Chapter 5: Permutation Groups

Definitions and Basic Concepts

Definition: Permutation of A
A permutation of a set A is a function from A to A that is both one-to-one and onto.

Definition: Permutation Group of A
A permutation group of a set A is a set of permutations of A that forms a group under function composition.

- Focus on finite sets $A = \{1, 2, 3, \ldots, n\}$
- The group of all permutations of the set $\{1, 2, 3, \ldots, n\}$ is called the symmetric group and is denoted by S_n.
- Array notation: place $\alpha(j)$ directly below j. **Example of Array Notation:** For $\alpha : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ where $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$, $\alpha(4) = 4$:
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Composition of Permutations

- Performed from right to left
- Go from top to bottom, then top to bottom again

Detailed Example: Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ and $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$

Step-by-step calculation of $\gamma\sigma$:

- $(\gamma\sigma)(1) = \gamma(\sigma(1)) = \gamma(2) = 4$
- $(\gamma\sigma)(2) = \gamma(\sigma(2)) = \gamma(4) = 2$
- $(\gamma\sigma)(3) = \gamma(\sigma(3)) = \gamma(3) = 1$
- $(\gamma\sigma)(4) = \gamma(\sigma(4)) = \gamma(5) = 3$
- $(\gamma\sigma)(5) = \gamma(\sigma(5)) = \gamma(1) = 5$

Therefore: $\gamma\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$

Example 1 - Symmetric Group S_3

Definition: $S_3 =$ set of all one-to-one functions from $\{1, 2, 3\}$ to itself

All Six Elements:

- $\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ (identity), $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
- $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Key Properties:

- $\beta\alpha = \alpha^2\beta$ (verify this!)
- S_3 is non-Abelian
- $|S_3| = 6$
- Relation $\beta\alpha = \alpha^2\beta$ allows computation without arrays

Example 2 - General Symmetric Group S_n

Definition: $S_n =$ symmetric group of degree n = set of all permutations of $\{1, 2, \ldots, n\}$

Order Calculation:

- Choose $\alpha(1)$: n choices
- Choose $\alpha(2)$: $n-1$ choices (must be different from $\alpha(1)$)
- Choose $\alpha(3)$: $n-2$ choices
- Continue this pattern...
- Total: $n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1 = n!$

Key Facts:

- $|S_n| = n!$
- S_n is non-Abelian for $n \geq 3$
- S_4 has 30 subgroups
- S_5 has over 100 subgroups
- $|S_{60}| \approx$ number of atoms in the universe!

Example 3 Symmetries of a Square (D_4 as Subgroup of S_4)

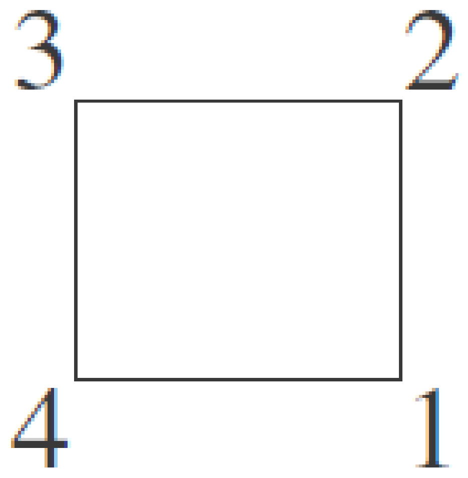
Setup: Label square corners as $1, 2, 3, 4$ and track their positions

90° Counterclockwise Rotation:

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

Horizontal Reflection:

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



Key Insight:

- These two elements generate the entire dihedral group D_4
- D_4 can be viewed as a subgroup of S_4
- This shows how geometric symmetries relate to permutation groups

Cycle Notation - Introduction and Motivation

Basic Idea:

Instead of arrows showing $\alpha(1) \to 2 \to 4 \to 6 \to 3 \to 1$, we write $(1, 2, 4, 6, 3)$

Example Conversion:

$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$ becomes $\alpha = (1, 2)(3, 4, 6)(5)$

Terminology:

- Expression $(a_1, a_2, \ldots, a_m)$ is called an m-cycle or cycle of length m
- Cycles fix elements not appearing in them

Exercise:

Which of the following is true about D_n and S_n for all $n \geq 1$?

a) $D_n = S_n$
b) D_n is a subgroup of S_n
c) S_n is a subgroup of D_n
d) D_n and S_n have no relationship

Multiple Choice

Exercise:

For which values of $n \geq 1$ is $D_n = S_n$?

a) 1, and 2 only.

b) for all $n \geq 1$.

c) 1, 2, and 3 only.

d) No such values exists.

Multiple Choice

Cycle Notation - Detailed Examples

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

Tracing the cycles:

- Start with 1: $1 \to 5 \to 2 \to 3 \to 1$, so $(1, 5, 2, 3)$
- Remaining elements: $4 \to 6 \to 4$, so $(4, 6)$
- Result: $\beta = (1, 5, 2, 3)(4, 6)$ or equivalently $(4, 6)(5, 2, 3, 1)$

Example 2: Converting back to array form
If $\gamma = (134)$, then:

- $1 \to 3$, $3 \to 4$, $4 \to 1$
- $2 \to 2$ (fixed)
- Array form: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

Multiplying Cycles - Complex Example

Problem: Find $\alpha\beta$ where $\alpha = (13)(27)(456)(8)$ and $\beta = (1237)(648)(5)$

Method: Trace each element through all cycles from right to left

Detailed calculation for element 1:
(5) fixes 1 → (648) fixes 1 → (1237) sends 1 to 2 → (8) fixes 2 → (456) fixes 2 → (27) sends 2 to 7 → (13) fixes 7

Result: $1 \to 7$, so $\alpha\beta$ begins $(17\ldots)$

Continuing the process:

- $7 \to 3$: $(5) \to (648) \to (1237) \to (8) \to (456) \to (27) \to (13)$ gives $7 \to 7 \to 7 \to 7 \to 7 \to 7 \to 3$
- $3 \to 2$: similar tracing gives $3 \to 2$
- $2 \to 1$: tracing gives $2 \to 1$

Final Answer: $\alpha\beta = (1732)(48)(56)$

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.

Proof:

1. Start with any element $a_1 \in A$
2. Form sequence: $a_1, \alpha(a_1), \alpha^2(a_1), \alpha^3(a_1), \ldots$
3. Since A is finite, eventually $\alpha^m(a_1) = a_1$ for some m
4. This gives cycle $(a_1, \alpha(a_1), \alpha^2(a_1), \ldots, \alpha^{m-1}(a_1))$
5. If elements remain, pick b_1 not in first cycle and repeat
6. Continue until all elements are accounted for

Note that new cycles are disjoint from previous ones because if $\alpha^i(a_1) = \alpha^j(b_1)$, then b_1 would equal some $\alpha^t(a_1)$, contradicting the choice of b_1.

Theorem 5.2(Disjoint Cycles Commute)**:** If cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Proof: Consider $S = \{a_1, \ldots, a_m, b_1, \ldots, b_n, c_1, \ldots, c_k\}$ where c's are fixed by both α and β.

Case 1 - Element a_i:

- $(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$ (β fixes a-elements)
- $(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$ (β fixes a-elements)

Case 2 - Element b_j:

- $(\alpha\beta)(b_j) = \alpha(\beta(b_j)) = \alpha(b_{j+1}) = b_{j+1}$ (α fixes b-elements)
- $(\beta\alpha)(b_j) = \beta(\alpha(b_j)) = \beta(b_j) = b_{j+1}$

Case 3 - Element c_k:

- $(\alpha\beta)(c_k) = \alpha(\beta(c_k)) = \alpha(c_k) = c_k$
- $(\beta\alpha)(c_k) = \beta(\alpha(c_k)) = \beta(c_k) = c_k$

Conclusion: $\alpha\beta = \beta\alpha$ □

Theorem 5.3(Order of a Permutation (Ruffini, 1799))**:** The order of a permutation written in disjoint cycle form is the least common multiple of the lengths of the cycles.

n in

Proof Outline:

1. A cycle of length n has order n
2. For disjoint cycles α (length m) and β (length n):
   - Let $k = \text{lcm}(m, n)$
   - Both $\alpha^k = \varepsilon$ and $\beta^k = \varepsilon$
   - Since α and β commute: $(\alpha\beta)^k = \alpha^k\beta^k = \varepsilon$
   - So $|\alpha\beta|$ divides k
3. If $(\alpha\beta)^t = \varepsilon$, then $\alpha^t\beta^t = \varepsilon$
4. Since cycles are disjoint: $\alpha^t = \varepsilon$ and $\beta^t = \varepsilon$. So $m|t$ and $n|t$.
5. Since k is the least common multiple: $k \leq t$
6. Combined with step 2: $k = |\alpha\beta|$

Extension: The proof generalizes to products of more than two disjoint cycles.

Examples Using Theorem 5.3

Example 4 - Order Calculations:

a) $|(132)(45)| = \mathrm{lcm}(3,2) = 6$

b) $|(1432)(56)| = \mathrm{lcm}(4,2) = 4$

c) $|(123)(456)(78)| = \mathrm{lcm}(3,3,2) = 6$

d) $|(123)(145)| = ?$

- First convert to disjoint cycles: $(123)(145) = (14523)$
- $|(14523)| = 5$

Key Insight: Must convert to disjoint cycle form first when cycles overlap!

Exercise:

Question: Which of the following statements is TRUE?

a) The order of $(12)(34)(56)$ is $2 + 2 + 2 = 6$

b) To find the order of $(123)(345)$, we can directly compute $\mathrm{lcm}(3,3) = 3$

c) The permutation $(1234)(56)$ has order $\mathrm{lcm}(4,2) = 4$

d) Disjoint cycles always have the same length

Multiple Choice

Example 5 - Systematic Order Analysis in S_7

Goal: Determine all possible orders of elements in S_7

Method: List all disjoint cycle structures, compute lcm of cycle lengths 7

Cycle Structures in S_7: We write (k) to mean a cycle of k elements.

- (7)-cycle: order = 7,
- (6)(1): order = 6
- (5)(2): order = $\operatorname{lcm}(5,2) = 10$, (5)(1)(1): order = 5
- (4)(3): order = $\operatorname{lcm}(4,3) = 12$, (4)(2)(1): order = $\operatorname{lcm}(4,2) = 4$, (4)(1)(1)(1): order = 4
- (3)(3)(1): order = 3, (3)(2)(2): order = $\operatorname{lcm}(3,2) = 6$, (3)(2)(1)(1): order = $\operatorname{lcm}(3,2) = 6$, (3)(1)(1)(1)1): order = 3
- (2)(2)(2)(1): order = 2, (2)(2)(1)(1)(1): order = 2, (2)(1)(1)(1)(1)(1): order = 2
- (1)(1)(1)(1)(1)(1)(1): order = 1

Example: How many n-cycles in S_n?

Solution: An n-cycle in S_n uses all n elements.

Step-by-step counting:

1. Choose first element: n ways (but any element can start the cycle)
2. Choose second element: $(n-1)$ ways
3. Choose third element: $(n-2)$ ways
4. Continue until all elements are chosen: $n!$ total arrangements

Adjustment for cycle equivalence:

- The cycles $(1, 2, 3, \ldots, n)$, $(2, 3, \ldots, n, 1)$, $(3, \ldots, n, 1, 2)$, etc. all represent the same permutation
- There are n equivalent representations for each n-cycle
- Must divide by n to avoid overcounting

Answer: $\frac{n!}{n} = (n-1)!$ distinct n-cycles in S_n

Example: How many $(n-1)$-cycles in S_n?

Solution: An $(n-1)$-cycle in S_n uses $(n-1)$ elements and fixes one element.

Step-by-step counting:

1. Choose (n-1) elements to form the cycle: $\binom{n}{n-1} = n$ ways
2. Arrange them in an $(n-1)$-cycle: $(n-2)!$ ways (by the previous example)

Answer: $n \cdot (n-2)!$ distinct $(n-1)$-cycles in S_n

Example 6 - Counting Elements of Specific Order

Problem: How many elements in S_7 have order 12?

Analysis: Need cycle structure $(4)(3)$ by Theorem 5.3

Step-by-step counting:

1. Choose 4 elements for the 4-cycle: $\binom{7}{4}$ ways
2. Arrange them in a 4-cycle: $(4-1)! = 3!$ ways
3. Choose 3 elements from remaining for 3-cycle: $\binom{3}{3} = 1$ way
4. Arrange them in a 3-cycle: $(3-1)! = 2!$ ways

Calculation:

$$\binom{7}{4} \times 3! \times 1 \times 2! = 35 \times 6 \times 1 \times 2 = 420$$

Transpositions

Definition: A transposition is a 2-cycle (ab) that interchanges elements a and b.

Example 8 - Writing Cycles as Products of Transpositions:

$$(a_1 a_2 \ldots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)$$

Theorem 5.4: Every permutation in S_n $(n > 1)$ is a product of 2-cycles.

Proof:

- Identity: $\varepsilon = (12)(12)$
- By Theorem 5.1, any permutation $= (a_1 a_2 \ldots a_k)(b_1 b_2 \ldots b_t) \cdots$
- Each k-cycle $= (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)$ $\square$

Theorem 5.4: Every permutation in S_n $(n > 1)$ is a product of 2-cycles.

Proof:

- Identity: $\varepsilon = (12)(12)$
- By Theorem 5.1, any permutation $= (a_1 a_2 \ldots a_k)(b_1 b_2 \ldots b_t) \cdots$
- Each k-cycle $= (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)$ $\square$

Non-Uniqueness of Transposition Decompositions

Example 9 - Multiple Decompositions:

$$(12345) = (54)(53)(52)(51)$$

$$(12345) = (54)(52)(21)(25)(23)(13)$$

Key Observations:

- Decompositions use different numbers of transpositions (4 vs 6)
- BUT: both have even number of transpositions!
- This is not a coincidence...

Lemma: If $\varepsilon = \beta_1\beta_2 \cdots \beta_r$ where each β_i is a 2-cycle, then r is even.

Proof: Assume r is odd and $\varepsilon = \beta_1\beta_2 \cdots \beta_r$ where $\beta_1 = (ab)$. Clearly $r > 1$ (since a single 2-cycle is not the identity). There must be an $i > 1$ such that β_i contains a, say $\beta_i = (ac)$ for some c. May assume the product is chosen so that:

1. i is the smallest possible (i.e., a first reappears at position i).
2. The number of a occurrences is minimum.
3. The product has the fewest number of transpositions.

Case 1: If $i = 2$: Either $c = b \Rightarrow (ab)(ab) = \varepsilon$, contradicting (3). **Or** $c \neq b \Rightarrow (ab)(ac) = (ac)(bc)$, contradicting (2)

Case 2: If $i > 2$: β_{i-1} must contain c, otherwise β_{i-1} and β_i are disjoint $\beta_1 \cdots \beta_{i-2}\beta_i\beta_{i-1} \cdots \beta_r = \varepsilon$, contradicting (1). So $\beta_{i-1} = (dc)$ where $d \neq a$. But then $\beta_{i-1}\beta_i = (dc)(ac) = (ad)(dc)$, contradicting (1).

Therefore, no such odd r exists, so r must be even. $\square$

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 2-cycles must have an even (odd) number of 2-cycles.

Proof:

$\beta_1\beta_2\cdots\beta_r = \gamma_1\gamma_2\cdots\gamma_s$ implies: $\varepsilon = \gamma_1\gamma_2\cdots\gamma_s\beta_r\cdots\beta_2\beta_1$

Since 2-cycles are self-inverse: $\beta_i^{-1} = \beta_i$

By the Lemma, $s + r$ must be even, so r and s have same parity. $\square$

Significance: This allows unambiguous classification of permutations as "even" or "odd"

Even and Odd Permutations - Definitions

Even Permutation: A permutation that can be expressed as a product of an even number of 2-cycles.

Odd Permutation: A permutation that can be expressed as a product of an odd number of 2-cycles.

Examples:

- $(123) = (13)(12)$ → even (2 transpositions)
- (12) → odd (1 transposition)
- $(1234) = (14)(13)(12)$ → odd (3 transpositions)
- $\varepsilon = (12)(12)$ → even (2 transpositions)

Theorem 5.6: The set of even permutations in S_n forms a subgroup of S_n.

Proof: Must verify subgroup criteria: **Identity** $\varepsilon = (12)(12)$ is even so not empty.

Closure under Products: If α and β are even, then $\alpha\beta$ is even

- $\alpha =$ product of $2k$ transpositions and $\beta =$ product of $2j$ transpositions
- $\alpha\beta =$ product of $2k + 2j = 2(k + j)$ transpositions → even

Closure under Inverses: If α is even, then α^{-1} is even

- $\alpha = \tau_1\tau_2 \cdots \tau_{2k}$ (τ_i are transpositions)
- $\alpha^{-1} = \tau_{2k} \cdots \tau_2\tau_1 = \tau_{2k} \cdots \tau_2\tau_1$ (since $\tau_i^{-1} = \tau_i$)
- α^{-1} is product of $2k$ transpositions → even $\square$

Alternating Groups - Definition and Order

Definition: The alternating group of degree n, denoted A_n, is the group of all even permutations of n symbols.

Theorem 5.7: For $n > 1$, $|A_n| = \frac{n!}{2}$

Theorem 5.7: For $n > 1$, $|A_n| = \frac{n!}{2}$

Proof: Define $f : S_n \to S_n$ by $f(\alpha) = (12)\alpha$. **Claim:** f is a bijection.

f **is one-to-one:** If $f(\alpha) = f(\beta)$, then $(12)\alpha = (12)\beta$, which implies $\alpha = \beta$ by left cancellation.

f **is onto:** If $\beta \in S_n$, then $(12)\beta \in S_n$ and $f((12)\beta) = (12)((12)\beta) = \beta$.

Observation: The restriction $f : A_n \to A_n^c$ (where A_n^c denotes the set of odd permutations) is a bijection between even and odd permutations: If $\alpha \in A_n$ (even), then $(12)\alpha$ has one additional transposition, making it odd. Conversely, if α is odd, then $(12)\alpha$ is even. **So** $|A_n| = |A_n^c|$.

Since $S_n = A_n \cup A_n^c$ and the sets are disjoint we have:
$n! = |S_n| = |A_n| + |A_n^c| = 2|A_n|$

Therefore: $|A_n| = \frac{n!}{2}$ $\square$