Modern Algebra HW3

Michael Nameika

September 2022

Section 6 Problems

17. Find the number of elements in the cyclic subgroup of $\mathbb{Z}_{30}$ generated by 25.

Recall that a cyclic subgroup of G generated by some element $a \in G$ is given by

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$$

where we let $a^0 = e$ and $a^{-m} = (a^{-1})^m$ where a^{-1} denotes the inverse of a and m is some natural number. In our case, $a = 25$ and the operation is addition modulo 30. Let's begin by listing the elements:

$$a^1 = 25$$

$$a^2 = 25 +_{30} 25 = 20$$
$$a^3 = a^2 a = 20 +_{30} 25 = 15$$
$$a^4 = a^3 a = 15 +_{30} 25 = 10$$
$$a^5 = a^4 a = 10 +_{30} 25 = 5$$
$$a^6 = a^5 a = 5 +_{30} 25 = 0$$

That is, $a^6 = a^0 = e$. We can see then that the subgroup generated by 25 contains 6 elements.

20. Find the number of elements in the cyclic subgroup of $\mathbb{C}^*$ of Exercise 19 generated by $\frac{1+i}{\sqrt{2}}$

I claim that this subgroup contains 8 elements since it is the set of the eighth roots of unity. Let's verify. Let $a = \frac{1+i}{\sqrt{2}}$ and notice

$$a^1 = a = \frac{1+i}{\sqrt{2}}$$

$$a^2 = \left(\frac{1+i}{\sqrt{2}}\right)^2 = i$$

$$a^3 = a^2 a = i\left(\frac{1+i}{\sqrt{2}}\right) = -\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$$

$$a^4 = a^3 a = \left(-\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = -1$$

$$a^5 = a^4 a = -1\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = -\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}} = -a$$

$$a^6 = a^5 a = -a^2 = -i$$

$$a^7 = a^6 a = -a^2 a = -a^3 = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$$

$$a^8 = a^7 a = -a^3 a = -a^4 = 1$$

So we can see that this subgroup has 8 elements.

Section 8 Problems

For this section, let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} \qquad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$$

5. Compute $\sigma^{-1}\tau\sigma$.

Notice that $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 4 & 5 \end{pmatrix}$. This can be found by simply swapping the rows in σ and sorting the columns in ascending order based on the element in the first row. That is, we are reversing the operation of σ. Now, let's compute $\tau\sigma$:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$$

and finally $\sigma^{-1}\tau\sigma$:

$$\sigma^{-1}\tau\sigma = \sigma^{-1}(\tau\sigma)$$

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

so

$$\sigma^{-1}\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$$

8. Compute the following expression: σ^{100}

To begin, let us first find the order of the cyclic subgroup of S_6 generated by σ. That is, we wish to find the smallest integer power n such that $\sigma^n = e$. Well,

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 2 & 1 \end{pmatrix}$$

$$\sigma^3 = \sigma^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix}$$

$$\sigma^4 = \sigma^3\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\sigma^5 = \sigma^4\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 4 & 5 \end{pmatrix}$$

$$\sigma^6 = \sigma^5\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = e$$

So $n = 6$. That is, $|\langle\sigma\rangle| = 6$.

Now, we can compute σ^{100}. As in the division algorithm, notice

$$100 = 16(6) + 4$$

So

$$\begin{aligned} \sigma^{100} &= \sigma^{16(6)+4} \\ &= (\sigma^6)^{16}\sigma^4 \\ &= e^{16}\sigma^4 \\ &= \sigma^4 \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix} \end{aligned}$$

Section 9 Problems

12. Express the permutation σ as a product of disjoint cycles, and then as a product of transpositions:

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

This permutation tells us the following:

$$1 \to 3$$
$$2 \to 1$$
$$3 \to 4$$
$$4 \to 7$$
$$5 \to 2$$
$$6 \to 5$$
$$7 \to 8$$
$$8 \to 6$$

Writing these operations as a product of disjoint cycles, we find

$$\sigma = (1, 3, 4, 7, 8, 6, 5, 2)$$

Now, expressing this as a product of transpositions:

$$\sigma = (1, 2)(1, 5)(1, 6)(1, 8)(1, 7)(1, 4)(1, 3)$$

13. Recall that element a of a group G with identity element e has order $r > 0$ if $a^r = e$ and no smaller positive power of a is the identity. Consider the group S_8.

a. What is the order of the cycle (1,4,5,7)?

Notice that applying the cycle to itself yields:

$$(1, 4, 5, 7)(1, 4, 5, 7) = (7, 1, 4, 5)$$

So applying the cycle to itself n times will shift all elements to the right n times, with the final element become the first element. That is, it will take 4 products of the cycle with itself to return each element to their respective starting position. So the order of this cycle is 4.

b. State a theorem suggested by part (a).

Theorem: For a cycle of length n, the cycle has order n.

Proof: Left as an exercise to the River (Reader).

c. What is the order of $\sigma = (4, 5)(2, 3, 7)$? of $\tau = (1, 4)(3, 5, 7, 8)$?

In view of the theorem stated in part (b), and the fact that multiplication of disjoint cycles is commutative, we may observe that it since the order of $(2, 3, 7)$ is three and the order of $(4, 5)$ is two, the order of σ is given as $3 \cdot 2 = 6$. Similarly for τ, since the order of $(3, 5, 7, 8)$ is four, and the order of $(4, 5)$ is two, we have that the order of τ is four. To see this, observe the following:

$$\sigma^2 = (4, 5)^2(2, 3, 7)^2 = (5, 4)(3, 7, 2)$$

$$\sigma^3 = (4, 5)^3(2, 3, 7)^3 = (4, 5)(7, 2, 3)$$
$$\sigma^4 = (4, 5)^4(2, 3, 7)^4 = (5, 4)(2, 3, 7)$$
$$\sigma^5 = (4, 5)^5(2, 3, 7)^5 = (4, 5)(3, 7, 2)$$
$$\sigma^6 = (4, 5)^6(2, 3, 7)^6 = (5, 4)(7, 2, 3)$$

$$\sigma^7 = (4,5)^7(2,3,7)^7 = (4,5)(2,3,7) = \sigma$$

So it took 6 operations to return to σ. And for τ:

$$\tau^2 = (1,4)^2(3,5,7,8)^2 = (4,1)(5,7,8,3)$$

$$\tau^3 = (1,4)^3(3,5,7,8)^3 = (1,4)(7,8,3,5)$$

$$\tau^4 = (1,4)^4(3,5,7,8)^4 = (4,1)(8,3,5,7)$$

$$\tau^5 = (1,4)^5(3,5,7,8)^5 = (1,4)(3,5,7,8) = \tau$$

So it took 4 operations to return to τ.

d. Find the order of each of the permutations given in Exercises 10 through 12 by looking at its decomposition into a product of disjoint cycles.

Notice that we may write the permutation in Exercise 10 as (1,8)(3,6,4)(5,7). Following similar logic as in part (c), the order of this permutation is 6. Additionally, the permutation in Exercise 11 can be written as (1,3,4)(2,6)(5,8,7), which also has order 6 following similar logic in part (c). Finally, recall the permutation for Exercise 12 is given by (1, 3, 4, 7, 8, 6, 5, 2), which, by the theorem in part (b), has order 8. To see that the permutations for Exercise 10 and 11 are order 6, observe the following:

$$(1,8)^2(3,6,4)^2(5,7)^2 = (8,1)(6,4,3)(7,4)$$

$$(1,8)^3(3,6,4)^3(5,7)^3 = (1,8)(4,3,6)(4,7)$$

$$(1,8)^4(3,6,4)^4(5,7)^4 = (8,1)(3,6,4)(7,4)$$

$$(1,8)^5(3,6,4)^5(5,7)^5 = (1,8)(6,4,3)(4,7)$$

$$(1,8)^6(3,6,4)^6(5,7)^6 = (8,1)(4,3,6)(7,4)$$

$$(1,8)^7(3,6,4)^7(5,7)^7 = (1,8)(3,6,4)(4,7)$$

So it took 6 operations to return to permutation in Exercise 10. And for the permutation in Exercise 11:

$$(1,3,4)^2(2,6)^2(5,8,7)^2 = (3,4,1)(6,2)(8,7,5)$$

$$(1,3,4)^3(2,6)^3(5,8,7)^3 = (4,1,3)(2,6)(7,5,8)$$

$$(1,3,4)^4(2,6)^4(5,8,7)^4 = (1,3,4)(6,2)(5,7,8)$$

$$(1,3,4)^5(2,6)^5(5,8,7)^5 = (3,4,1)(2,6)(7,8,5)$$

$$(1,3,4)^6(2,6)^6(5,8,7)^6 = (4,1,3)(6,2)(8,5,7)$$

$$(1,3,4)^7(2,6)^7(5,8,7)^7 = (1,3,4)(2,6)(5,7,8)$$

So it took 6 operations to return to the permutation in Exercise 11.

e. State a theorem suggested by parts (c) and (d)

Theorem: The order of a permutation σ is the least common multiple of the lengths of all disjoint cycles of σ.