Math Circle Worksheet
The Symmetric Group

Wesley Hamilton

2/18/2017

1 General Group Theory

Remember that a group was defined as a set together with some operation, that satisfied a few extra properties.

1. Is $(\{0,1\},\times)$ a group? Here the group operation is multiplication.
2. What about $(\{-1,1\},\times)$? Is this a group?
3. Now let $(G,\cdot)$ be any group, i.e. not necessarily any of the groups we've worked with up till now. Suppose G has two identity elements e and e', so that for any a in G we have

$$a \cdot e = e \cdot a = a,$$
$$a \cdot e' = e' \cdot a = a.$$

   Must $e = e'$? Why or why not?

4. For the same $(G,\cdot)$, suppose a group element a has two inverses, which we'll call b and c. In other words,

$$a \cdot b = b \cdot a = e,$$
$$a \cdot c = c \cdot a = e.$$

   Must $b = c$? Why or why not?

We say a group is **abelian** or **commutative** if the order in which we combine group elements doesn't matter, i.e. $a \cdot b = b \cdot a$ for every a and b in G.

5. *The groups we saw last week ($(\mathbb{Z},+), (\mathbb{Q},+), (\mathbb{Q}^*,\times), (\mathbb{Z}_n,+)$, the One-Sock group) were all abelian. For each of those groups, briefly think of or say why it was abelian.
6. *Let $(G,\cdot)$ be any group, and suppose $a \cdot a = e$ for every a in G. Show that $(G,\cdot)$ is abelian. (This also tells us right away that the One-Sock Group is abelian (why?).)

2 The Symmetric Group

Remember that if we have a collection of n objects, say the integers $\{1, 2, ..., n\}$, the *permutations* of this set are all the invertible maps on this set. Hopefully an example makes this notion clearer:

Consider the set $\{1, 2, 3\}$, and the map σ which sends $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. Another way of writing this is $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$, or we can tabulate this as

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

We have another permutation on the same set that we can call τ, which sends $1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2$. As above, τ can also be written as

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

An example of something that isn't a permutation is the map ρ, which sends $1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 1$, also written

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \end{pmatrix}.$$

7. Verify that σ and τ are both permutations. In other words, what is the inverse map for each of these permutations?

8. Why isn't ρ a permutation?

The two-layer notation is a bit cumbersome to write, so often times we'll write these permutations in *cycle notation*. This amounts to finding each of the "closed loops" of the permutation, and writing the elements in the order they appear. Also, if a permutation doesn't do anything to an object (or number) then we omit that number from the cycle notation. For example, σ sends 1 to 2, so we write (12. Next, 2 gets sent to 3, so we include 3 in that cycle, giving (123. Since 3 gets sent back to 1, which is already included in the cycle, we close the bracket, resulting in (123). In this way, we associate the permutation σ with the cycle (123).

9. What is the cycle decomposition for $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$?

As another example, consider the permutation of the set $\{1, 2, 3, 4, 5, 6\}$ given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}.$$

We start by finding the cycle containing 1: since 1 gets sent to 3, we can start writing (13. Then 3 goes to 4, and 4 goes to 6, so including these two in our cycle gives (1346. Notice that we still haven't found a closed loop, so we need to look at where 6 goes. Luckily, 6 gets mapped to 1, and we close up the cycle: (1346).

10. The cycle we found doesn't correspond to the permutation completely. What's missing?

11. Find the missing component.

Using the cycle decomposition notation makes writing permutations much easier. For example, instead of writing out the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 8 & 7 \end{pmatrix},$$

we can just write (78).

So far we've been working with a single permutation (or cycle) "applied" to a set just once. But what happens if we keep iterating the same cycle over and over?

12. What is the cycle $(1624)^2 = (1624)(1624)$? In other words, how would you write this as a single cycle?

13. What about the cycle $(1624)^{-1}$? Remember that $(1624)^{-1}$ is the inverse to the cycle (1624), i.e. $(1624)^{-1}(1624) = (1624)(1624)^{-1} = 1$, the identity.

14. How would you write $(1624)^3$ as a cycle?

15. Now what about the permutation $[(16273)(458)]^4$?

16. *For the general case, consider a cycle $\sigma = (i_1 i_2 ... i_k)$, where $i_1, ..., i_k$ can be any integer. What is σ^l, where l is some positive integer?

17. *Suppose, using the same σ and l, we have $\sigma^l = 1$, the identity permutation. What relation is there between l and k?

18. *What if we now have $\sigma = \sigma_1 \cdots \sigma_n$, where each permutation $\sigma_j = (i_{1_j} ... i_{k_j})$ is a cycle, and all of the σ_j are disjoint (take a minute to think and make sure you understand the set-up)? What would σ^l be? If $\sigma^l = 1$, how must l and each of the integers i_{k_j} (running over the index j) relate?

In some sense *transpositions* (permutations that only switch two elements of the set, cycles of length two, etc.) are the simplest permutations out there. A good question is: can every cycle be written as a product of transpositions?

19. We can write (132) as (32)(21). Check that each permutation (the 3-cycle and two transpositions) behave the same way. How would you write (123) as a product of transpositions?

20. How would you write (4268) as a product of transpositions? (There may be multiple ways.)

21. If we can write a single cycle (like (132), for example) as a product of transpositions, then the transpositions cannot be disjoint. In other words, two or more of the transpositions must move the same set element. Why is this the case?

22. One of the possible ways of writing (4268) is (42)(26)(68). What do you notice about each of the transpositions?

23. *Suppose we don't know what the actual integers in the cycle are, say $\sigma = (i_1...i_k)$, where each i_j, $1 \leq j \leq k$ is some integer. Using the idea from the last question, how would you write σ as a product of transpositions?

24. Consider now the permutation (37). How would you write this permutation as a product of adjacent transpositions? In other words, how would you write (37) only using the transpositions $(34), (45), (56), (67)$?

25. *Generalize the last problem to the transposition (ab), where a and b are integers with $a < b$.

If transpositions are the building blocks for permutations, then certainly *adjacent transpositions* (transpositions involving integers next to each other) are the atomic building blocks. With this in mind, we can write any permutation as a product of adjacent transpositions.

26. Recall that (4625) = (42)(26)(68). How would you write (4625) as a product of adjacent transpositions?

27. *Generalize this to the cycle $\sigma = (i_1...i_k)$, i.e. write the cycle σ as a product of adjacent transpositions.

Another possibility is to write the permutation as a product of (not-necessarily adjacent) transpositions, where each transposition moves a common elements. For example, earlier we wrote (132) as (13)(32), but we could also have written (132) as (12)(13).

28. Verify that (132) and (12)(13) are indeed the same permutation.

29. How would you express the permutation (528397) in this way, i.e. as a product $(5i_1)(5i_2)...(5i_k)$? What should the i_j be?

30. *Now consider the general case: how would you express $\sigma = (i_1...i_k)$ as a product of transpositions, where each transposition acts on a common element?

The final topic we'll talk about is the *parity* of a permutation. Roughly speaking, the parity p of a cycle σ is

$$p(\sigma) = (-1)^{\text{length of } \sigma + 1}.$$

If we have a permutation that is a product of cycles, say $\sigma = \sigma_1 \cdots \sigma_k$, then we define

$$p(\sigma) = p(\sigma_1 \cdots \sigma_k) = p(\sigma_1) \cdots p(\sigma_k).$$

In other words, the parity of a product of permutations is the product of the parities.

Some examples:

$$\begin{aligned} p((12)) &= (-1)^{2+1} = -1, \\ p((132)) &= (-1)^{3+1} = 1, \\ p((13)(12)) &= p((13))p((12)) = (-1) \cdot (-1) = 1. \end{aligned}$$

31. Notice that $(132) = (13)(32)$, and $p(132) = p((13)(12))$. This suggests that the parity of a permutation doesn't depend on how we write the permutation. Do you think this is actually the case? Why or why not?

32. If you multiply a permutation with parity 1 by a permutation of parity -1, what will the parity of the resulting permutation be?

33. Do the parity 1 permutations form a group? Why or why not? What about the parity -1 permutations?

3 The 15-Puzzle

Consider the 15-puzzle, where you have a 4×4 grid of the numbers $1, 2, ..., 15$, and the bottom right corner is empty. The goal of the puzzle is to, by sliding tiles into the empty square, transform the original configuration into the neutral configuration. A natural question (we'll call this the **important question**) is if any starting position can be transformed into the neutral configuration, and the symmetric group gives us a nice, easy answer (no, not every configuration can be).

To start, we'll play around with a few easy examples involving a simpler board: a 2×2 grid with the bottom right corner removed.

34. Suppose the 1-tile is in the 2-tile place, the 2-tile is in the 3-tile place, and the 3-tile is in the 1-tile place. Note that this corresponds to a permutation (123). Is this puzzle solvable?

35. What about the board corresponding to the permutation (132)? Is this board solvable?

36. Finally, what about the board corresponding to the transposition (12)? Is this board solvable? Why or why not?

As you solve the, say, 15-puzzle, notice that the empty square travels around the board (up and away from its starting position). One important step in our efforts to answer the **important question** is to label the empty square 16.

37. How would you express, using cycle notation, the trip the empty cell takes around our 15-puzzle grid? In other words, what permutation represents sliding a tile into the empty slot?

Instead of starting with an attainable board and trying to slide tiles around to get it to the neutral board, we could also start with the neutral board, slide the tiles around, and arrive at an attainable board.

38. If you want to make an attainable board from the neutral board, you can take successive transpositions of the empty tile with an adjacent square. In other words, you'll start constructing a permutation that looks like $\cdots(16\,11)(16\,15)$. Why?

39. If after the empty (16-)tile slides around, where does it need to end up for the board to be an attainable board? What does the corresponding permutation look like?

40. What is the parity of this permutation?