Assignment 4 – Solutions

MATH 3175–Group Theory

Problem 1. For each of the following group actions, we will determine their orbits and stabilizer subgroups, and decide whether those actions are faithful, free, or transitive (or any combination thereof).

(1) Let $\mathrm{Sym}(X)$ be the symmetric group on a set X, acting on X by $\mathrm{Sym}(X) \times X \to X$ where $(\sigma, x) \mapsto \sigma(x)$.

Given any $x, y \in X$, there is a bijection $\sigma\colon X \to X$ such that $\sigma(x) = y$ (for instance, the permutation that transposes x and y and leaves everything else fixed). Thus, $Gx = X$ for all $x \in X$ and the action is transitive. Each stabilizer G_x is isomorphic to $\mathrm{Sym}(X \setminus \{x\})$; thus, if $|X| > 1$, the action is not free, but, nevertheless, it is faithful.

(2) The dihedral group $G = D_n$ acts on the set of vertices of an n-gon, denoted by $V = \{1, 2, 3, ..., n\}$ in the usual fashion, with generators r the rotation acting as a cyclic permutation $(12 \dots n)$ and s the reflection acting as the transposition (12).

The orbit of any vertex is the whole vertex set V, and so the action is transitive. Each vertex v is left fixed by at least one reflections, and thus has a non-trivial stabilizer, so the action is not free. Nevertheless, no vertex is left fixed by all the non-trivial group elements, so the action is faithful.

(3) The general linear group $G = \mathrm{GL}_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication: $\mathrm{GL}_n(\mathbb{R}) \times \mathbb{R} \to \mathbb{R}$ where $(M, x) \mapsto Mx$.

The vector $0 \in \mathbb{R}^n$ is fixed by this action; thus $G \cdot 0 = \{0\}$ and $G_0 = G$, and so the action is neither free, nor transitive. On the other hand, if $v \in \mathbb{R}^n \setminus \{0\}$ is a non-zero vector, then $G \cdot v = \mathbb{R}^n \setminus \{0\}$, and $G_v = \{I_n\}$, where I_n is the identity $n \times n$ matrix, so the action is both free and transitive on non-zero vectors. On the whole, the action is faithful, since the intersection of all the stabilizers is $\{I_n\}$.

(4) Let G be a group acting on itself by left multiplication: $G \times G \to G$ where $(a, b) \mapsto ab$.

Given any $x, y \in G$, there is a $g \in G$ such that $gx = y$ (simply take $g = y^{-1}x$). Thus, $Gx = G$ and the action is transitive. Moreover, if $gx = x$, then $g = e$, and so $G_x = \{e\}$. This implies that the action is free and thus, faithful.

(5) Let G be a group acting on itself by conjugation: $G \times G \to G$, where $(a, b) \mapsto aba^{-1}$.

The orbit of $b \in G$ is $Gb = Cl(b)$, the conjugacy class of b, while its stabilizer is $G_b = C(b)$, the centralizer of b. Thus, the action is transitive if and only if there is a single conjugacy class, which only happens if G is trivial. The action is free if and only if G is abelian and it is faithful if and only if the center $Z(G)$ is trivial.

(6) Let H be a subgroup of G. Then G acts on the set of left cosets G/H by left multiplication: $G \times G/H \to G/H$ where $(a, bH) \mapsto abH$.

The action permutes the cosets of H, and thus is transitive: if aH and bH are two cosets, then $(ba^{-1}) * aH = bH$. The stabilizer of a coset bH is the subgroup bHb^{-1}; indeed, $a \in G_{bH}$ iff $abH = bH$ iff $b^{-1}ab \in H$ iff $a \in bHb^{-1}$. Thus, the action is never free (unless H is trivial to start with, which is the situation from case 4). Furthermore, the intersection of all the stabilizers of cosets of H is the normalizer $N(H)$; thus, the action is faithful if and only if H is a normal subgroup of G.

(7) Let H be a normal subgroup in G; then G acts on G/H by conjugation: $G \times G/H \to G/H$ where $(a, bH) \mapsto aba^{-1}H$. Indeed, $x * (y * (bH)) = x * (yby^{-1}H) = xyby^{-1}x^{-1}H = (xy)b(xy)^{-1}H = (xy) * bH$, and also $e * bH = bH$, and so this is a valid group action.

If H is trivial, we are back to case 5. Otherwise, the orbit of a coset bH is the union of all cosets cH where c runs through the conjugacy class of b, while the stabilizer $G_{bH} = \{a \in G \mid aba^{-1}H = H\}$ coincides with H, since H is normal. Thus, the action is neither transitive, nor faithful (and hence, not free).

(8) Let $f \colon G \to \mathrm{Sym}(X)$ be a homomorphism; then G acts on X by $G \times X \to X$ where $(a, x) \mapsto f(a)(x)$. Indeed, $a * (b * x) = a * (f(b)(x)) = f(a)(f(b)(x)) = (f(a) \circ f(b))(x) = f(ab)(x) = (ab) * x$, and also $e * x = f(e)(x) = \mathrm{id}_X(x) = x$, and so this is a valid group action. In fact, any group action arises in this fashion, so the orbits and stabilizers can be arbitrary (except that they still need to satisfy the conclusion of the orbit-stabilizer theorem), while the action need not be either free, transitive, or faithful.

Problem 2.

(1) Notice that $1331 = 11^3$. Hence, G is a p-group. Then, by problem 4.1 it follows that the center is non-trivial. $\square$

(2) Consider the dihedral group D_{2k+1}. Then, the order of this group is $4k+2$. Assume we have an element $x \neq e$ in the center $Z(D_{2k+1})$. Since $x \in D_{2k+1}$, we can write $x = r^i s^j$ (since r and s generate D_{2k+1}). So, if $x \in Z(D_{2k+1})$, then

$$xr = rx \implies r^i s^j r = r r^i s^j \implies r^{i+1} s^j = r^i s^j r \implies r s^j = s^j r.$$

We have two possibilities for j which occur; either $j = 0$ or $j = 1$. Assuming that $j = 0$, then we obtain $r = r$, which is true. Alternatively if $j = 1$, then our computation demands that $rs = sr$. Recalling the dihedral group relation $rs = sr^{-1}$, we find that

$$sr = sr^{-1} \implies r = r^{-1} \implies r^2 = e.$$

It cannot be that $r = e$ since $x \neq e$, so instead we must accept that $\mathcal{O}(r) = 2$. However, this implies that $2 \mid 2k+1$, which is absurd since $2k+1$ is odd by definition. Hence, we must have that $j = 0 \implies x = r^i$ for some $0 \leq i < 2k+1$. We again make use of the dihedral group relation

$$xs = r^i s = sr^{-i} = sr^{2k+1-i},$$

that shows that x commutes with s only if

$$i = 2k+1-i \implies 2i = 2k+1,$$

which is clearly a contradiction. Therefore, we must reject our assumption that $Z(G)$ is non-trivial.

Problem 3. Let G be a group and let H be a subgroup of G.

(1) Assume that $H \subset Z(G)$. Let $a \in G, h \in H$. Then

$$h \in Z(G) \implies ah = ha \implies aha^{-1} = h \implies aha^{-1} \in H,$$

showing that H is a normal subgroup of G. □

(2) We will begin by showing the case where $H = Z(G)$, so suppose that

$$\mathrm{Inn}(G) \cong \frac{G}{Z(G)} \cong \langle aZ(G) \rangle$$

for some $a \in G$. Because inner automorphisms are simply conjugations, the cyclicity of $\mathrm{Inn}(G)$ asserts that for every $g \in G$, there exists some $n \in \mathbb{Z}$ such that

$$gxg^{-1} = a^n x a^{-n}$$

for any $x \in G$. In particular, $a \in Z(G)$ by the computation

$$gag^{-1} = a^n a a^{-n} = a \implies ga = ag.$$

With this established, we see that

$$gxg^{-1} = a^n x a^{-n} = x \implies gx = xg,$$

so G is Abelian. Now suppose instead that $H \leq Z(G)$ and that G/H is cyclic (G/H a group by part (1)). By invoking the correspondence and 3rd isomorphism theorems, we observe that

$$\frac{Z(G)}{H} \leq \frac{G}{H} \implies \frac{G/H}{Z(G)/H} \cong G/Z(G)$$

is cyclic as the quotient of a cyclic group. We conclude that G is Abelian by our first argument.

Problem 3.2 (Alternate) Suppose that $H \leq Z(G)$ and G/H is cyclic. First, observe that by part 3.1, $H \trianglelefteq G$, so G/H forms a group. Next, note that G/H cyclic $\implies G/H = \langle aH \rangle$ for some $a \in G$.

Now consider an element of G, say g. Then, $gH = (aH)^k = a^k H$ for some $k \in \mathbb{Z}$. Also recall that g is equivalent to a^k modulo H if and only if $(a^k)^{-1} g \in H$, that is, $a^{-k} g = h$ for some $h \in H$, implying we can write $g = a^k h$. We will use this fact to show that G is Abelian.

Let $g_1, g_2 \in G$. We have seen above that we can write $g_1 = a^{k_1} h_1$ and $g_2 = a^{k_2} h_2$ for some $h_1, h_2 \in H$, where a is the representative of the left coset that generates the cyclic group G/H. So, $g_1 g_2 = a^{k_1} h_1 a^{k_2} h_2$. Now, since $h_1, h_2 \in Z(G)$, they commute with all elements in G, and so

$$g_1 g_2 = h_1 a^{k_1} a^{k_2} h_2 = h_1 a^{k_1 + k_2} h_2 = h_1 a^{k_2} a^{k_1} h_2 = a^{k_2} h_2 a^{k_1} h_1 = g_2 g_1.$$

This shows that G is Abelian. □

Problem 4.

(1) Let p be prime, and let G be a p-group, so that $|G| = p^n$ for some $n \geq 1$. We wish to show that the center $Z(G)$ is non-trivial. If $n = 1$, i.e., G has prime order, then G is cyclic, and

thus Abelian, i.e., $Z(G) = G$, and so the center is non-trivial. So we may assume $|G| = p^n$, for some $n \geq 2$.

Consider now the conjugation action of G on itself. Then the conjugacy class of an element $a \in G$ is equal to the orbit Ga of this action (i.e., $C_G(a) = Ga$ here). Also, as we have seen in the proof of the class equation, $G_a = C_G(a)$, so $C_G(a)$ is a subgroup of G by Problem 1, and thus we can use the orbit stabilizer theorem. Consider the class equation,

$$|G| = |Z(G)| + \sum_{i \in I} [G : C_G(a_i)],$$

where $\{a_i\}_{i \in I}$ is a set of representatives for the non-trivial conjugacy classes of G. Since these conjugacy classes are non-trivial, we must have $|Ga_i| > 1$ (they contain more than just a_i). This implies that $[G : C_G(a_i)] = |Ga_i| > 1$. Also, by Lagrange's theorem we have

$$|G| = [G : C_G(a_i)] \mid C_G(a_i)|.$$

So, taking these two results into consideration, it must be the case that $[G : C_G(a_i)]$ divides $|G| = p^n$, and also $[G : C_G(a_i)] \neq 1$. Thus, $[G : C_G(a_i)] = p^k$, for some $1 \leq k < n$ (since $n \geq 2$). Applying this to the class equation ,we get

$$p^n = |Z(G)| + \sum_{i \in I} p^{k_i} \implies p^n - \sum_{i \in I} p^{k_i} = |Z(G)| \implies p\left(p^{n-1} - \sum_{i \in I} p^{k_i - 1}\right) = |Z(G)|.$$

(We can factor out a p and still obtain p times an integer, since all the powers of p are greater than one). Thus, p divides $|Z(G)|$, and since $|Z(G)| \geq 1$ (since it contains the identity element), we have that $|Z(G)| \geq p$, and thus $Z(G)$ is non-trivial. □

(2) We now use part a) to show that every group of order a square of a prime is Abelian. First, let's prove that $Z(G)$ is a subgroup of G:

- Closure: let $a, b \in Z(G)$, then $ax = xa, bx = xb$ for every $x \in G$. So, $(ab)x = abx = axb = xab = x(ab)$, so $ab \in Z(G)$.
- Inverses: let $a \in Z(G)$, then $ab = ba$ for every $b \in G$. Thus, $a^{-1}ab = a^{-1}ba \implies b = a^{-1}ba \implies ba^{-1} = a^{-1}b$. So, $a^{-1} \in Z(G)$.
- Finally, $Z(G) \neq \varnothing$ since it contains the identity.

Thus, the center is a subgroup of G, and, in fact, a normal subgroup of G: this follows immediately from the definition of the center.

Assume now that $|G| = p^2$, for some prime p. Since $Z(G)$ is a subgroup of G, its order divides the order of G, that is, $|Z(G)|$ divides p^2. Furthermore, by part a), $|Z(G)| \neq 1$, and so $|Z(G)| \geq p$. We have two cases to consider:

Case 1: $|Z(G)| = p^2$. In this case the center is the entire group, so every element in the group commutes with every other element of the group. Thus, G is Abelian.

Case 2: $|Z(G)| = p$. Since $Z(G)$ is a normal subgroup of G, the quotient $G/Z(G)$ is a group. We will show that this quotient group is cyclic. By Lagrange,

$$|G/Z(G)| = [G : Z(G)] = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p.$$

Thus, by (Homework 2, Problem 2a), the group $G/Z(G)$ is cyclic. Since $Z(G) \subset Z(G)$, we can now apply Problem 3b), and conclude that G is an Abelian group. But this implies that G is $Z(G)$, which contradicts our assumption that $|Z(G)| = p$, so this case can never happen. Thus, we have shown that G is Abelian. $\square$

Problem 5. Because cycle shape determines the conjugacy class in S_n, we will provide a cycle shape as indicative of each conjugacy class in S_6. The letters a, b, c, d, e, and f will take on values 1 through 6 inclusive but will never take the same value within a given permutation. Notice that the sum of the conjugacy class sizes is $6! = 720$.

Shape	Size of Conjugacy Class
()	$\binom{6}{0} = 1$
(ab)	$\binom{6}{2} = 15$
(ab)(cd)	$\frac{\binom{6}{2} \cdot \binom{4}{2}}{2!} = 45$
(ab)(cd)(ef)	$\frac{\binom{6}{2} \cdot \binom{4}{2} \cdot \binom{2}{2}}{3!} = 15$
(abc)	$\binom{6}{3} \cdot 2! = 40$
(abc)(def)	$\frac{\binom{6}{3} \cdot \binom{3}{3}}{2!} = 40$
(abc)(de)	$\binom{6}{3} \cdot 2! \cdot \binom{3}{2} = 120$
(abcd)	$\binom{6}{4} \cdot 3! = 90$
(abcd)(ef)	$\binom{6}{4} \cdot 3! \cdot \binom{2}{2} = 90$
(abcde)	$\binom{6}{5} \cdot 4! = 144$
(abcdef)	$\binom{6}{6} \cdot 5! = 120$