MAT414 - Modern Algebra - Permutation Groups

Cycle Notation [1]

Miraj Samarakkody

Tougaloo College

Updated - April 13, 2025

Cycle Notation

Write the followings in the cyclic notations:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$$

Cycle Notation

Write the followings in the cyclic notations:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$$

Find $\alpha\beta$.

Properties of Permutations

Theorem 5.1 - Products of Disjoint Cycles

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem 5.2

Disjoint Cycles Commute

If the pair of cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Theorem 5.3

Order of a Permutation

The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Theorem 5.3

Order of a Permutation

The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Find

- $|(132)(45)|$
- $|(1432)(56)|$
- $|(123)(456)(78)|$
- $|(123)(145)|$

Example 5

Determine the orders of the elements of S_7.

Example 6

Determine the number of elements in S_7 of order 12.

Example 7

Determine the number of elements in S_7 of order 3.

Theorem 5.4

Product of 2-Cycles

Every permutation of in S_n, $n > 1$, is a product of $2-$cycles.

Example

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

Lemma

In S_n, if $\epsilon = \beta_1\beta_2\beta_3 \ldots \beta_r$, where the β_i's are 2-cycles, then r is even.

Theorem 5.5

Always Even or Always Odd

If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2−cycles must have an an even (odd) number of 2−cycles.

In symbols, if

$$\alpha = \beta_1\beta_2\dots\beta_r \text{ and } \alpha = \gamma_1\gamma_2\dots\gamma_s,$$

where the β's and γ's are 2−cycles, then r and s are both even or both odd.

Even and Odd Permutations

Definition

A permutation that can be expressed as a product of an even number of $2-$cycles is called an **even permutation**. A permutation that can be expressed as a product of an odd number of $2-$cycles is called an **odd permutation**.

Even Permutations Form a Group

Theorem 5.6
The set of all even permutations of S_n is a subgroup of S_n and is denoted by A_n.

Alternating Group of Degree n

Definition

The alternating group of degree n, denoted A_n, is the set of all even permutations of S_n.

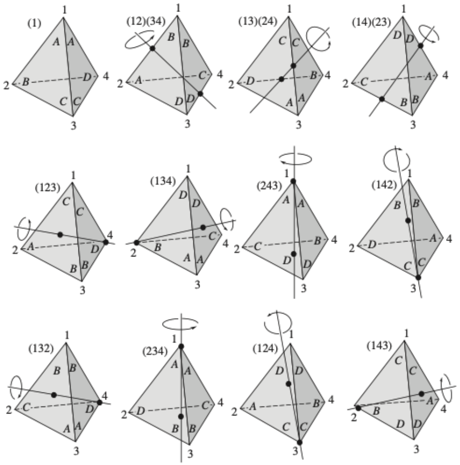
Theorem

Theorem 5.7

For $n > 1$, A_n has order $n!/2$.

Example 10 - Rotations of a Tetrahedron

The 12 rotations of a regular tetrahedron can be conveniently described with the elements of A_4.



Example 10 - Rotations of a Tetrahedron

The 12 rotations of a regular tetrahedron can be conveniently described with the elements of A_4.

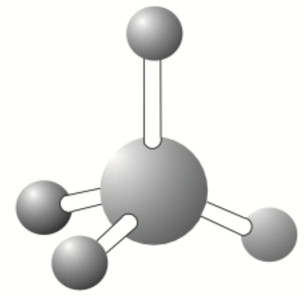
Table 5.1 The Alternating Group A_4 of Even Permutations of {1, 2, 3, 4}

(In this table, the permutations of A_4 are designated as $\alpha_1, \alpha_2, \ldots, \alpha_{12}$ and an entry k inside the table represents α_k. For example, $\alpha_3 \alpha_8 = \alpha_6$.)

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

Applications

Many molecules with chemical formulas of the form AB_4, such as methane (CH_4) and carbon tetrachloride (CCl_4), have A_4 as thier symmetry group.



Encryption Using a Permutation

- An intersting application of permutations is in the field of cryptography.

Encryption Using a Permutation

- An intersting application of permutations is in the field of cryptography.
- cryptography is the science of encoding and decoding messages.

Encryption Using a Permutation

- An intersting application of permutations is in the field of cryptography.
- cryptography is the science of encoding and decoding messages.
- The process of encoding a message is called encryption, and the process of decoding a message is called decryption.

Encryption Using a Permutation

- An intersting application of permutations is in the field of cryptography.
- cryptography is the science of encoding and decoding messages.
- The process of encoding a message is called encryption, and the process of decoding a message is called decryption.
- First known cryptosystme is th Caesar cipher.

Encryption Using a Permutation

- An intersting application of permutations is in the field of cryptography.
- cryptography is the science of encoding and decoding messages.
- The process of encoding a message is called encryption, and the process of decoding a message is called decryption.
- First known cryptosystme is th Caesar cipher.
- The Caesar cipher is a substitution cipher, which means that each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.

Rubik's Cube

- It was invented in 1974 by Hungarian architect and professor of architecture Ernő Rubik.

Rubik's Cube

- It was invented in 1974 by Hungarian architect and professor of architecture Ernő Rubik.
- The cube has 6 faces, each with 9 stickers of one of 6 solid colors.

Rubik's Cube

- It was invented in 1974 by Hungarian architect and professor of architecture Ernő Rubik.
- The cube has 6 faces, each with 9 stickers of one of 6 solid colors.
- The cube can be rotated about its axes, and the goal is to return the cube to its original state after it has been scrambled.

Rubik's Cube

- It was invented in 1974 by Hungarian architect and professor of architecture Ernő Rubik.
- The cube has 6 faces, each with 9 stickers of one of 6 solid colors.
- The cube can be rotated about its axes, and the goal is to return the cube to its original state after it has been scrambled.
- The cube has $43,252,003,274,489,856,000$ possible configurations.

Rubik's Cube

- It was invented in 1974 by Hungarian architect and professor of architecture Ernő Rubik.
- The cube has 6 faces, each with 9 stickers of one of 6 solid colors.
- The cube can be rotated about its axes, and the goal is to return the cube to its original state after it has been scrambled.
- The cube has $43,252,003,274,489,856,000$ possible configurations.
- God's number is 20, which means that any configuration of the cube can be solved in 20 moves or less.

Rubick's Cube

			1	2	3						
			4	top	5						
			6	7	8						
9	10	11	17	18	19	25	26	27	33	34	35
12	left	13	20	front	21	28	right	29	36	rear	37
14	15	16	22	23	24	30	31	32	38	39	40
			41	42	43						
			44	bottom	45						
			46	47	48						

References

Joseph A. Gallian.
Contemporary Abstract Algebra.
Cengage Learning, 9th edition, 2017.