\tilde{h}h^{-1} \implies g = \tilde{g}\tilde{h}h^{-1}\tilde{g}^{-1} \implies g \in \tilde{g}H\tilde{g}^{-1}$

If $g \in \tilde{g}H\tilde{g}^{-1}$, $g = \tilde{g}h\tilde{g}^{-1} \implies g\tilde{g} = \tilde{g}h$ for some $h \in H$. Then, $\forall \tilde{h} \in H, g\tilde{g}\tilde{h} = \tilde{g}h\tilde{h} \in \tilde{g}H$. Therefore, $g\tilde{g}H \subseteq \tilde{g}H$. Since cosets are orbits of right multiplication, having common elements means $g\tilde{g}H = \tilde{g}H$. Therefore, $g\tilde{g}H = \tilde{g}H \iff g\tilde{g}H = \tilde{g}H$.

So $\ker \rho = \{g \in G : \rho(g) = \mathrm{Id}\} = \{g \in G : \forall \tilde{g}H \in G/H, g\tilde{g}H = \tilde{g}H\} = \{g \in G : \forall \tilde{g} \in G, g \in \tilde{g}H\tilde{g}^{-1}\} = \cap_{\tilde{g} \in G}\tilde{g}H\tilde{g}^{-1}$

Relabeling $\tilde{g}$ as g, we get $\ker \rho = \cap_{g \in G}gHg^{-1}$.

A group action $G \curvearrowright X$ is **faithful** if the group action homomorphism
$$\rho : G \to \mathrm{Bij}(X)$$
is *injective.*

(7) Show that, if G is an abelian group and $H \leq G$ is a non-trivial subgroup, then the action $G \curvearrowright G/H$ on the set of left cosets of H in G is never faithful.

Lemma 2. $\ker \rho \neq \{e\} \implies \rho$ *is not injective.*

Proof. Suppose a nonidentity element $g \in \ker \rho$ exists. Claim: $\rho(g) = \rho(g^2)$
First, $g \in \ker \rho \implies \rho(g) = \mathrm{Id}$. Then, $\rho(g^2) = \rho(g) \circ \rho(g) = \mathrm{Id} \circ \mathrm{Id} = \mathrm{Id}$.
Now, $g^2 \neq g$, for $g^2 = g \implies g = e$ is a contradiction. However, $\rho(g) = \rho(g^2) \wedge g \neq g^2$. As such, injectivity must fail.
$\square$

Lemma 3. $gHg^{-1} = H$ *if G is abelian.*

Proof. $\forall h \in H, ghg^{-1} = gg^{-1}h = h \in H$. Therefore, $gHg^{-1} \subseteq H$. Now, $\forall h \in H, hg = gh \implies h = ghg^{-1} \in gHg^{-1}$, proving $H \subseteq gHg^{-1}$. Therefore, $gHg^{-1} = H$.
$\square$

From problem 6c, $\ker \rho = \cap_{g \in G}gHg^{-1} = \cap_{g \in G}H = H$ is nontrivial. So ρ is never injective, and the group action is never faithful.

(8) Suppose that G has order 75, and let $H \leq G$ be a subgroup of index 3. Show that, if $H' \leq G$ is any subgroup of index 3, then in fact $H' = H$. *Hint: Consider the left multiplication action of H' on $X = G/H$ and think about fixed points.*

$H' \curvearrowright G/H$ via left multiplication action: $h' \cdot gH = h'gH$.

Well defined ness: $\forall h', \tilde{h} \in H', h'H = \tilde{h}H \iff \tilde{h}^{-1}h' \in H \iff (h\tilde{h})^{-1}hh' \in H \iff hh'H = h\tilde{h}H \iff h \cdot h'H = h \cdot \tilde{h}H$. Identity: $e \cdot gH = egH = gH$.

"Associativity": $h_1' \cdot (h_2' \cdot gH) = h_1' \cdot h_2'gH = h_1'h_2'gH = h_1'h_2' \cdot gH$.

Recall that we proved in HW4P5 $|X^G| \equiv |X| \pmod{p}$ given G is a p-group acting on X, a finite set. Now, H' is a p-group ($|H'| = |G|/|G : H'| = 75/3 = 25 = 5^2$) acting on G/H with $[G : H] = 3$ elements.

Now, $|H/G^{H'}| \equiv |H/G| \pmod{5}$.

Notice that $|G/H| = 3$, meaning $|G/H|^{H'} \equiv 3 \pmod{5}$. Furthermore, since $G/H^{H'} \subseteq G/H$, it must be the case that $|G/H^{H'}| = 3$, meaning $G/H^{H'}$ consists of all the elements in G/H.

So, $G/H^{H'} = \{gH : g \in G, \forall h' \in H', h' \cdot gH = h'gH = gH\}$. Since $eH \in \{G/H^{H'}\}$, $\forall h' \in H', h' \cdot eH = h'eH = eH$ means $h'H = H$ means $h' \in H$.

Therefore, $H' \subseteq H$. Now, $|H| = |G|/|G : H| = 75/3 = 25$. So $|H'| = |H| = 25$ so $H' = H$.