From Mathematics to Generic Programming

Brooks Mershon

April 2017

11.1

Solution.

Recall from exercise 6.6 that we can represent the group of nonzero remainders modulo 7 in a table:

	1	**2**	**3**	**4**	**5**	**6**	*order*
1	1	2	3	4	5	6	1
2	2	4	6	1	5	5	3
3	3	6	2	5	1	4	6
4	4	1	5	2	6	3	3
5	5	3	1	6	4	2	6
6	6	5	4	3	2	1	2

This table provides a hint as to how we might prove that every element g of some finite group G with n elements is isomorphic to some element s in S_n. Looking at each row of the table, we see a *permutation* of the elements of G.

It just so happens that this particular group G was based on the set of elements $\{1, 2, 3, 4, 5, 6\}$. Multiplying 3 (row) by 1 (column) yields 3; multiplying 3 (row) by 4 (column) yields 5. Said another way, we see that the particular element 3, when multiplied on the left by the elements specified in the column header of the table, yields the value found in the cell; that is, 3 *permutes* the set $\{1, 2, 3, 4, 5, 6\}$, thereby producing the *permutation* $\{3, 6, 2, 5, 1, 4\}$. For each row of this table, we can associate with the row a permutation that it induces in the fixed set $\{1, 2, 3, 4, 5, 6\}$. The elements of G, therefore, can be put in one-to-one correspondence with some permutation of the elements of G.

Now, the fixed set $\{1, 2, 3, 4, 5, 6\}$ that we referred to happened to be the underlying set for our group under consideration, but we could also choose to simply assign a number to each element of a group after lining the elements up in an arbitrary order. For the nonzero remainders modulo 7, the order was straightforward: number the *number* the same. But by ordering any group element in a similar manner as to what is seen in the above table and noting the indices to which left multiplication of the given row by the given column causes the elements of G to move (the number assigned to each element g_i might be considered it's position), we can generate a permutation in S_n all the same.

Each permutation we assign to g describes the way g affects each group member (including itself). *Naturally, one of the group members (the identity element) will be assigned the identity (do nothing) permutation.*

Therefore, all elements of a group of finite order n can be put into one-to-one correspondence with elements forming a subgroup of the symmetric group S_n.