MATH 502, PROBLEM SET 2, REVISED

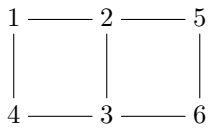
DUE IN MATEI'S MAILBOX IN THE MATH OFFICE BY NOON ON MONDAY, SEPT. 30

A. Transitive permutations groups, blocks and conjugations in S_n.

1. Suppose G is a group acting on a finite non-empty set A. Suppose the action of G on A is transitive, in the sense that given $a, b \in A$, there is some $g \in G$ such that $a = g(b)$. A block of A is a non-empty subset B of A such that for all $g \in G$, either $g(B) = \{g(b) : b \in B\}$ equals B or $g(B)$ and B are disjoint.
   a. Show that if $g_1(B), \ldots, g_m(B)$ are the distinct images of a block B of A under the elements of G then A is the disjoint union $g_1(B) \coprod g_2(B) \coprod \cdots \coprod g_m(B)$ of the $g_i(B)$.
   b. The (transitive) action of G on A is called primitive if the only blocks for this action are either all of A or one element sets. Show that the action of the symmetric group $G = S_4$ on $A = \{1, 2, 3, 4\}$ is primitive.
   c. In class we talked about the action of the dihedral group D_{2n} of order $2n$ by isometries on a regular n-gon in the Euclidean plane $\mathbb{R}^2$. Show that when $n = 4$, the action of D_8 on the four vertices of a square is not primitive.
2. Let g and f be elements of the symmetric group S_n. Suppose g is a product of cycles, which need not be disjoint:
$$g = (a_1, a_2, \ldots, a_m) \cdot (b_1, b_2, \ldots, b_t) \cdots .$$
Prove that
$$fgf^{-1} = (f(a_1), f(a_2), \ldots, f(a_m)) \cdot (f(b_1), \cdots, f(b_t)) \cdots$$
results from applying f to each of the entries in the product for g. (Hint: If $g_1, g_2 \in S_n$ then $f(g_1 g_2)f^{-1} = fg_1f^{-1}fg_2f^{-1}$.)

B. A subgroup of the Rubik cube group

Suppose we number the vertices of two adjoining faces of a Rubik's cube in this way:



Here one face has vertices $\{1, 2, 3, 4\}$ and the other has vertices $\{2, 5, 6, 3\}$. This exercise has to do with analyzing the subgroup G of the permutation group S_6 on the vertices which is generated by clockwise twists around the two faces. These twists have cycle descriptions $A = (1, 2, 3, 4)$ and $B = (2, 5, 6, 3)$, so that G has generators A and B. One byproduct is going to be a way to bring all the vertices of the cube back to their original positions.

3. Show that $C = AB$ has order 5 and $D = ABA$ has order 6, and write down the cycle descriptions of these as permutations.
4. Find an element T of G which is a power of D such that $\beta = TCT^{-1}$ is a 5-cycle which leaves 1 fixed. (Hint: First find an element of $\{1, \ldots, 6\}$ which C leaves fixed. Then use the fact that some power of D sends this element to 1, and use problem #2).

5. Suppose h is an arbitrary element of G. Show that there are integers $0 \leq \ell \leq 5$, $0 \leq q \leq 4$ and $0 \leq \alpha \leq 3$ such that $B^\alpha \cdot \beta^q \cdot D^\ell \cdot h$ fixes each of 1, 4 and 3. (Hint: First use a power of D to bring $h(1)$ back to 1, and then continue.)

6. Conversely, given distinct elements i, j, k of $\{1, 2, 3, 4, 5, 6\}$, show that there is an $h \in G$ of the form $(B^\alpha \cdot \beta^q \cdot D^\ell)^{-1}$ such that $h(1) = i$, $h(4) = j$ and $h(3) = k$. This shows G is triply transitive on $\{1, 2, 3, 4, 5, 6\}$. (Hint: Run the algorithm in part (5) in reverse.)

7. With the notation of part (5), the element $B^\alpha \cdot \beta^q \cdot D^\ell \cdot h$ is in the subgroup H of G which leaves each of 1, 4 and 3 fixed. Define the following subset T of G:

$$T = \{D^{-\ell} \cdot \beta^{-q} \cdot B^{-\alpha} : 0 \leq \ell \leq 5, 0 \leq q \leq 4, 0 \leq \alpha \leq 3\} \tag{0.1}$$

Show that T contains $A = (1, 2, 3, 4)$ and that T has exactly 120 elements. Assuming that T is a group, show that H is trivial and $G = T$. (Proving that T is a group is an extra credit problem below.)

Hints: Part (5) is really an algorithm for producing ℓ, q and α for a given h. Apply this algorithm to $h = A = (1, 2, 3, 4)$ and check that in fact, A is exactly equal to the resulting $D^{-\ell} \cdot \beta^{-q} \cdot B^{-\alpha}$. To count the number of elements of T, it is enough to show that

$$D^{-\ell} \cdot \beta^{-q} \cdot B^{-\alpha} = D^{-\ell'} \cdot \beta^{-q'} \cdot B^{-\alpha'} \tag{0.2}$$

implies $D^{-\ell} = D^{-\ell'}$, $\beta^{-q} = \beta^{-q'}$ and $B^{-\alpha} = B^{-\alpha'}$. To check this, first consider where each side of (0.2) sends 1 in order to prove $D^{-\ell} = D^{-\ell'}$. Then multiply each side by $D^\ell = D^{\ell'}$ and consider where the results send 4, etc.)

8. Show that G is not contained in the stabilizer of any element of $\{1, 2, 3, 4, 5, 6\}$. Since $\#S_6 = 720 = 6 \cdot \#G$, the set S_6/G of left cosets gG of G in S_6 has 6 elements. Let S_6 act on these cosets on the left. Show that this gives an isomorphism $\tau : S_6 \to \mathrm{Perm}(S_6/G)$ which sends G isomorphically to the subgroup of $\mathrm{Perm}(S_6/G)$ which fixes the coset G. You can use without proof the fact that any homomorphism from S_6 to another group is either injective or has image of order 1 or 2; we are going to prove this later when we consider simple groups. Conclude that τ gives an isomorphism between G and S_5.

9. Label the cosets S_6/G by $\{1, 2, 3, 4, 5, 6\}$ in some way, and identify $\mathrm{Perm}(S_6/G)$ with S_6 by this labeling. Show the isomorphism τ in part (8) cannot be an inner automorphsm, i.e. there is no element $\sigma \in S_6$ such that $\tau(g) = \sigma g \sigma^{-1}$ for all $g \in S_6$. Thus τ is an outer automorphism of S_6. It is remarkable that the existence of this outer automorphism can be proved using a Rubik's cube! (Hint: Show that if τ were an inner automorphism, then the fact that $\tau(G)$ fixes some element of S_6/G would imply that G has to fix some element of $\{1, \ldots, 6\}$, which is not true.)

1. Extra Credit Problems

10. Show that the set T defined in (0.1) is a group.

Hints: First show that the elements β and B generate a group Γ of order 20 in which β generates a normal 5-Sylow subgroup. For this it is enough to show that $B\beta B^{-1}$ is a power of β. Argue that this proves T is taken to itself by multiplication on the right by either β or B. Show that to prove T is a group, it is then enough to show that right multiplication by D takes T to itself. To show this reduce to checking that for $i \in \{1, 2, 3, 4, 5\}$ and $g \in \{\beta, B\}$, there is an integer $j(i, g)$ and an element $g' \in \Gamma$ such that $gD^i = D^{j(i,g)}g'$. To find $j(i, g)$

and g', you need to use the algorithm discussed in Problem 7 a total of 10 times, each time checking that you indeed get a g' in Γ.)

11. Show that the allowed rotations of all the faces of a Rubik's cube generate the full permutation group S_8 of the corners of the cube.

    Hints: First argue that it is enough to prove that if we allow rotations about all of the faces, we can produce an arbitrary permutation vertices numbered $1, 2, 3, 4, 5, 6$ while holding the remaining two vertices 7 and 8 fixed. Problem #7 shows that if we only allow rotations about the two faces containing vertices $1, 2, 3, 4, 5, 6$ we can only achieve the permutations in the group G. Show that if we allow rotations about all of the faces, we can find a permutation σ which fixes each of 7 and 8 and whose actions on the vertices $\{1, 2, 3, 4, 5, 6\}$ is not in G. One way to come up with such a σ is described on pages 13 and 14 of https://math.berkeley.edu/~hutching/rubik.pdf ; it is useful to know that the group H in problem #7 is trivial. To finish the argument using G and σ, you can use that the only normal subgroups of S_6 are $\{e\}$, A_6 and S_6.