Permutations and Groups

Training problems for M2 2018 term 2

Ted Szylowiec
tedszy@gmail.com

1 Permutations

1. What is a permutation? Explain it.

2. Is it a permutation or not? Explain why.

(a) $abcd \to aabc$. (b) $abcd \to cadb$. (c) $cbda \to aebdc$. (d) $dcba \to bca$.

3. What is a transposition?

4. What is a regular permutation? Regular permutations are also called *derangements*.

5. What is the identity permutation?

6. Write down all the different permutations of uv.

7. Write down all the different permutations of abc.

8. Write down all the different permutations of $wxyz$.

9. I have five boxes colored red, green, blue, yellow, and orange. I have five balls colored red, green, blue, yellow and orange. How many different ways can I arrange the balls into the boxes, with one ball in each box?

10. I want to arrange 10 different people in a row. How many ways can I do this?

11. Prove that the number permutations of m objects is $m!$.

12. Prove that the number of permutation machines having m boxes per row is $m!$.

13. How many elements are in...

(a) S_2? (b) S_3? (c) S_4? (d) S_5? (e) S_7?

14. What is the difference between a permutation symbol and a permutation machine?

15. Write the permutation symbol that does the given permutaion.

(a) $abc \to bac$. (b) $bac \to abc$. (c) $abcd \to badc$. (d) $badc \to abcd$.

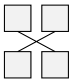
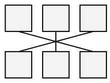
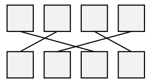
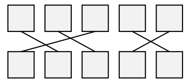
16. Draw the permutation machine that does the given permutaion.

(a) $abc \to cab$. (b) $cab \to abc$. (c) $abcd \to dcba$. (d) $dcba \to abcd$.

17. Change from permutation symbol to permutation machine.

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

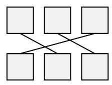
18. Change from permutation machine to permutation symbol.

(a)  (b)  (c)  (d) .

19. Apply the permutation symbol to the objects. What is the result?

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

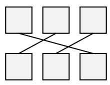
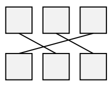
20. Put the objects into the permutation machine. What is the result?

abc .

21. Apply the permutations to the objects. What happens?

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

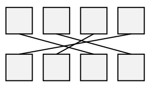
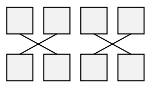
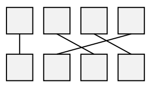
22. Put the objects into the permutation machines. What happens?

abc  .

23. Apply the permutation symbols to the objects.

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

24. Put the objects into the permutation machines. What do you get?

$abcd$   

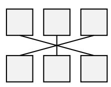
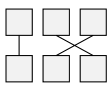
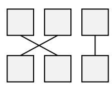
25. Multiply permutation symbols.

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

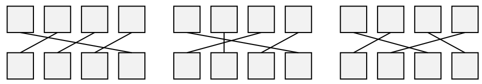
26. Multiply permutation symbols.

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

27. Multiply permutation machines.

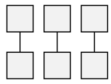
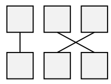
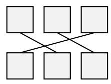
  .

28. Multiply permutation machines.

 .

2 S_3 and S_4

29. Fill in this table for the elements of S_3.

machine	symbol	symbol	machine
		$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	
		$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	
		$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	

30. Write down all the permutation symbols for S_3 and examine the size of the derangements (how many elements are changed). Then fill in this table:

Size of derangement	Number of elements that do it
0	
1	
2	
3	

31. Write down all the permutation symbols for S_4. Examine them and fill in this table (like you did in problem **30**):

Size of derangement	Number of elements that do it
0	
1	
2	
3	
4	

32. Can you find an organized way to write down all the regular permutations (derangements) of S_5? It's a big project. There should be 44 of them.

33. Use these standard definitions for S_3 permutation symbols...

$$e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \qquad t_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \qquad t_2 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$t_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \qquad s_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \qquad s_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

...to fill in this mini S_3 multiplication table:

	e	s_1	s_2
e			
s_1			$s_1 s_2$
s_2			

The entry $s_1 s_2$ tells you how to combine the symbols. Take s_1 from the leftmost column, and then put s_2 from the top row.

34. Use the standard S_3 definitions from problem **33** to construct the full S_3 multiplication table:

	e	t_1	t_2	t_3	s_1	s_2
e						
t_1						$t_1 s_2$
t_2						
t_3						
s_1						
s_2						

The entry $t_1 s_2$ tells you how to combine the symbol from the leftmost column (t_1), with the symbol from the top row (s_2).

35. Examine the table in problem **34**. Notice that no row has two of the same elements. Also notice that no column has two of the same elements. You can use these facts to fill in the table faster. I was able to get 9 free table entries this way, where I did not have to do any multiplication of permutation symbols. Can you do it in such a way as to get more than 9 free ones?

36. Define the symbols e and t and use them to construct multiplication tables for S_2 and S_1. How many elements do S_2 and S_1 have?

37. Look at the multiplication tables for S_1, S_2 and S_3. What permutation symbols behave like the identity in S_1, S_2 and S_3?

38. What permutation symbols behave like the identity in S_5? In S_6?

39. Is S_2 inside S_3? Explain how.

40. Is S_3 inside S_4? Explain how.

41. Consider these elements of S_4:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Make a multiplication table with e, a, b, c. Is the table perfect (each row contains each symbol exactly once and each column contains each symbol exactly once)?

42. Consider these elements of S_4:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Make a multiplication table with e, p, q, r. Is the table perfect?

3 Inverse

43. Use the S_3 multiplication table in problem **34** to find the inverses of e, t_1, t_2, t_3, s_1 and s_2. Do it two different ways:

(a) using $x \cdot x^{-1} = e$. (b) using $x^{-1} \cdot x = e$.

44. Find the inverses of e, t_1, t_2, t_3, s_1 and s_2 *without* using the S_3 multiplication table. Do it two different ways:

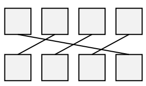
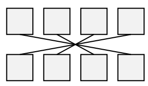
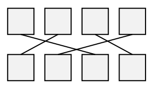
(a) using $x \cdot x^{-1} = e$. (b) using $x^{-1} \cdot x = e$.

45. Find the inverses of these S_4 permutation symbols.

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

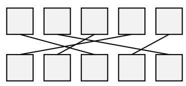
Do it two different ways: using $x \cdot x^{-1} = e$ and then using $x^{-1} \cdot x = e$.

46. Find the inverses of these S_4 permutation machines.

(a) . (b) . (c) .

Do it two different ways: using $x \cdot x^{-1} = e$ and then using $x^{-1} \cdot x = e$. Remember that machines multiply to the right.

47. Find the inverses of these S_5 symbols and machines. Do it two different ways: using $x \cdot x^{-1} = e$ and $x^{-1} \cdot x = e$.

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

48. Study the patterns in the S_3 multiplication table of problem **34**. Is it possible for an element to have two different inverses? Prove that if x is an element of S_n then x cannot have two different inverses.

49. Prove that the inverse of abc is $c^{-1}b^{-1}a^{-1}$. Hint: use $xx^{-1} = e$ and $x^{-1}x = e$.

4 Symmetries

50. What is an isometry?

51. Write down the three different kinds of isometries.

52. What are symmetries?

53. What kind of thing has translational symmetries? Draw some examples.

54. What did the Ancient Greeks think about beauty and symmetry?

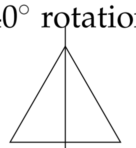
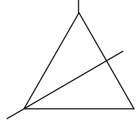
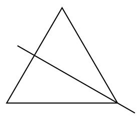
55. According to the Ancient Greeks, what is the most beautiful geometric shape? Why did they think so?

56. Find all symmetries of a scalene triangle. Make a multiplication table. (It's not very big.)

57. An isoceles triangle has two symmetries. Find them. Use Roman letters a, b,... for rotational symmetries and Greek letters α, β,... for reflection symmetries. Make a multiplication table. Which symmetry behaves like the identity?

58. Find all symmetries of an equilateral triangle. How many are there? Which symmetry behaves like the identity?

59. An equilateral triangle has six symmetries. Three rotational symmetries and three reflection symmetries. We use Roman and Greek letters to give them names:

Symbol	Symmetry
a	0° rotation.
b	120° rotation.
c	240° rotation.
α	
β	
γ	

Construct a multiplication table for the symmetries of the equilateral triangle:

	a	b	c	α	β	γ
a						
b						
c						
α						
β						
γ						

Remember: symmetries are combined from right to left, just like permutation symbols.

60. Compare S_1 to the symmetries of a scalene triangle. Are the multiplication tables similar?

61. Compare S_2 to the symmetries of an isoceles triangle. Are the multiplication tables similar?

62. Compare S_3 to the symmetries of an equilateral triangle. What can you say about the multiplication tables of these two things?

5 Groups

63. Write down the symmetries of an isoceles triangle and construct the multiplication table. Prove that they form a group by showing that there is an identity element, that the multiplication table is closed and all symmetries have inverses.

64. Prove that S_2 is a group by showing the three group properties: identity, closure and inverse.

65. Let $K = \{a, b, c, d\}$ with the following multiplication table:

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Prove that K is a group.

66. Let $L = \{x, y, z, w\}$ with the following multiplication table:

	x	y	z	w
x	z	w	x	y
y	w	z	y	x
z	x	y	z	w
w	y	x	w	z

Prove that L is a group.

67. Let $G = \{a, b, c, \alpha, \beta, \gamma\}$ be the symmetries of an equilateral triangle, as in **59**. Construct the multiplication table for G and prove that G is a group. Show identity, closure, inverse.

68. Let $S_3 = \{e, t_1, t_2, t_3, s_1, s_2\}$ according to the standard definitions that we used in problem **33**. Show that S_3 is a group by showing that it has the properties of idenitity, closure and inverse.

69. Let G be a group. Prove that the multiplication table for G has the following magical property: no row has more than one of the same element.

70. Let G be a group. Prove that the multiplication table for G has another magical property: no column has more than one of the same element.

71. We saw before that the inverse of x must satisfy two conditions: $x^{-1}x = e$ and $xx^{-1} = e$ where e is the identity. Let y in $yx = e$ be the *left inverse* of x and let z in $xz = e$ be the *right inverse* of x. Prove that the left inverse must be equal to the right inverse. Hint: it's very easy.

72. Let $G = \{u, w, x, y, z\}$ and consider the Cayley table:

	u	w	x	y	z
u	w	x	u	z	y
w	z	y	w	x	u
x	u	w	x	y	z
y	x	z	y	u	w
z	y	u	z	w	x

This table looks good. No element appears twice in any row and no element appears twice in any column. Also, G has an identity element, x. But G is still not a group!

(a) Look at the left and right inverses of the elements of G. What do you see?

(b) Use problem **71** to show that some of the elements of G must be equal to each other and therefore G is not a set of 5 distinct elements.

73. Construct a group G of order 5. Make sure G has an identity element and make sure to check $x^{-1}x = xx^{-1} =$ identity (left and right inverses must be equal.) Find the order each element $g \in G$ and show that $g^{|G|}$ for all g in G. Find all generators of G. Is G cyclic?

74. Let $G = \{a, b, c, d, e, f\}$ and consider the Cayley table:

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	c	f	d
c	c	d	f	e	b	a
d	d	f	a	b	c	e
e	e	c	d	f	a	b
f	f	e	b	a	d	c

The table looks good. No row has two of the same and no column has two of the same. But G is still not a group. Show that G has identity and closure properties, but does not have the inverse property. You can also argue that that some of the elements of G must be equal to each other, which contradicts the assertion that they are all different. (Credit: Eggyolk from M2/1.)

75. Let $G = \{a, b, c, d\}$ with the following Cayley table:

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	d	c	a	b
d	c	d	b	a

The table looks pretty good: no row has repeated elements and no column has repeated elements. But G is still not a group. Why not? Hint: when checking the identity property, you have to check both ways:

$$(\text{identity})x = x \quad \text{and} \quad x(\text{identity}) = x.$$

Both must be true for all x in G.

76. Let $G = \{a, b, c, d, e, f\}$ with Cayley table

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

Prove that G is a group.
(a) What is the identity?
(b) Check left and right identity properties.
(c) Check left and right inverses.
(d) Check closure.
(e) What are the orders of all the elements?
(f) Find all generators.
(g) Is G cyclic?

77. Construct a group of order 7. Prove that it is a group. When you check the inverse property, make sure to check left inverse and right right inverse. Both must be equal. Find the orders of all the elements. Find all generators. Is the group cyclic?

78. Let G be a group and let $g \in G$. Prove that if $g^2 = g$ then g must be the identity element. You can try using contradiction. Assume g isn't the identity, and try to get a contradiction.

79. Show that $g^{|S_3|} = e$ for all elements $g \in S_3$.

80. Find the order of every element in S_3.

81. Construct an order-3 group G. Find the order of each element in G. Verify that if $g \in G$ then $g^{|G|}$ is the identity. Find all generators (if any). Is this group cyclic?

82. Let $G = \{a, b, c, d\}$ with the following Cayley table:

	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

Find the order of each element in G. Verify that $g^{|G|}$ is the identity for all g in G. Find all generators of G. Is G a cyclic group?

83. Find all generators of S_3 (if any). Is S_3 a cyclic group?

84. Is it possible to construct two groups of order 3 that are not isomorphic? In other words, can we construct two different Cayley tables with the same symbols a, b, c in the same order, which cannot be matched by an isomorphism map?

	a	b	c
a			
b			
c			

	a	b	c
a			
b			
c			

Try it.

85. Construct two order 4 groups $G = \{a, b, c, d\}$ and $H = \{w, x, y, z\}$ that are not isomorphic.

	a	b	c	d
a				
b				
c				
d				

	w	x	y	z
w				
x				
y				
z				

86. Let $G = \{a, b, c, d, e\}$, $H = \{v, w, x, y, z\}$ and consider their Cayley tables:

	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

	v	w	x	y	z
v	y	z	v	w	x
w	z	v	w	x	y
x	v	w	x	y	z
y	w	x	y	z	v
z	x	y	z	v	w

Prove that G and H are isomorphic.

(a) Get clues. Find inverses and orders of all elements.
(b) Make the isomorphism map
(c) Arrange the Cayley tables in the same order as your isomorphism map.
(d) Show that the tables match perfectly.

6 Modular arithmetic

87. Who discovered modular arithmetic?

88. Where was Carl Gauss from? Tell me two great things he did in mathematics and one great thing he did in astronomy.

89. Let G be the set of residues $\{0, 1, 2, 3, 4\}$ with addition mod 5.

$+$ mod 5	0	1	2	3	4
0					
1					
2					
3					
4					

(a) Fill in the Cayley table for G. Show that the Cayley table is closed. Find the identity element. Check the left and right identity properties:

$$\text{identity} + x = x, \quad x + \text{identity} = x.$$

(b) Find the inverse of every element. Check that left and right inverses are equal:

$$(\text{inverse x}) + x = \text{identity}, \quad x + (\text{inverse x}) = \text{identity}.$$

(c) Find the order of each element in G. Remember, you care combining elements by addition mod 5.
(d) Find all generators of G (if any). Is G cyclic?

We say that G is the *additive residue group mod 5*.

90. Use addition mod 6 with the residues $G = \{0, 1, 2, 3, 4, 5\}$. Follow all the same steps as in problem **89** and prove that G is a group. We call it the *additive residue group mod 6*.

91. Use addition mod 7 with residues mod 7. Follow the steps of problem **89**. Does this form a group?

92. Same as problem **89** but with addition mod 10 and let G be the set of residues mod 10. Does this form a group?

93. (Naive mod 5 multiplicative attempt.)

94. Find these GCDs.

(a) $(18, 16)$.
(b) $(18, 6)$.
(c) $(77, 66)$.
(d) $(88, 66)$.
(e) $(72, 48)$.
(f) $(81, 45)$.

95. Find these GCDs.

(a) $(17, 13)$.
(b) $(15, 29)$.
(c) $(35, 16)$
(d) $(1, 1)$.
(e) $(1, 109)$.
(f) $(31, 1)$.

96. Find these GCDs.

(a) $(0, 25)$.
(b) $(42, 0)$.
(c) $(1, 0)$
(d) $(0, 1)$.
(e) $(44, 13)$.
(f) $(43, 120)$.

97. Circle the numbers that are coprime to 10.

2 5 15 17 21 26 30 31 49

98. Circle the numbers coprime to 210.

49 99 57 121 143 143 111 169

99. Circle the numbers coprime to 12. Put an `X` on the numbers *not* coprime to 12.

0 1 2 3 4 5 6 7 8 9 10 11

100. Circle the numbers coprime to 18. Put an `X` on the ones that are *not* coprime to 18.

0 1 2 3 4 5 6 7 8 4 10 11 12 13 14 15 16 17

101. Construct a reduced residue set mod 9. How many elements does it have?

102. Construct a reduced residue set mod 24. How many elements does it have?

103. Construct a reduced residue set mod 11. How many elements does it have?

104. Construct a reduced residue set mod p, where p is a prime number. How many elements does it have?

105. There are exactly two kinds of groups of order 4: the Klein-4 group and the cyclic-4 group. Let $K_4 = \{a, b, c, d\}$ be the Klein-4 group and let $C_4 = \{w, x, y, z\}$ be the cyclic-4 group. K_4 and C_4 have these Cayley tables:

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

	w	x	y	z
w	w	x	y	z
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y

All other groups of order 4 are isomorphic to one of these. This fact opens up many interesting questions about modular arithmetic groups.

The Let G be the additive residue group mod 4. What type of group is G? Is it isomorphic to K_4 or isomorphic to C_4?

106. Let G be the multiplicative residue group mod 5. Find all generators. Is it cyclic? Use problem **105** and figure out if G is isomorphic to K_4 or to C_4.

107. Let G be the multiplicative residue group mod 8. Find all generators (if any). Find the order of each element. Is G cyclic? What is G isomorphic to, K_4 or C_4?

108. Let G be the multiplicative residue group mod 10. Find all generators, if any. Find the order of each element. Is G cyclic? Is G isomorphic to K_4 or to C_4. Prove it by making an isomorphism map, putting the Cayley tables in order, and showing that they match.

109. Let G be the multiplicative residue group mod 12. Find the order of each element. Find all generators, if any. Is G cyclic? What is G isomorphic to, the Klein-4 group or the cyclic-4 group? Prove it by making the isomorphism map, arranging the Cayley tables in order, and showing that they match perfectly.