MTH 4441 Test #3 - Solutions

FALL 2021

Pat Rossi Name ______________________________

1. Define - permutation

Let X be a non-empty set. A one to one and onto function $f : X \to X$ is called a **permutation** of X.

2. Define - r-cycle (or **cycle**).

Suppose that $x_1, x_2, \ldots, x_r$, with $1 \le r \le n$, are distinct elements of $\{1, 2, 3, \ldots, n\}$. The r**-cycle** $(x_1, x_2, \ldots, x_r)$ is the permutation of S_n that maps $x_1 \to x_2, x_2 \to x_3, \ldots, x_{r-1} \to x_r, x_r \to x_1$, and leaves all other elements fixed.

3. Prove: Let $S = \{1, 2, 3, \ldots, n\}$ and let S_n be the set of all permutations $f : S \to S$. Furthermore, let $\circ$ be the operation of function composition. Then $(S_n, \circ)$ is a group.

pf/

i. The operation $\circ$ on S_X is **closed.**

Let $f, g \in S_X$. Then $f \circ g \in S_X$, since the composition of one to one and onto functions on a set X is also a one to one and onto function on X.

ii. 1_X,the identity function on X, is the identity.

First, note that $1_X \in S_X$, since 1_X is one to one and onto.

Let $f \in S_X$. Then $(1_X \circ f)(x) = 1_X(f(x)) = f(x)$ and $(f \circ 1_X)(x) = f(1_X(x)) = f(x)$.

i.e., $1_X \circ f = f = f \circ 1_X$

iii. Given $f \in S_X$, f **has an inverse.**

Since every permutation $f \in S_X$ is one to one and onto, **every permutation** $f \in S_X$ **has an inverse** $f^{-1} \in S_X$,which has the property that $f^{-1} \circ f = 1_X = f \circ f^{-1}$.

iv. $\circ$ is associative, since the operation of function composition is, in general, associative.

Since $(S_n, \circ)$ satisfies all of the group axioms, it is a group. ■

4. Define - disjoint cycles

Two cycles are **disjoint** exactly when they do not "move" (or "act on") the same element.

5. Define - transposition

A **transposition** is a 2-cycle. (i.e., a cycle that "moves" or "acts on" exactly two elements).

6. For Exercises 6-7, State two theorems about permutations.

Thm - Let $f \in S_n$.Then there exist disjoint cycles $f_1, f_2, \ldots, f_m \in S_n$, such that $f = f_1 \circ f_2 \circ \ldots \circ f_m$. (i.e., every permutation on $\{1, 2, \ldots, n\}$ can be written as the "product" (actually "composition") of disjoint cycles. The order of these cycles is arbitrary.

7.

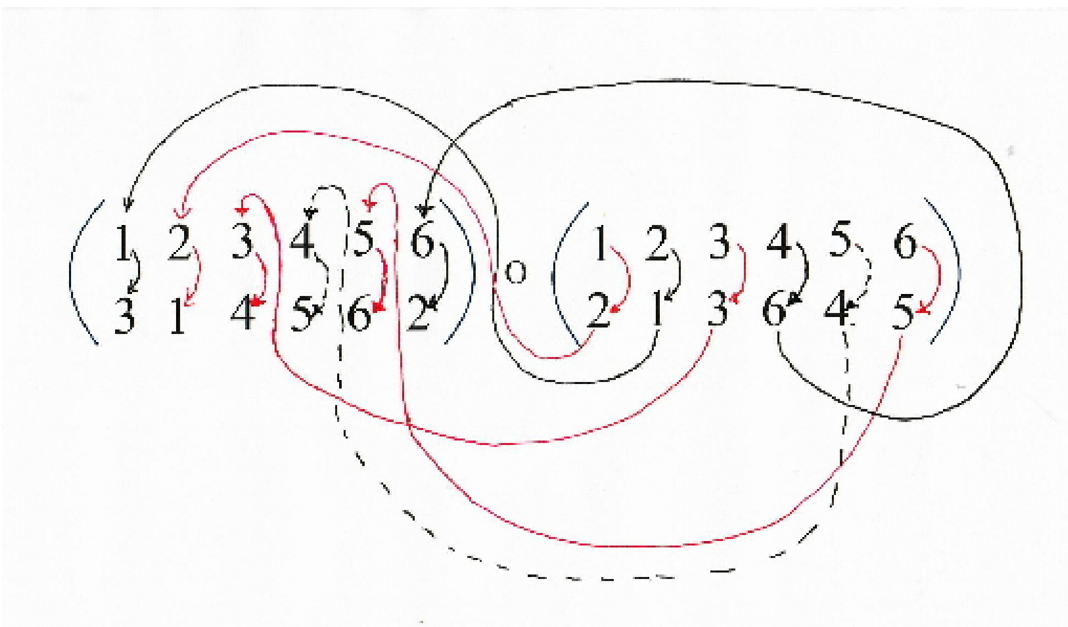
Thm - Every cycle can be expressed as the "product" of transpositions. (in the case of the identity permutation, it can be written as $(1, 2) \circ (1, 2)$)

Thm - A permutation can be expressed as the "product" an even number of transpositions or an odd number of transpositions, but not both. This expression is not unique.

8. Perform the indicated operations in S_6

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

Recall: We begin with the permutation on the right.



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

Alternatively: We can combine this in one diagram

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

9. Express the permutation as a “product” of disjoint cycles and then as the “product” of transpositions. Classify the permutation as being either **even** or **odd.**

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

Starting with 1, note that the permutation maps 1 to 3, 3 to 2, 2 to 4, and 4 back to 1. This yields the cycle $(1,3,2,4)$

We continue with the leftmost element that was not “moved” by cycle $(1,3,2,4)$.

The permutation maps 5 to 6 and 6 back to 5. This yields the cycle $(5,6)$.

We continue with the leftmost element that has not been “moved” by the cycles $(1,3,2,4)$ and $(5,6)$.

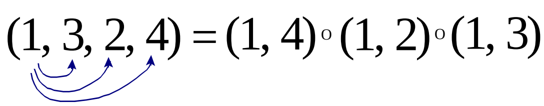
The permutation maps 7 to 8 and 8 back to 7. This yields the cycle $(7,8)$.

Thus, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 6 & 5 & 8 & 7 \end{pmatrix} = (1,3,2,4) \circ (5,6) \circ (7,8)$

The order of the cycles is arbitrary, since the cycles are disjoint.

The cycle $(1,3,2,4)$ can be expressed as the product of transpositions according to the following pattern:

$(1,3,2,4) = (1,4) \circ (1,2) \circ (1,3)$



i.e., $(1,3,2,4) = (1,4) \circ (1,2) \circ (1,3)$ (The order is fixed - it cannot be changed, since the cycles are not disjoint.

Thus, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 6 & 5 & 8 & 7 \end{pmatrix} = \underbrace{(1,4) \circ (1,2) \circ (1,3)}_{=(1,3,2,4)} \circ (5,6) \circ (7,8)$

i.e., $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 6 & 5 & 8 & 7 \end{pmatrix} = (1,4) \circ (1,2) \circ (1,3) \circ (5,6) \circ (7,8)$

Since the permutation can be expressed as the “product” of 5 transpositions, it is an **odd** permutation.

10. Given $(U_5, \odot) = (\{1,2,3,4\}, \odot)$, construct a group of permutations on U_5 that is isomorphic to $(U_5, \odot)$, and exhibit an isomorphism from $(U_5, \odot)$ to this group.

The standard way of generating such a group of isomorphisms, given a group $(G, *)$, is as follows:

For each element $g \in G$, define the function f_g on G as follows: $f_g(x) = g * x$

Let's apply this to $(U_5, \odot) = (\{1,2,3,4\}, \odot)$

$f_1(x) = 1 \odot x$, for all $x \in U_5$

$f_1(1) = 1 \odot 1 = 1$

$f_1(2) = 1 \odot 2 = 2$

$f_1(3) = 1 \odot 3 = 3$

$f_1(4) = 1 \odot 4 = 4$

$\Rightarrow f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ $\leftarrow$ This is the row headed by 1 in the group table

$f_2(x) = 2 \odot x$, for all $x \in U_5$

$f_2(1) = 2 \odot 1 = 2$

$f_2(2) = 2 \odot 2 = 4$

$f_2(3) = 2 \odot 3 = 1$

$f_2(4) = 2 \odot 4 = 3$

$\Rightarrow f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ $\leftarrow$ This is the row headed by 2 in the group table

$f_3(x) = 3 \odot x$, for all $x \in U_5$

$f_3(1) = 3 \odot 1 = 3$

$f_3(2) = 3 \odot 2 = 1$

$f_3(3) = 3 \odot 3 = 4$

$f_3(4) = 3 \odot 4 = 2$

$\Rightarrow f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ $\leftarrow$ This is the row headed by 3 in the group table

$f_4(x) = 4 \odot x$, for all $x \in U_5$

$f_4(1) = 4 \odot 1 = 4$

$f_4(2) = 4 \odot 2 = 3$

$f_4(3) = 4 \odot 3 = 2$

$f_4(4) = 4 \odot 4 = 1$

$\Rightarrow f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ $\leftarrow$ This is the row headed by 4 in the group table

Thus, we have:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Observe that: f_1 is the **identity** permutation and that $f_4 = f_4^{-1}$

Also: $f_2 \circ f_3 = f_1$, hence $f_2 = f_3^{-1}$ and $f_3 = f_2^{-1}$

Thus, every element of $\{f_1, f_2, f_3, f_4\}$ has an **inverse** under the operation of $\circ$.

The operation $\circ$ is **associative**, as function composition is associative in general.

We have not yet shown that $\circ$ is closed on $\{1, 2, 3, 4\}$. However, we will do better than that.

Since $\circ$ is **associative**, it follows that for $i, j \in U_5$, $(f_i \circ f_j)(x) = f_i(f_j(x)) = i \odot (j \odot x) = (i \odot j) \odot x = f_{i \odot j}(x)$

i.e., $f_i \circ f_j = f_{i \odot j}$

What this means is this: where the element $i \odot j$ appears in the group table for $(U_5, \odot)$, the element $f_{i \odot j}$ appears in the table for $(\{f_1, f_2, f_3, f_4\}, \circ)$

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_4	f_1	f_3
f_3	f_3	f_1	f_4	f_2
f_4	f_4	f_3	f_2	f_1

Thus, $\circ$ is closed on $\{f_1, f_2, f_3, f_4\}$ because $\odot$ is closed on U_5

Furthermore, because $f_i \circ f_j = f_{i \odot j}$, the structures of the two group tables are identical, the function $\phi : (U_5, \odot) \to (\{f_1, f_2, f_3, f_4\}, \circ)$, given by $\phi(g) = f_g$ is an isomorphism. ■

11. Consider the group $(G, *)$ given in the table below:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Construct a group of permutations on G that is isomorphic to $(G, *)$, and exhibit an isomorphism from $(G, *)$ to this group.

Recall: The **standard method** of finding such a group of permutations on G is as follows:

For each element $g \in G$, define the function f_g on G as follows: $f_g(x) = g * x$

Thus, for $e \in G$, $f_e(x) = e * x = x$, $\forall x \in G$

i.e., $f_e(x) = x$, $\forall x \in G$. Therefore, f_e will turn out to be the **identity** in our group of permutations.

Given any other function $f_g(x)$, we have:

$(f_e \circ f_g)(x) = f_e(f_g(x)) = f_g(x)$ and $(f_g \circ f_e)(x) = f_g(f_e(x)) = f_g(x)$

i.e., $f_e \circ f_g = f_g = f_g \circ f_e$

Therefore, f_e is the identity.

$$f_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} \leftarrow \text{ The row headed by } e \text{ in the group table}$$

In similar fashion, $f_a(x) = a * x$

Thus:

$f_a(e) = a * e = a$

$f_a(a) = a * a = e$

$f_a(b) = a * b = c$

$f_a(c) = a * c = b$

$$f_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} \leftarrow \text{ The row headed by } a \text{ in the group table}$$

In similar fashion, $f_b(x) = b * x$,

Thus:

$f_b(e) = b * e = b$

$f_b(a) = b * a = c$

$f_b(b) = b * b = e$

$f_b(c) = b * c = a$

$f_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}$ $\leftarrow$ The row headed by b in the group table

In similar fashion, $f_c(x) = c * x$

Thus:

$f_c(e) = c * e = c$

$f_c(a) = c * a = b$

$f_c(b) = c * b = a$

$f_c(c) = c * c = e$

$f_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}$ $\leftarrow$ The row headed by c in the group table

Some sample computations:

$$f_b \circ f_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} \circ \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} = f_e$$

i.e., $f_b \circ f_b = f_e$

$$f_c \circ f_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} \circ \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} = f_e$$

i.e., $f_c \circ f_c = f_e$

The group tables for $(G, *)$ and $(\{f_e, f_a, f_b, f_c\}, \circ)$ are given below:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\circ$	f_e	f_a	f_b	f_c
f_e	f_e	f_a	f_b	f_c
f_a	f_a	f_e	f_c	f_b
f_b	f_b	f_c	f_e	f_a
f_c	f_c	f_b	f_a	f_e

Key Observation: You may notice that the function $\phi : (G, *) \to (\{f_e, f_a, f_b, f_c\}, \circ)$, given by $\phi(x) = f_x$ transforms the group table for $(G, *)$ into the group table for $(\{f_e, f_a, f_b, f_c\}, \circ)$. Thus, the two groups are isomorphic and ϕ is the isomorphism that we seek.

(The reasoning above is sufficient proof. to show that $\phi : (G, *) \to (\{f_e, f_a, f_b, f_c\}, \circ)$ is an isomorphism.)

Alternatively: Given $\phi : (G, *) \to (\{f_e, f_a, f_b, f_c\}, \circ)$, defined by: $\phi(g) = f_g$, where $f_g(x) = g * x$, $\forall x \in G$, note that f is clearly one to one and onto.

Next note that:

$f_{(x_1 * x_2)}(x) = (x_1 * x_2) * x = x_1 * (x_2 * x) = x_1 * (f_{x_2}(x)) = f_{x_1}(f_{x_2}(x)) = (f_{x_1} \circ f_{x_2})(x)$

i.e., $f_{(x_1 * x_2)} = f_{x_1} \circ f_{x_2}$

Hence, $\phi(x_1 * x_2) = f_{(x_1 * x_2)} = f_{x_1} \circ f_{x_2} = \phi(x_1) \circ \phi(x_2)$

i.e., $\forall x_1, x_2 \in G$, $\phi(x_1 * x_2) = \phi(x_1) \circ \phi(x_2)$

Thus, $\phi : (G, *) \to (\{f_e, f_a, f_b, f_c\}, \circ)$ is an isomorphism. ■

12. We are given a group $(G, *)$, and an element $x \in G$. Given also that $x^5 = e$ and that $x^3 = e$, prove that $x = e$.

Observe: $e = x^5 = x^3 * x^2 = e * x^2 = x^2$

i.e., $e = x^2$

Observe: Because $x^2 = e$, $x^{-2} = e$ also.

Hence, $x = x^3 * x^{-2} = e * e = e$

i.e., $x = e$ ■

(Other Solutions are possible)