0.1 Preliminary

Problem 1.7.21. Show that the group of rigid motions of cube is isomorphic to S_4.

There are many ways to show the group isomorphism. By identifying opposite vertices as the same object (and hence thinking of the problem as the rigid motions of the *diagonals* of the cube) we can reduce the problem to thinking about action on the vertices. For simplicity, suppose the cube is centered on the origin, with radius 1, and that each face is perpendicular to a co-ordinate axis. Label the vertices so that $1 \overset{\text{def}}{=} (1,1,1) \equiv (-1,-1,-1)$, $2 \overset{\text{def}}{=} (-1,1,1) \equiv (1,-1,-1)$, $3 \overset{\text{def}}{=} (-1,-1,1) \equiv (1,1,-1)$, $4 \overset{\text{def}}{=} (1,-1,1) \equiv (-1,1,-1)$.

In fact, since the cube is symmetric with regards to the three spatial axes this problem reduces even further: if we can find a single transposition among these elements then we will have found (by symmetry) transpositions for all the elements.

0.2 Approach 1: Direct Approach

The first approach is to examine some subgroups of the group of rigid motions (from here on called G), and from those subgroups seek out a transposition. There are some easy subgroups to find from G: if we consider just rotations around the axes through each face (the x, y, and z axes).

- Rotation around x axis: $\{e, (1324), (12)(34), (1423)\} \overset{\text{def}}{=} G_x$
- Rotation around y axis: $\{e, (1243), (14)(23), (1342)\} \overset{\text{def}}{=} G_y$
- Rotation around z axis: $\{e, (1234), (13)(24), (1432)\} \overset{\text{def}}{=} G_z$

Now: elements of subgroups are by definition group elements of their parent group. So observe that (1324), taken from G_x, and (13)(24), taken from G_z, has product $(1324)(13)(24) = (12)$, the transposition. Since these are all subgroups, (12) must therefore be an element of the overarching group G. Since the cube is symmetric, the existence of (12) guarantees the existence of all transpositions (ij). S_4 is generated by the set of all transpositions; hence $S_4 \leq G$.

We can show $G = S_4$ by working with the size of the group. G has a 2-cycle: rotation around the line drawn from the midpoint of an edge through the center by 180 degrees. G has a 3-cycle: rotation around a vertex will rotate the 3 neighboring vertices of a vertex. G has a 4-cycle, as evidenced by the existence of the subgroups generated by face rotation (G_x, above). From Lagrange's Theorem ($|G| = [G : H]\,|H|$) this suggests many ways of showing $|G| = 24$. For example: the subgroup representing rotation of a face has 6 possible faces to manifest over, indicating $|G| = 6 * 4 = 24$. Similarly and equivalently for vertices and edge-based rotation. Thus G has the same size as S_4, and since G contains generators of S_4, G must be equal to S_4.

0.3 Approach II: Orbit-Stabilizer Theorem

The last step of the first approach, in which we invoke Lagrange's Theorem, suggests to us an interpretation of this problem from the notion of group actions and orbits. The Orbit-Stabilizer Theorem (which is the notion of Lagrange's Theorem applied to group actions instead of cosets) states that for any set and any group action on that set,

$$|\mathrm{Orb}_x| = [G : \mathrm{Stab}_x] = \frac{|G|}{|\mathrm{Stab}_x|}$$

The proof will proceed much as in the first approach, but we can shorten our work for the step that determined the order of G by recognizing that every possible rigid motion is a group action on the set of vertices. For example: if we consider the set of all faces, then the group action induced by rigid motions has stabilizer of order 4 (since four vertices on a face can be rotated without changing the face defined between them) with an orbit of 6 (since there are 6 faces total on the cube). Hence $|G| = 24$. Similarly: rotation through corners has a stabilizer of order 3 (since the neighboring vertices of a vertex don't change under this rotation) with orbit 8 (there are 8 vertices total). Finally, the action of rotation around the axis drawn from the center of an edge has stabilizer 2 (each edge is uniquely defined by two vertices) and has orbit 12 (there are 12 edges).

1 Group Actions $G \curvearrowright G$

1.1 Conjugation

One way in which a group can act on itself is by conjugation. The action in this case is $g \cdot x \stackrel{\text{def}}{=} gxg^{-1}$. The class equation (previously covered in the section on cosets) is

$$|G| = \sum(\text{orders of conjugacy classes}) \tag{1}$$

The center of G, $Z(G)$, is effectively a conjugacy class of the identity. Thus we can pry out one term from (1):

$$|G| = |Z(G)| + \sum(\text{orders of conjugacy classes except the center}) \tag{2}$$

The orbit of any element of G under this group action is in fact the conjugacy class of that element. The stabilizer of any element in G is in fact identical to the centralizer of that element $C_G(x)$ (comparing the definition of stabilizer and centralizer will show this fact). The orbit-stabilizer theorem thus implies in this case that:

$$|G| = |C_G(x)|\,|O_x| \tag{3}$$

Again, the orbit of an element under the action of conjugation is identical to the conjugacy class of that element. This allows us to reinterpret (2) as:

$$|G| = |Z(G)| + \sum_{x_i} \frac{|G|}{|C_G(x_i)|} \tag{4}$$

Here x_i is a representative of a conjugacy class, and we are summing up over the conjugacy classes (typically not every element of G). This suggests to us the following theorem on p-groups (groups of size p^α, a power of a prime):

Theorem 1.1. *Every p-group has nontrivial center.*

Proof. $Z(G)$ contains at least the identity. Thus $|Z(G)| \geq 1$. Since the size of an orbit (and hence a conjugacy class) must be an integer, it must be the case that $|C_G(x_i)|$ divides $|G|$; since $|G| = p^\alpha$, it must be the case that $\dfrac{|G|}{|C_G(x_i)|} = p^{k_i}$ for some positive integer k_i. Hence (4) is rewritten as:

$$|G| = |Z(G)| + \sum_i p^{k_i}$$
$$p^\alpha = |Z(G)| + \sum_i p^{k_i}$$

Since p divides the left, it must also divide the right. The sum is all divisible by p; hence $Z(G)$ must be divisible by p. Thus $Z(G)$ must be some multiple of p; hence $Z(G) \geq p$. This means $Z(G)$ has more elements in it than the identity. □

1.2 Left Cosets

If we have a group G with subgroup $H \leq G$, we can define a group action G on G/H (the set of left cosets of H), by left multiplication: $g \cdot (g_1 H) = g g_1 \cdot H$. The stabilizer of the coset $eH \cong H$ is simply H (since $hH \cong H$). The stabilizer for any arbitrary left coset gH must be gHg^{-1}: since $gHg^{-1} \cdot gH = gHH = gH$. What can we say about the "kernel" of this action?

Let $\varphi : G \to \text{Perm}\,(G/H)$. The kernel of this homomorphism is what we will say is the kernel of the group action. The kernel of φ will be the set of all elements that are fixed in any coset; in other words, the elements that stabilize $g_i H$ for all i. $\ker \varphi \cong \bigcap G_{g_i H}$; $\ker \varphi \cong \bigcap_{g \in G} gHg^{-1}$. We know already that the kernel must be a normal subgroup, so $\bigcap_{g \in G} gHg^{-1} \trianglelefteq G$