MATH 343 · GROUP THEORY · CHAPTER 5

Permutation Groups

Array and Cycle Notation · Orders of Permutations · Even and Odd Permutations · with Interactive Exercises

Fahd M. Alshammari

Part 1 — Permutations and Their Products

GOAL. Meet the groups that were studied first, and learn to compute in them.

- Permutations, and groups made of them
- Array notation, and composition from right to left
- The symmetric groups S_3 and S_n
- D_4 as a group of permutations of four corners

Permutations and Permutation Groups

DEFINITIONS. A **permutation** of a set A is a function from A to A that is both one-to-one and onto. A **permutation group** of A is a set of permutations of A that forms a group under function composition.

- We work with finite sets, usually $A = \{1,2, \dots, n\}$
- The identity is the identity map ε; the inverse of α is the inverse function α^{-1}

Array Notation

EXAMPLE. The permutation α of $\{1,2,3,4\}$ with $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$, $\alpha(4) = 4$ is written

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix},$$

with $\alpha(j)$ directly below j. Likewise, on $\{1, \dots, 6\}$,

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

- Each symbol appears exactly once in the bottom row

Composition Is Read from Right to Left

DEFINITION. The product $\gamma\sigma$ is the composite: $(\gamma\sigma)(x) = \gamma\big(\sigma(x)\big)$, so σ acts **first**. For

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}, \qquad \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix},$$

we get $(\gamma\sigma)(1) = \gamma\big(\sigma(1)\big) = \gamma(2) = 4$, and in full

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}.$$

WARNING. Some books compose left to right. This course, like Gallian, always composes right to left.

The Symmetric Group S_3

EXAMPLE. S_3 is the set of all one-to-one functions from $\{1,2,3\}$ to itself. Under composition it is a group with six elements:

$$\varepsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \quad \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

- Check one: $(\alpha\beta)(2) = \alpha\big(\beta(2)\big) = \alpha(3) = 1$

S_3 Is Non-Abelian

EXAMPLE. Computing $\beta\alpha$ directly,

$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \alpha^2\beta \neq \alpha\beta,$$

so S_3 is non-Abelian. The relation $\beta\alpha = \alpha^2\beta$ computes other products with no arrays at all:

$$\beta\alpha^2 = (\beta\alpha)\alpha = \left(\alpha^2\beta\right)\alpha = \alpha^2(\beta\alpha) = \alpha^2\alpha^2\beta = \alpha^4\beta = \alpha\beta.$$

- The last step uses $\alpha^3 = \varepsilon$

The Symmetric Group S_n

EXAMPLE. The set of all permutations of $\{1,2,\ldots,n\}$ is the **symmetric group of degree** n, written S_n.

There are n choices for $\alpha(1)$, then $n-1$ for $\alpha(2)$ since α is one-to-one, then $n-2$ for $\alpha(3)$, and so on:

$$|S_n| = n(n-1)\cdots 3\cdot 2\cdot 1 = n!$$

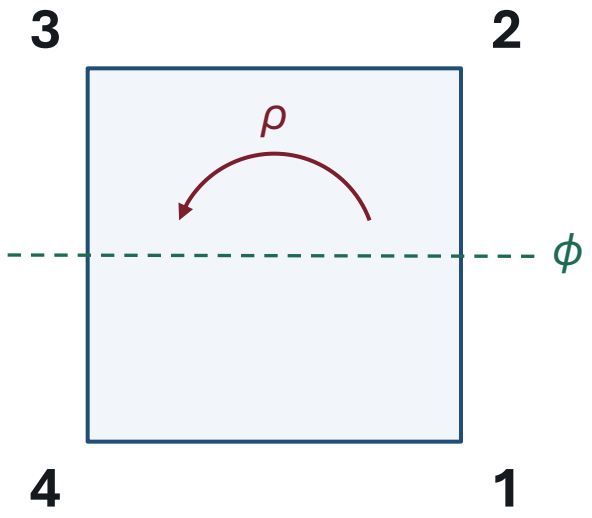
- S_n is non-Abelian for every $n \geq 3$ (Exercise 51)
- It is rich in subgroups: S_4 has 30 and S_5 has 156

D_4 as Permutations of the Corners

EXAMPLE. Label the corner positions as shown, and keep the labels fixed. The rotation ρ by 90° counterclockwise and the reflection φ in the horizontal axis permute them:

$$\rho = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}, \quad \varphi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

They generate D_4, so D_4 is a subgroup of S_4: 8 of its 24 elements.



The labels mark positions, which stay put. The square moves.

Part 2 — Cycle Notation

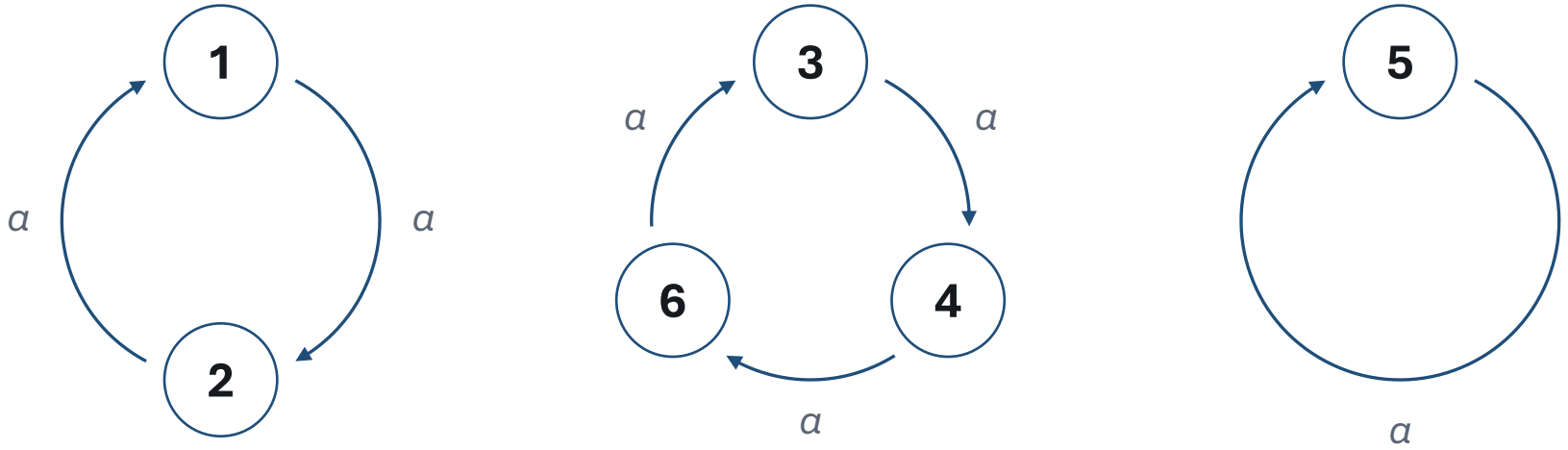
GOAL. A notation that shows at a glance what a permutation does, and makes products quick to compute.

- Cycles and m-cycles, with Gallian's picture
- Multiplying cycles: keep moving, right to left
- Disjoint cycle form

Cycle Notation

EXAMPLE. Follow each symbol under

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



Leave out the arrows and write α = (1, 2)(3, 4, 6)(5).

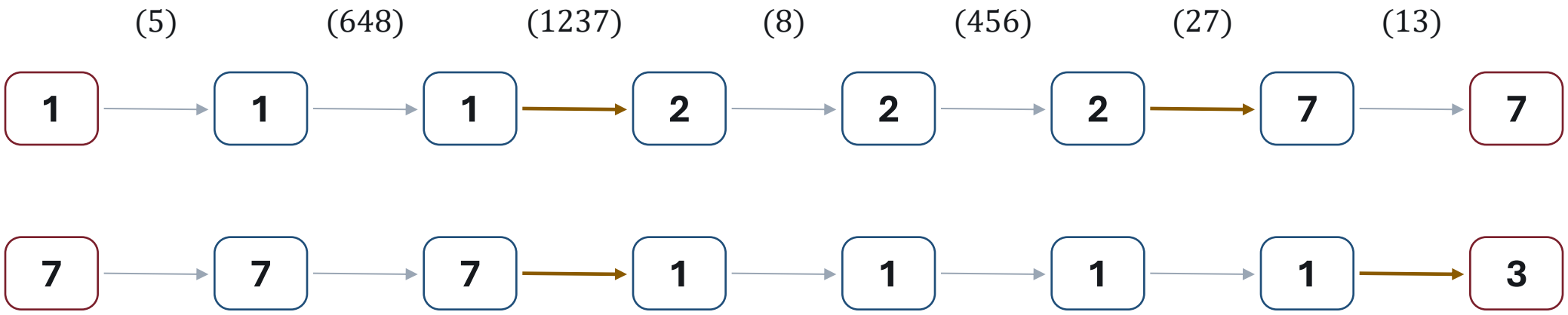
Cycles — Definition and Conventions

DEFINITION. An expression $(a_1, a_2, \ldots, a_m)$ is a **cycle of length** m, or an m**-cycle**. It sends $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_m \mapsto a_1$ and fixes every other symbol.

- A cycle can start anywhere: $\beta = (2,3,1,5)(6,4) = (4,6)(3,1,5,2)$
- 1-cycles are left out: $(1,2)(3)(4,5) = (1,2)(4,5)$
- The identity keeps one, say $\varepsilon = (1)$
- With single digits the commas are dropped: $(13)(27)(456)$

Multiplying Cycles — Keep Moving

EXAMPLE. In S_8 let $\alpha = (13)(27)(456)(8)$ and $\beta = (1237)(648)(5)$. To find $\alpha\beta$, send each symbol through all seven cycles, from right to left:



Amber: that cycle moves the symbol. Grey: it fixes it. So 1 ↦ 7 and 7 ↦ 3; carrying on the same way, αβ = (1732)(48)(56).

Multiplying Cycles — a Second Example

EXAMPLE. Here

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{bmatrix} = (12)(3)(45),$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} = (153)(24).$$

- (24) fixes 1, (153) sends 1 to 5, (45) sends 5 to 4, and (3) and (12) fix 4: so $\alpha\beta$ sends $1 \mapsto 4$
- Continuing the same way, $\alpha\beta = (14)(253)$

Part 3 — Disjoint Cycles and Orders

GOAL. Prove that disjoint cycle form always exists and that disjoint cycles commute, then read off the order of any permutation.

- Theorem 5.1: every permutation is a product of disjoint cycles
- Theorem 5.2: disjoint cycles commute
- Theorem 5.3: the order is the lcm of the cycle lengths
- Counting the elements of a given order in S_n

Theorem 5.1 — Products of Disjoint Cycles

THEOREM 5.1. Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

PROOF. Let α be a permutation of $A = \{1, \dots, n\}$. Choose $a_1 \in A$ and put $a_2 = \alpha(a_1)$, $a_3 = \alpha^2(a_1)$, and so on. As A is finite, some $\alpha^i(a_1) = \alpha^j(a_1)$ with $i < j$, so $\alpha^{j-i}(a_1) = a_1$. Stopping at the first return, $a_1 = \alpha^m(a_1)$, gives

$$\alpha = (a_1, a_2, \dots, a_m) \cdots .$$

Proof of Theorem 5.1 — the Cycles Are Disjoint

PROOF (CONTINUED). If some $b_1 \in A$ is not yet used, build $(b_1, b_2, \ldots, b_k)$ from it in the same way. It shares nothing with the first cycle: if $\alpha^i(a_1) = \alpha^j(b_1)$, then $b_1 = \alpha^{i-j}(a_1)$ would already be one of the a's.

Continue until A is used up:

$$\alpha = (a_1, \ldots, a_m)(b_1, \ldots, b_k) \cdots (c_1, \ldots, c_s).$$

Theorem 5.2 — Disjoint Cycles Commute

THEOREM 5.2. If the cycles $\alpha = (a_1, \ldots, a_m)$ and $\beta = (b_1, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

PROOF. Compare both sides at each symbol x. If $x = a_i$ then, as β fixes every a,

$$(\alpha\beta)(a_i) = \alpha(a_i) = a_{i+1} \quad \text{and} \quad (\beta\alpha)(a_i) = \beta(a_{i+1}) = a_{i+1},$$

reading a_{m+1} as a_1. The b's work the same way, and a symbol fixed by both cycles is fixed by both products.

Theorem 5.3 — the Order of a Permutation

THEOREM 5.3 (RUFFINI, 1799). 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**.

- A cycle of length m has order m
- The hypothesis is disjoint cycle form: overlapping cycles must be rewritten first

Proof of Theorem 5.3

- **PROOF (TWO CYCLES).** Let α, β be disjoint cycles of lengths m, n, say $\alpha = (a_1, \dots, a_m)$ and $\beta = (b_1, \dots, b_n)$ .Let $k = \text{lcm}(m, n)$ .Then $\alpha^k = \beta^k = \varepsilon$,and as $\alpha\beta = \beta\alpha$, $(\alpha\beta)^k = \alpha^k\beta^k = \varepsilon$ .So $t = |\alpha\beta|$ divides k (Corollary 2 of Theorem 4.1).
- Also $\varepsilon = (\alpha\beta)^t = \alpha^t\beta^t$ .Since α^t moves only a's and β^t only b's, and for all possible i and j:

$$\alpha^t(a_i) = \alpha^t\beta^t(a_i) = \varepsilon(a_i) = a_i$$

$$\beta^t(b_i) = \beta^t\alpha^t(b_i) = \varepsilon(b_i) = b_i$$

- So both α^t and β^t are ε. So $m \mid t$ and $n \mid t$, giving $k \leq t$. Hence $t = k$.
- More than two cycles: the same argument, one cycle at a time

Orders at a Glance

EXAMPLE. By Theorem 5.3,

$$|(132)(45)| = \operatorname{lcm}(3,2) = 6,$$
$$|(1432)(56)| = \operatorname{lcm}(4,2) = 4,$$
$$|(123)(456)(78)| = \operatorname{lcm}(3,3,2) = 6.$$

WARNING. In $(123)(145)$ the cycles overlap. Rewrite first: $(123)(145) = (14523)$, of order 5 — not $\operatorname{lcm}(3,3) = 3$.

The Orders of the Elements of S_7

EXAMPLE. Write (n) for an n-cycle and omit 1-cycles. The 15 possible cycle structures in S_7 give every order that occurs: 1, 2, 3, 4, 5, 6, 7, 10 and 12.

structure	order	structure	order	structure	order
(7)	7	(4)(2)	4	(3)	3
(6)	6	(4)	4	(2)(2)(2)	2
(5)(2)	10	(3)(3)	3	(2)(2)	2
(5)	5	(3)(2)(2)	6	(2)	2
(4)(3)	12	(3)(2)	6	ε	1

Counting the Elements of Order 12 in S_7

EXAMPLE. By the table, an element of order 12 in S_7 has the form $(a_1a_2a_3a_4)(a_5a_6a_7)$.

- $7 \cdot 6 \cdot 5 \cdot 4$ ways to fill the 4-cycle, but each 4-cycle is counted 4 times: $(2741) = (7412) = (4127) = (1274)$
- $3 \cdot 2 \cdot 1$ ways to fill the 3-cycle, each counted 3 times

So the number of elements of order 12 is

$$\frac{(7 \cdot 6 \cdot 5 \cdot 4)(3 \cdot 2 \cdot 1)}{4 \cdot 3} = 420.$$

Counting the Elements of Order 3 in S_7

EXAMPLE. Order 3 in S_7 needs the form $(a_1a_2a_3)$ or $(a_1a_2a_3)(a_4a_5a_6)$.

- One 3-cycle: $(7 \cdot 6 \cdot 5)/3 = 70$
- Two 3-cycles: $(7 \cdot 6 \cdot 5)(4 \cdot 3 \cdot 2)/(3 \cdot 3 \cdot 2) = 280$, the extra 2 because the two cycles can be written in either order
- Total: $70 + 280 = 350$ elements of order 3

REMARK. For k cycles of the same length, also divide by $k!$: there are $(7 \cdot 6)(5 \cdot 4)(3 \cdot 2)/(2 \cdot 2 \cdot 2 \cdot 3!) = 105$ elements of the form $(a_1a_2)(a_3a_4)(a_5a_6)$.

Part 4 — Even and Odd Permutations

GOAL. Show that every permutation has a well-defined parity, and meet the alternating groups.

- Theorem 5.4: every permutation is a product of 2-cycles
- A lemma and Theorem 5.5: the number of 2-cycles is always even or always odd
- Theorems 5.6 and 5.7: the even permutations form A_n, of order $n!/2$

2-Cycles, or Transpositions

DEFINITION. A 2-cycle (ab), with $a \neq b$, is also called a **transposition**: it interchanges a and b and fixes everything else.

EXAMPLE. Cycles can be split into 2-cycles:

$$(12345) = (15)(14)(13)(12),$$

$$(1632)(457) = (12)(13)(16)(47)(45).$$

- Check the first at 2: (12) sends 2 to 1, (13) sends 1 to 3, and (14), (15) fix 3 — so $2 \mapsto 3$

Theorem 5.4 — Product of 2-Cycles

THEOREM 5.4. Every permutation in S_n, $n > 1$, is a product of 2-cycles.

PROOF. The identity is $(12)(12)$. Otherwise write the permutation in disjoint cycle form (Theorem 5.1) and split each cycle as

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

WARNING. The order of the factors matters: $(a_1 a_2)(a_1 a_3) \cdots (a_1 a_k)$ is the inverse cycle $(a_1 a_k \cdots a_2)$.

The Decomposition Is Not Unique

EXAMPLE. The same 5-cycle, written two different ways:

$$(12345) = (54)(53)(52)(51),$$
$$(12345) = (54)(52)(21)(25)(23)(13).$$

Four 2-cycles one way, six the other. The **number** of 2-cycles can change; its **parity** cannot — that is Theorem 5.5.

A Lemma — the Identity Is Even

LEMMA. If $\varepsilon = \beta_1\beta_2 \cdots \beta_r$, where the β's are 2-cycles, then r is even.

PROOF. $r \neq 1$, since a 2-cycle is not ε, and $r = 2$ is even; induct on r. Let a be a symbol of the rightmost factor, $\beta_r = (ab)$. The factor just before it has one of four forms, and each can be rewritten:

$$(ab)(ab) = \varepsilon, \qquad (bc)(ab) = (ac)(bc),$$

$$(ac)(ab) = (ab)(bc), \qquad (cd)(ab) = (ab)(cd).$$

Proof of the Lemma, Continued

In the first case, delete the pair: then ε is a product of $r-2$ two-cycles, so $r-2$ is even by induction. In the other three cases, rewrite: still r factors, still ε, but the rightmost a is now one factor further left.

Repeat. The first case must occur eventually: otherwise a would end up only in β_1, and the product would move a — impossible for ε. So $r-2$, and hence r, is even.

Theorem 5.5 — Always Even or Always Odd

THEOREM 5.5. If a permutation α can be written as a product of an even (odd) number of 2-cycles, then every such decomposition of α has an even (odd) number of 2-cycles.

PROOF. Say $\alpha = \beta_1 \cdots \beta_r = \gamma_1 \cdots \gamma_s$, all 2-cycles. A 2-cycle is its own inverse, so

$$\varepsilon = \gamma_1 \cdots \gamma_s \beta_r^{-1} \cdots \beta_1^{-1} = \gamma_1 \cdots \gamma_s \beta_r \cdots \beta_1.$$

By the lemma, $r + s$ is even, so r and s are both even or both odd.

Even and Odd Permutations

DEFINITIONS. A permutation is **even** if it can be written as a product of an even number of 2-cycles, and **odd** if it can be written as a product of an odd number. By Theorems 5.4 and 5.5, every permutation is one or the other, never both.

EXAMPLE. $(12345) = (15)(14)(13)(12)$ is even; $(1632)(457) = (12)(13)(16)(47)(45)$ is odd.

- By the formula in Theorem 5.4, a k-cycle is a product of $k - 1$ two-cycles

Theorem 5.6 — Even Permutations Form a Group

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

PROOF. The identity is even, as $\varepsilon = (12)(12)$. If α and β are products of r and s two-cycles with r, s even, then $\alpha\beta$ is a product of $r + s$ two-cycles, and $r + s$ is even. So the set is closed; as S_n is finite, the Finite Subgroup Test (Theorem 3.3) finishes the proof.

- Directly: if $\alpha = \beta_1 \cdots \beta_r$, then $\alpha^{-1} = \beta_r \cdots \beta_1$, with the same number of factors

The Alternating Group A_n

DEFINITION. The group of even permutations of n symbols is the **alternating group of degree** n, written A_n.

THEOREM 5.7. For $n > 1$, A_n has order $n!/2$.

PROOF. For each odd α, $(12)\alpha$ is even, and $(12)\alpha \neq (12)\beta$ whenever $\alpha \neq \beta$, by cancellation.

- So there are at least as many even permutations as odd ones.
- The same map sends distinct even permutations to distinct odd ones.
- So the two sets have the same size, and each has $n!/2$ elements.

Where the Names Come From

A polynomial in $x_1, \ldots, x_n$ is **symmetric** if transposing any two variables leaves it unchanged, and **alternating** if every such transposition changes its sign:

$$x_1 x_2 x_3 \text{ is symmetric;}$$

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \text{ is alternating.}$$

- Every permutation is a product of transpositions, so symmetric polynomials are unchanged by all of S_n
- An even permutation changes the sign an even number of times, so alternating polynomials are unchanged by all of A_n

The Alternating Group A_4

EXAMPLE. A_4 has $4!/2 = 12$ elements:

- the identity ε
- three products of two disjoint 2-cycles: $(12)(34)$, $(13)(24)$, $(14)(23)$
- eight 3-cycles: (123), (132), (124), (142), (134), (143), (234), (243)

So every element of A_4 has order 1, 2 or 3. Gallian's Table 5.1 is its full multiplication table.

Why Permutation Groups Matter

- Until about 1850, groups of permutations were the only groups anyone studied
- Cayley's theorem (Chapter 6): every group is a group of permutations, up to isomorphism
- A_4 returns in Chapter 7 as a group of order 12 with no subgroup of order 6
- A_5, of order 60, is the smallest non-Abelian simple group — the key to why the general quintic has no formula in radicals

What to Take Away

- Compose right to left: $(\alpha\beta)(x) = \alpha\big(\beta(x)\big)$
- Every permutation is a product of disjoint cycles, and disjoint cycles commute
- $|\alpha|$ is the lcm of the cycle lengths — in disjoint cycle form only
- Every permutation is even or odd, never both; a k-cycle is a product of $k - 1$ two-cycles
- A_n, the even permutations, is a subgroup of S_n of order $n!/2$