MATH 31 – HOMEWORK 4 SOLUTIONS!

due Wednesday, July 26

Instructions: This assignment is due at the *beginning* of class. Staple your work together (do not just fold over the corner). Please write the questions in the correct order. If I cannot read your handwriting, you won't receive full credit.

1. (8.4 and 8.10) *(8 points)*

   (a) *(3 points)* Let $\pi = (\ x_1\ x_2\ \cdots\ x_r\ ) \in S_n$. Show that $o(\pi) = r$. (Note: this means implicitly that all the x_i are different.)

   Proof: This question asks us to show that if a permutation π of length n consists of a single cycle of length r (an "r-cycle") for short, and the rest of the elements are in 1-cycles, then π has order r.

   Let $\pi = (\ x_1\ x_2\ \cdots\ x_r\ )$. So, π sends x_1 to x_2, sends x_2 to x_3, and more generally sends x_i to x_{i+1} if $i < r$, and sends x_r to x_1.

   Define $[i]$ to mean the number between 1 and r that is the equivalent to i modulo r. For example, $[3] = 3$ and also $[r+3] = 3$ This allows us to simply the previous paragraph, and simply say that π always sends x_i to $x_{[i+1]}$.

   Now, what does π^2 do? Remember that π^2 is the composition of π with itself. Since π sends x_1 to x_2 and sends x_2 to x_3, we see that π^2 sends x_1 to x_3. Similarly, π^2 sends x_2 to x_4, and more generally it sends x_i to $x_{[i+2]}$.

   What does π^3 do? By the same logic, π^3 sends x_i to $x_{[i+3]}$ for all i.

   We've now convinced ourselves that π^k is a permutation that sends x_i to $x_{[i+k]}$. If $k < r$ then x_1, for example, is always being sent to x_{1+k} which does not equal x_1 itself. Thus, if $k < r$ then π^k is not the identity. On the flip side, π^r is the permutation that sends x_i to $x_{[i+r]}$, but since $[i+r] = i$, this proves that π^r is identity.

   Hence, we have proved that $o(\pi) = r$. □

   (b) *(3 points)* Suppose that a permutation π is the product of disjoint cycles $\pi_1, \pi_2, \ldots, \pi_m$. Show that $o(\pi)$ is the least common multiple of $\{o(\pi_1), o(\pi_2), \ldots, o(\pi_m)\}$.

   Proof: Let π be a permutation that is a product of disjoint cycles $\pi_1, \pi_2, \ldots, \pi_m$. Recall that disjoint cycles commute, because the elements moved by each one are not moved by the other. So, a power of π can be written as

   $$\pi^k = (\pi_1)^k (\pi_2)^k \cdots (\pi_m)^k.$$

   The order of π is the smallest positive integer k such that π^k is the identity.

   Define $N = \text{lcm}(o(\pi_1), o(\pi_2), \ldots, o(\pi_m))$.

   Claim: The order of π is N.

   Proof of claim: We'll show this in two steps. First we'll show that π^N is the identity, and then we'll verify that π^ℓ is not the identity for all $1 \leq \ell < N$.

   For the first part, we simply need to note that

   $$\pi^N = (\pi_1)^N (\pi_2)^N \cdots (\pi_m)^N.$$

Since N is the least common multiple of the orders of the π_i, N is evenly divisible by all π_i. Thus $(\pi_i)^N$ is the identity for all i and hence so is π^N.

Now we must check that π^ℓ is not the identity when $1 \leq \ell < N$. By the definition of least common multiple, if ℓ is a positive integer less than N, then it must not be divisible by the order of at least one of the π_i. This means it's not possible that $(\pi_i)^\ell$ is the identity, and so neither is π^ℓ. The claim is now proved. □

(c) *(2 points)* Find the order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 7 & 5 & 9 & 8 & 4 & 11 & 3 & 1 & 12 & 2 & 10 \end{pmatrix}$$

in S_{12}.

Solution: Part (b) makes this easy. First convert to cycle notation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 7 & 5 & 9 & 8 & 4 & 11 & 3 & 1 & 12 & 2 & 10 \end{pmatrix} = (\,1\,6\,4\,9\,)(\,2\,7\,11\,)(\,3\,5\,8\,)(\,10\,12\,)$$

The orders of the cycles are $4, 3, 3, 2$, and the least common multiple of these is 12. So, by part (b) that is the order of this permutation. **Note:** The fact that this order came out to be 12 isn't because the group is S_{12}. This group has elements with many different orders.

---

2. *(4 points)* (8.12) Does A_6 have an element of order 6? Does A_7?

Solution: The group A_6 does not have an element of order 6, but the group A_7 does. Question 1 is very helpful in proving this.

First, let's point something out that will save us some time down the road. Let $\pi = (\,x_1\ x_2\ \cdots\ x_r\,)$ be a permutation that is just a single nontrivial cycle, plus some fixed entries (like in part (a)). We don't need to write out π as a product of transpositions to figure out if it is even or odd. We know that one way to write it as a product of transpositions is

$$(\,x_1\ x_r\,)\cdots(\,x_1\ x_3\,)(\,x_1\ x_2\,),$$

which is a product containing $r-1$ terms. So, we now know, for the rest of time, that a cycle with an even number of entries is an odd permutation and a cycle with an odd number of entries is an even permutation.

Moreover, if π is a product of disjoint cycles, we can determine if π is even or odd by looking at its cycles. Just like regular addition of integers, the product of two even or two odd permutations is even, and the product of one even and one odd permutation is odd. Think of it this way: if $\pi = \pi_1\pi_2$, where π_1 and π_2 are disjoint cycles, then one way to write π as a product of transpositions is to do it for π_1 and π_2 separately, then join the results together. If π_1 is written as the product of T_1 transpositions and π_2 is written as the product of T_2 transpositions, then π is written as the product of $T_1 + T_2$ transpositions. So, my claim at the beginning of this paragraph follows.

Now we are ready to answer the question. What kinds of permutations in S_6 could have order 6? By Question 1, part (b), such a permutation must be in one of the two forms:

(i) A single 6-cycle,

(ii) A 2-cycle and a 3-cycle.

This is because the only ways to make a list of numbers that adds up to at most 6 and has least common multiple 6 are $\{6\}$ and $\{2, 3\}$.

This is a problem, because our prelude to this answer shows that a permutation that is a single 6-cycle is odd, and a permutation that is a 2-cycle and a 3-cycle is the product of an odd and an even permutation, and is also odd. By definition, A_6 is the subgroup of even permutations, so A_6 can have no permutation of order 6.

On the other hand, A_7 does have allowable cycle structures that produce even permutations of order 6. In particular, any permutation of the form

$$(\ a\ b\ )(\ c\ d\ )(\ e\ f\ g\ )$$

is even because it is the product of two odd permutations and an even permutation and has order 6 because the least common multiple of $\{2, 2, 3\}$ is 6.

---

3. *(4 points)* Find the right cosets of the subgroup $H = \langle(1,1)\rangle$ in $\mathbb{Z}_4 \times \mathbb{Z}_4$.

   Solution: The right cosets of $H = \langle(1,1)\rangle$ in $\mathbb{Z}_4 \times \mathbb{Z}_4$ are all the sets of the form Ha, for $a \in \mathbb{Z}_4 \times \mathbb{Z}_4$. Since we're operating within a group whose operation is addition, it's preferable to write $H + a$ rather than Ha.

   Recall that by definition

   $$H + a = \{h + a : h \in H\},$$

   in other words, it's the set formed by taking everything in H and "translating" it by a. Since $|\mathbb{Z}_4 \times \mathbb{Z}_4| = 16$, there are at first glance 16 different possibilities for $H + a$, but actually many of them are the same.

   Recall that for cosets in general $Ha = Hb$ if and only if $ab^{-1} \in H$. In additive notation, $H + a = H + b$ if and only if $a - b \in H$.

   Let us point out that

   $$H = \{(0,0), (1,1), (2,2), (3,3)\}$$

   and begin to construct cosets.

   The first coset is just H itself, or more precisely $H + (0,0)$. This is the same coset as $H + (1,1)$, $H + (2,2)$, and $H + (3,3)$.

   Now consider $H + (1,0) = \{(1,0), (2,1), (3,2), (0,3)\}$. This is the same coset as $H + (2,1)$, $H + (3,2)$, and $H + (0,3)$.

   Next up let's look at $H + (0,1) = \{(0,1), (1,2), (2,3), (3,0)\}$. this is the same coset as $H + (1,2)$, $H + (2,3)$, and $H + (3,0)$.

   So far we have accounted for 12 elements out of the 16 total elements in $\mathbb{Z}_4 \times \mathbb{Z}_4$. Since we haven't found $(2,0)$ yet, let us consider $H + (2,0) = \{(2,0), (3,1), (0,2), (1,3)\}$.

   Now, as all 16 elements are accounted four, we have found the for distinct cosets:

   $$H + (0,0),$$
   $$H + (1,0),$$
   $$H + (0,1),$$
   $$H + (2,0).$$

---

4. *(4 points)* (9.13) Suppose G is a group and A and B are subgroups of G. Define a relation R on G by

   $$x\ R\ y \text{ if and only if there exist } a \in A \text{ and } b \in B \text{ such that } x = ayb.$$

   Prove that R is an equivalence relation on G.

   Solution: To prove that R is an equivalence relation, we need to prove that it is reflexive, symmetric, and transitive.

   To prove that R is reflexive, we must check that $x\ R\ x$ for all $x \in G$. This is certainly true because we can pick $a = e$ and $b = e$, and now $x = axb$.

To prove that R is symmetric, we must check that for all $x, y \in G$, if $x\,R\,y$ then $y\,R\,x$. (Note: The condition for symmetry is really an if and only if, but since x and y are chosen arbitrarily, this takes care of both directions at once.)

Assume that $x\,R\,y$. This implies that there exist two elements, which we'll call α and β, such that $x = \alpha y \beta$. It follows that $y = \alpha^{-1} x \beta^{-1}$. This means that the criterion for $y\,R\,x$ is satisfied with $a = \alpha^{-1}$ and $b = \beta - 1$. Therefore R is symmetric.

Lastly we need to prove transitivity. To do this, we prove that if $x\,R\,y$ and $y\,R\,z$, then it must follow that $x\,R\,z$. To this end, let us assume that $x\,R\,y$ and $y\,R\,z$. This implies that there exist $\alpha, \beta, \gamma, \delta \in G$ such that

$$x = \alpha y \beta \qquad \text{and} \qquad y = \gamma z \delta.$$

Taken together, these two equations imply

$$x = (\alpha\gamma) z (\beta\delta).$$

So, with $a = \alpha\gamma$ and $b = \beta\delta$, we see that the condition is satisfied and $x\,R\,z$.

As we have confirmed that R is reflexive, symmetric, and transitive, we can conclude that R is an equivalence relation. □