Math 462: Homework 8 solutions

Paul Hacking

4/25/10

1. What is the largest possible order of an element of the symmetric group S_9? What is the largest possible order of an element of the alternating group A_6? [Hint: What are the possible cycle types?]

Recall that the cycle type of an element of S_n is a sequence $(l_1, \ldots, l_r)$ of cycle lengths such that $l_1 + l_2 + \cdots + l_r \leq n$ (remember that we omit cycles of length 1 in the notation). We may assume the cycles are arranged in order of increasing length, so $l_1 \leq l_2 \leq \cdots \leq l_r$. The order of an element of cycle type $(l_1, \ldots, l_r)$ is the lowest common multiple $\operatorname{lcm}(l_1, \ldots, l_r)$ of the cycle lengths. Now we can compute for S_9 as follows. If $r = 1$ the maximum order is 9 (corresponding to a single 9-cycle). If $r = 2$ and $l_1 = 2$ then the maximum order is $14 = 2 \cdot 7$ for cycle type $(2, 7)$. If $r = 2$ and $l_1 = 3$ then the maximum order is $3 \cdot 5 = 15$ for cycle type $(3, 5)$. (Note: this is larger than the order $6 = \operatorname{lcm}(3, 6)$ of cycle type $(3, 6)$ because 3 and 6 have a common factor.) If $r = 2$ and $l_1 = 4$ then the maximum order is $4 \cdot 5 = 20$ for cycle type $(4, 5)$. If $r \geq 3$ then we find that some pair of the l_i have a common factor. It follows that these cycle types cannot have maximal order. Combining our results we see that the maximum order is 20, given by cycle type $(4, 5)$.

Recall that A_n is the the subgroup of S_n consisting of even permutations, that is, permutations that can be expressed as a product of an even number of transpositions. If a permutation has cycle type $(l_1, \ldots, l_r)$ then it can be expressed as a product of $\sum_{i=1}^{r}(l_i - 1)$ of transpositions. So the cycle types occurring in A_n are those for which $\sum_{i=1}^{r}(l_i - 1)$ is even. For A_6 we can now compute in a similar way to above. If $r = 1$ the maximum order is 5 corresponding to a single 5-cycle. (Note that a single 6-cycle is not an even permutation.) If $r = 2$ then the possible cycle types are $(2, 4)$, $(2, 2)$, and $(3, 3)$, with maximum order $4 = \operatorname{lcm}(2, 4)$. There are no cycle types with $r \geq 3$. So we see that the maximum order is 5, given by a single 5-cycle.

2. A card dealer shuffles a pack of $2n$ cards as follows: He first divides the pack into 2 halves consisting of n cards each. He then interleaves the cards so that the new top card is the top card from the bottom half, the new second card is the top card from the top half, the new third card is the second card from the bottom half, the new fourth card is the second card from the top half, and so on.

(a) Number the positions of the cards in the deck $1, 2, \ldots, 2n$, starting at the top, and consider the permutation f of $\{1, 2, \ldots, 2n\}$ corresponding to the shuffle. Express f as a composite of disjoint cycles for $n = 4$ and $n = 5$. What is the order of f in each case? (In other words, how many shuffles are required before the cards return to their original positions?)

(b) Check the following: when one such shuffle is performed, the card originally in position j is moved to position $2j \bmod (2n + 1)$.

(c) Using part (b), show that the order of the shuffle permutation is the least number k such that $2^k \equiv 1 \bmod (2n + 1)$.

(d) Now find the order of the shuffle for an ordinary pack of cards (52 cards in the deck). [Hint: Fermat's little theorem asserts that $a^{p-1} \equiv 1 \bmod p$ for p a prime and a a number not divisible by p.]

(a) $f = (124875)(36)$ for $n = 4$, of order 6. $f = (1, 2, 4, 8, 5, 10, 9, 7, 3, 6)$ for $n = 5$, of order 10.

(b) If $j \leq n$, then the card in position j is moved to position $2j$. If $j > n$, then the card in position j is moved to position $2(j - n) - 1 = 2j - (2n + 1)$. In both cases, the final position is given by $2j \bmod (2n + 1)$.

(c) Applying the shuffle permutation k times gives the permutation $j \mapsto 2^k j \bmod (2n + 1)$ (by part (b)). This is the identity permutation if $2^k j \equiv j \bmod (2n+1)$ for each j. This is equivalent to $2^k \equiv 1 \bmod (2n+1)$. So the order of the shuffle permutation is the least positive integer k such that $2^k \equiv 1 \bmod (2n + 1)$.

(d) If there are 52 cards in the deck then $2n = 52$ so $n = 26$. By part (c) we need to find the least number k such that $2^k \equiv 1 \bmod 53$. Notice that 53 is prime so by Fermat's little theorem $2^{52} \equiv 1 \bmod 53$. So the least number k such that $2^k \equiv 1 \bmod 53$ must divide 52. The prime factorization of 52 is $52 = 2^2 \cdot 13$ so the numbers dividing 52 are $1, 2, 4, 13, 26$ and 52. We check that 2^4 and 2^{26} are not congruent to 1 modulo 53. So $k = 52$.

3. In class we showed that the group G of symmetries of the cube can be identified with $S_4 \times \{\pm 1\}$. The identification is given by associating to a symmetry $g \in G$ the induced permutation of the 4 interior diagonals of the cube together with its determinant $\det(g)$. (Here we choose coordinates so the center of the cube is at the origin. Then $g(\mathbf{x}) = A\mathbf{x}$ for some 3×3 orthogonal matrix A, and $\det(g) := \det(A)$.)

(a) For each cycle type of permutation in S_4, describe the corresponding *direct* symmetries ($\det(g) = +1$) geometrically.

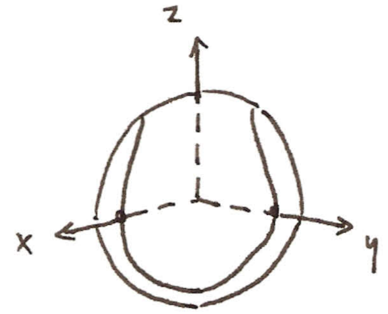
(b) For each cycle type of permutation in S_4, describe the corresponding *opposite* symmetries ($\det(g) = -1$) geometrically.

(a) The cycle types of S_4 are (2), (3), (4), $(2,2)$, and the identity. A 2-cycle corresponds to a rotation through π about the axis joining the midpoints of two opposite edges of the cube. A 3-cycle corresponds to a rotation through $2\pi/3$ about the axis joining two opposite vertices of the cube. A 4-cycle corresponds to a rotation through $\pi/2$ about the axis joining the centers of two opposite faces of the cube. The cycle type $(2,2)$ corresponds to a rotation through π about the axis joining the centers of two opposite faces of the cube.

(b) A 2-cycle corresponds to reflection in the plane containing two opposite edges of the cube. A 3-cycle corresponds to a rotary reflection given by rotation by $\pi/3$ about the axis joining two opposite vertices of the cube followed by reflection in the plane normal to this axis. A 4-cycle corresponds to a rotary reflection given by rotation by $\pi/2$ about the axis joining the centers of two opposite faces of the cube followed by reflection in the plane normal to this axis. The cycle type $(2,2)$ corresponds to reflection in the plane through the origin parallel to two opposite faces of the cube. The identity corresponds to the symmetry $T(\mathbf{x}) = -\mathbf{x}$ we discussed in class and in HW7 Q1. Geometrically it is a rotary reflection given by rotation by π about the axis joining the centers of two opposite faces of the cube followed by reflection in the plane normal to this axis. (In fact as we discussed earlier the choice of axis in this case is irrelevant: we can take the axis to be any line through the center of the cube.)

4. Describe the group G of symmetries of a baseball, taking into account the stitching. [Hint: It may be easiest to first consider the rotational symmetries.]

The rotational (direct) symmetries are the identity together with rotations by π about each of 3 orthogonal axes (see picture). We choose coordinates as shown so that these axes are the coordinate axes. The opposite symmetries are given by the reflections in the planes $(y = x)$ and $(y = -x)$ and rotary reflection about the z-axis through angle $\pm\pi/2$. It is a good idea to check that $|G| = 8$ using the orbit-stabilizer theorem to see that we have accounted for all of the symmetries.

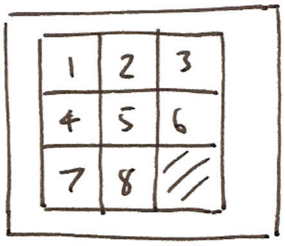


5. In class we showed that a finite subgroup of rotations in $\mathbb{R}^3$ is either a cyclic group $C_n = \mathbb{Z}/n\mathbb{Z}$, a dihedral group D_n, or the group of rotational symmetries of a regular polyhedron (tetrahedron, cube / octahedron, or dodecahedron / icosahedron). Give examples of polyhedra whose groups of rotational symmetries are C_n and D_n, for each integer $n \geq 3$.

A pyramid (HW5 Q3a) with base a regular n-gon has group of rotational symmetries C_n. (Note: In the case $n = 3$ we need to ensure that the pyramid is not a regular tetrahedron, otherwise there are additional symmetries. We can do this by choosing the height of the pyramid to be different from that of the tetrahedron.)

A prism (HW5 Q3b) with base a regular n-gon has group of rotational symmetries D_n. (Note: Again, if $n = 4$, we need to ensure that the prism is not a cube, and we can do this by choosing the height to be different from that of the cube.)

6. (This question is optional and is harder than the others). We are going to study the game pictured below (you have probably seen it before). The 8 tiles can be moved around by repeatedly sliding a tile into the empty space. Now consider the permutations of the 8 tiles that can be obtained by a sequence of moves of this type, such that at the end of the sequence the empty space is again at the bottom right. These permutations form a subgroup of the symmetric group S_8. What is this subgroup?



The subgroup is the alternating subgroup $A_8 \subset S_8$. The solution for a 4×4 grid is explained in Reid and Szendroi, p. 100. The same proof works in the 3×3 case.