MATH 100A: Homework #4

Due on October 26, 2023 at 12:00pm

Professor McKernan

Section A02 5:00PM - 5:50PM
Section Leader: Castellano

Source Consulted: Textbook, Lecture, Discussion

Ray Tsai

A16848188

Problem 1

Find the order of all the elements of U_{18}. Is U_{18} cyclic?

Proof. We know that $18 = 2 \cdot 3^2$, and so $U_{18} = \{[1], [5], [7], [11], [13], [17]\}$. Notice that

$$\begin{aligned}
[5]^1 &= 5 \\
[5]^2 &= 7 \\
[5]^3 &= 17 \\
[5]^4 &= 13 \\
[5]^5 &= 11 \\
[5]^6 &= 1.
\end{aligned}$$

Thus, we know that U_{18} is a cyclic group. Let $[5] = a$. We can represent each element in U_{18} as a^i, for some $0 < i \leq \varphi(18) = 6$. Hence, for all $a^i \in U_{18}$, the order of a^i is equal to the least common multiple of i and $\varphi(18) = 6$ divided by i, namely

$$o(a^i) = \frac{\operatorname{lcm}(i,6)}{i} = \frac{6i}{i \cdot \gcd(i,6)} = \frac{6}{\gcd(i,6)}.$$

Therefore,

$$\begin{aligned}
o([1]) &= \frac{6}{\gcd(6,6)} = 1 \\
o([5]) &= \frac{6}{\gcd(1,6)} = 6 \\
o([7]) &= \frac{6}{\gcd(2,6)} = 3 \\
o([11]) &= \frac{6}{\gcd(5,6)} = 6 \\
o([13]) &= \frac{6}{\gcd(4,6)} = 3 \\
o([17]) &= \frac{6}{\gcd(3,6)} = 2.
\end{aligned}$$

□

Problem 2

Find the order of all the elements of U_{20}. Is U_{20} cyclic?

Proof. We know that $20 = 2^2 \cdot 5$, and so $U_{20} = \{[1], [3], [7], [9], [11], [13], [17], [19]\}$. Notice that

$$\begin{array}{lllllll}
[3]^1 = [3] & [7]^1 = [7] & [17]^1 = [17] & [13]^1 = [13] & [9]^1 = [9] & [11]^1 = [11] & [19]^1 = [19] \\
[3]^2 = [9] & [7]^2 = [9] & [17]^2 = [9] & [13]^2 = [9] & [9]^2 = [1] & [11]^2 = [1] & [19]^2 = [1] \\
[3]^3 = [7] & [7]^3 = [3] & [17]^3 = [13] & [13]^3 = [17] & & & \\
[3]^4 = [1] & [7]^4 = [1] & [17]^4 = [1] & [13]^4 = [1] & & &
\end{array}$$

Thus,we have

$$\begin{aligned}
o([1]) &= 1 \\
o([3]) &= 4 \\
o([7]) &= 4 \\
o([9]) &= 2 \\
o([11]) &= 2 \\
o([13]) &= 4 \\
o([17]) &= 4 \\
o([19]) &= 2
\end{aligned}$$

Since we cannot represent all the elements as powers of a single element in U_{20}, we know U_{20} is not a cyclic group. □

Problem 3

If p is a prime number of the form $4n+3$, show that we cannot solve

$$x^2 \equiv -1 \mod p.$$

Proof. Suppose for the sake of contradiction that $x^2 \equiv -1 \mod p$ for some x. Then, $x^4 \equiv 1 \mod p$. Since $x^2 \equiv -1 \mod p$, we know $x \not\equiv \pm 1 \mod p$, and so $x^3 = x \cdot x^2 \not\equiv 1 \mod p$. Therefore, we know that $[x]$ is of order 4 in U_p. By Lagrange's Theorem, we know that $4|\varphi(p) = p-1 = 4n+2$, contradiction. Therefore, we cannot solve the above equation. $\square$

Aliter. We can assume that p does not divide x, otherwise we get $x^2 \equiv 0 \mod p$. Then, we know $x^{p-1} \equiv 1 \mod p$, by Fermat's theorem. We thus get $x^{4n+2} = (x^2)^{2n+1} \equiv 1 \mod p$, but $(-1)^{2n+1} \equiv -1 \mod p$, and so the equation cannot be solved. $\square$

Problem 4

Find the products:

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

Proof.

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

□

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$.

Proof.

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

□

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$.

Proof.

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

□

Problem 5

Find the order of the product you obtained in the previous problem.

Proof. Since $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 5 & 3 & 2 \end{pmatrix}$, the order of it is the least common multiple of the size of the two cycles, namely 6.

Since $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$ is a 3-cycle in S_5, the order of it is 3.

Since $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ is a 2-cycle in S_5, the order of it is 2. □

Problem 6

Show that if σ, τ are two disjoint cycles, then $\sigma\tau = \tau\sigma$.

Proof. Let $\sigma, \tau \in S_n$, where $S = \{1, 2, \ldots, n\}$. Let $i \in S$. If i is not in σ nor τ, then $\sigma\tau(i) = \tau\sigma(i) = i$. Since σ, τ are disjoint cycles, i is not in cycle τ if it is already in σ, and thus $\sigma\tau(i) = \sigma(i) = \tau\sigma(i)$. By symmetry, we also know that if i is in τ, we get $\tau\sigma(i) = \tau(i) = \sigma\tau(i)$, and we exausted all cases.

$\square$

Problem 7

Find the cycle decomposition and order.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 6 & 9 & 8 & 5 \end{pmatrix}$.

Proof. The above permutation can be decomposed into

$$\begin{pmatrix} 1 & 3 & 4 & 2 \end{pmatrix} \begin{pmatrix} 5 & 7 & 9 \end{pmatrix},$$

and the order of it is the least common multiple of the size of the disjoint cycles, namely 12. □

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$.

Proof. The above permutation can be decomposed into

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

and the order of it is the least common multiple of the size of the disjoint cycles, namely 2. □

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}$.

Proof.

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

and the order of it is the least common multiple of the size of the disjoint cycles, namely 6. □

Problem 8

Express as the product of disjoint cycles and find the order.

(c) $\begin{pmatrix}1 & 2 & 3 & 4 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 6\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 7\end{pmatrix}$.

Proof.

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

Since it's a 7-cycle, the order of it is 7. □

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

Proof.

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

Since it's the identity element, the order is 1. □

Problem 9

Express the permutations in the previous problem as the product of transpositions.

Proof. For (c),

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

For (d),

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

□

Problem 10

Find the conjugate of $\sigma = (1,4,7,2)(3,6,5) \in S_7$ by $\tau = (1,2,3)(4,7,5)$. What is the order of σ and τ?

Proof.

$$\begin{aligned}\tau\sigma\tau^{-1} &= \begin{pmatrix}\tau(1) & \tau(4) & \tau(7) & \tau(2)\end{pmatrix}\begin{pmatrix}\tau(3) & \tau(6) & \tau(5)\end{pmatrix} \\ &= \begin{pmatrix}2 & 7 & 5 & 3\end{pmatrix}\begin{pmatrix}1 & 6 & 4\end{pmatrix}.\end{aligned}$$

The order of σ and τ are 12 and 3 respectively. □

Problem 11

Find an element $\tau \in S_7$ that carries $\sigma = (1,2,5)(3,6,7,4)$ into $\sigma' = (3,1,4)(2,7,6,5)$, that is find $\tau \in S_7$ such that

$$\sigma' = \tau\sigma\tau^{-1}.$$

Proof. Consider

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

$$\begin{aligned} \tau\sigma\tau^{-1} &= \begin{pmatrix} \tau(1) & \tau(2) & \tau(5) \end{pmatrix} \begin{pmatrix} \tau(3) & \tau(6) & \tau(7) & \tau(4) \end{pmatrix} \\ &= \begin{pmatrix} 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 7 & 6 & 5 \end{pmatrix} \\ &= \sigma', \end{aligned}$$

and so τ is what we're looking for. $\square$