Group Theory Exercises 3

Jason Sass

July 24, 2023

Permutation Groups

Exercise 1. Find the inverse of each permutation in S_3.

Solution.

Let $S = \{1, 2, 3\}$.

The symmetric group of 3 symbols, denoted S_3, contains $|S_3| = 3! = 6$ permutations of S.

The permutations are:

I. (1 2 3)

$$\text{id} = id^{-1} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

II. (1 3 2)

$$\alpha = \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \text{ keep position 1 fixed, and swap 2 and 3}$$

III. (2 1 3)

$$\beta = \beta^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \text{ keep position 3 fixed, and swap 1 and 2}$$

IV. (2 3 1)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \text{ rotate each position once to the left}$$

V. (3 1 2)

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \text{ rotate each position once to the right}$$

VI. (3 2 1)

$$\tau = \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \text{ keep position 2 fixed, and swap 1 and 3}$$

$\square$

Exercise 2. Verify that $(ab)^{-1} \neq a^{-1}b^{-1}$ in S_3.

$$\text{Let } a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\text{Let } b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Solution. Observe that

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$(ab)^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$a^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$b^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$a^{-1}b^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Therefore, $(ab)^{-1} \neq a^{-1}b^{-1}$. $\square$

Exercise 3. Analyze the order of the group $(S_3, \circ)$.

Solution. Observe that S_3 is the symmetric group of order $3! = 6$ under function composition.

The Cayley table for $(S_3, \circ)$ is shown below.

$\circ$	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	(1)	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	(1)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	(1)	(1 2 3)

The cyclic subgroups generated by each element are shown below.
$\langle(1)\rangle = \{(1)\}$ and $|(1)| = 1$
$\langle(1\ 2)\rangle = \{(1), (1\ 2)\}$ and $|(1\ 2)| = 2$
$\langle(1\ 3)\rangle = \{(1), (1\ 3)\}$ and $|(1\ 3)| = 2$
$\langle(2\ 3)\rangle = \{(1), (2\ 3)\}$ and $|(2\ 3)| = 2$
$\langle(1\ 2\ 3)\rangle = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ and $|(1\ 2\ 3)| = 3$
$\langle(1\ 3\ 2)\rangle = \{(1), (1\ 3\ 2), (1\ 2\ 3)\}$ and $|(1\ 3\ 2)| = 3$
There are no generators of S_3, so S_3 is not cyclic.

The order of the inverse of an element is the same as the order of the element.
$|(1)| = |(1)^{-1}| = |(1)| = 1$
$|(1\ 2)| = |(1\ 2)^{-1}| = |(1\ 2)| = 2$
$|(1\ 3)| = |(1\ 3)^{-1}| = |(1\ 3)| = 2$
$|(2\ 3)| = |(2\ 3)^{-1}| = |(2\ 3)| = 2$
$|(1\ 2\ 3)| = |(1\ 2\ 3)^{-1}| = |(1\ 3\ 2)| = 3$
$|(1\ 3\ 2)| = |(1\ 3\ 2)^{-1}| = |(1\ 2\ 3)| = 3$

□

Exercise 4. Show that the solution to the linear equation $ax = b$ may not be the same as the solution to the equation $ya = b$ for given elements a and b of a group.

Solution. Consider the symmetric group $(S_3, \circ)$.
Let

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

and

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

The equation $ax = b$ has solution

$$x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

The equation $ya = b$ has solution

$$y = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Observe that $x \neq y$. □

Exercise 5. Let $G = \{id, \sigma, \tau, \mu\}$ be a subset of the symmetric group $(S_5, \circ)$ where

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

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

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

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

Show that $(G, \circ)$ is a subgroup of S_5.

Solution. Each element of G is a permutation of the set $X = \{1, 2, 3, 4, 5\}$, so G is a subset of S_5, the symmetric group on 5 symbols.

The Cayley table is below.

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

We prove G is a subgroup of S_5.

Since $id \in G$, then $G \neq \emptyset$.

Since $|G| = 4$, then G is a finite set.

Since $G \neq \emptyset$ and G is finite and G is a subset of S_5, then G is a nonempty finite subset of S_5.

The Cayley multiplication table shows that G is closed under function composition.

Since G is a nonempty finite subset of S_5 and G is closed under function composition, then by the finite subgroup test, G is a subgroup of S_5, so $G < S_5$.

Therefore, G is a permutation group on X.

Observe that G is abelian even though S_5 is non-abelian. □

Cycle notation for permutations

Exercise 6. Write the permutation below using cycle notation.

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

Solution. Observe that $\sigma = (1\ 6\ 2\ 3\ 5\ 4)(7) = (1\ 6\ 2\ 3\ 5\ 4)$.

We see that σ is a cycle of length 6.

In cycle notation a loop(1 cycle = a single element that maps to itself) doesn't change the permutation, so there is no need to write it explicitly.

Therefore, we omit the loop when writing a permutation using cycle notation. □

Exercise 7. Write the permutation below using cycle notation.

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

Solution. Observe that $\tau = (1)(2\ 4\ 3)(5)(6) = (2\ 4\ 3)$.

We see that τ is a 3 cycle. □

Exercise 8. A cycle can be written in multiple ways.

Let $a = (1\ 2\ 5)$

Solution. Observe that $a = (1\ 2\ 5) = (5\ 1\ 2) = (2\ 5\ 1)$. □

Exercise 9. Compute the inverse of the cycle below.

Let $\tau = (1\ 3\ 5)$

Solution. Observe that $\tau^{-1} = (1\ 5\ 3) = (3\ 1\ 5) = (5\ 3\ 1)$.

Note that if we visualize τ as a cycle with elements in order clockwise, then τ^{-1} is the same elements of τ listed counter-clockwise. □

Exercise 10. Write the permutation below using cycle notation.

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

Solution. There are many ways to decompose this permutation.

Observe that

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

The conventional way is to write the smallest number first, so we can write $\alpha = (1\ 2\ 4\ 3)(5\ 6)$.

We see that α is a product of a 4 cycle and a 2 cycle. □

Exercise 11. Write the permutation below using cycle notation.

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

Solution. Observe that

$$a = (1\ 2\ 4\ 5\ 3)$$

We see that a is a 5 cycle. $\square$

Exercise 12. Write the permutation below using cycle notation.

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

Solution. There are many ways to write this permutation.
Observe that

$$b = (1\ 4)(2)(3\ 5) = (1\ 4)(3\ 5)$$

We see that b is a product of 2 cycles. $\square$

Exercise 13. Write the permutation below using cycle notation.

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

Solution. There are many ways to write this permutation.
Observe that

$$c = (1\ 3)(2\ 5)(4) = (1\ 3)(2\ 5)$$

We see that c is a product of 2 cycles. $\square$

Exercise 14. Write the permutation below using cycle notation.

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

Solution.
Observe that

$$d = (1)(2\ 4)(3)(5) = (2\ 4)$$

We see that d is a 2 cycle(transposition). $\square$

Exercise 15. Multiply the below permutations.

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Solution. Observe that $ab = (1\ 3\ 2)(1\ 3) = (1\ 2)(3) = (1\ 2)$ and $b = (1\ 3)(1\ 3\ 2) = (1)(2\ 3) = (2\ 3)$.
We see that $ab \neq ba$. $\square$

Exercise 16. Multiply the below permutations.
$a = (1\ 3\ 5\ 2)$
$b = (2\ 5\ 6)$.

Solution. Observe that

$$ab = (1\ 3\ 5\ 2)(2\ 5\ 6) = \begin{pmatrix} 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 5 & 6 \\ 5 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 & 6 & 2 \\ 3 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\ 3\ 5\ 6)(2) = (1\ 3\ 5\ 6)$$

Therefore, $ab = (1\ 3\ 5\ 6)$. □

Exercise 17. Multiply the below permutations.
$a = (1\ 3\ 5\ 2)$
$b = (1\ 6\ 3\ 4)$.

Solution. We compute $ab = (1\ 3\ 5\ 2)(1\ 6\ 3\ 4) = (1\ 6\ 5\ 2)(3\ 4)$. □

Exercise 18. Multiply the below permutations.
$a = (1\ 3\ 4\ 5)$
$b = (2\ 3\ 4)$.

Solution. We compute $ab = (1\ 3\ 4\ 5)(2\ 3\ 4) = (1\ 3\ 5)(2\ 4)$. □

Exercise 19. Let $a = (1\ 3\ 5)$ and $b = (2\ 7)$.
Then a and b are disjoint cycles.

Solution. Since cycles a and b have no elements in common, then a and b are disjoint cycles.
Observe that $ab = (1\ 3\ 5)(2\ 7)$ and $ba = (2\ 7)(1\ 3\ 5) = (1\ 3\ 5)(2\ 7)$.
Therefore, $ab = ba$, so a and b commute. □

Exercise 20. Let $a = (1\ 3\ 5)$ and $b = (3\ 4\ 7)$.
Then a and b are not disjoint cycles.

Solution. Since 3 is a common element in cycles a and b, then a and b are not disjoint cycles.
Observe that $ab = (1\ 3\ 5)(3\ 4\ 7) = (1\ 3\ 4\ 7\ 5)$ and $ba = (3\ 4\ 7)(1\ 3\ 5) = (1\ 4\ 7\ 3\ 5)$.
Therefore, $ab \neq ba$, so a and b do not commute. □

Exercise 21. Compute the products and write as a decomposition of disjoint cycles.

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

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

Solution. Observe that

$\sigma = (1\ 6\ 2\ 4)(3)(5) = (1\ 6\ 2\ 4)$ is a 4 cycle
and
$\tau = (1\ 3)(2)(4\ 5\ 6) = (1\ 3)(4\ 5\ 6)$ is a product of 2 disjoint cycles
and
$\sigma\tau = (1\ 3\ 6)(2\ 4\ 5)$ is a product of 2 disjoint cycles
and
$\tau\sigma = (1\ 4\ 3)(2\ 5\ 6)$ is a product of 2 disjoint cycles. □

Exercise 22. Compute $(1\ 6)(2\ 5\ 3)$ in different ways.

Solution. Since $(1\ 6)(2\ 5\ 3) = (1\ 6)(2\ 3)(2\ 5) = (1\ 6)(4\ 5)(2\ 3)(4\ 5)(2\ 5)$, then there is no unique representation of a permutation as a product of transpositions. Hence, there are many ways to write a permutation as a product of transpositions. □

Exercise 23. Compute the product of the cycles below in S_8.
$(1\ 4\ 5)(7\ 8)(2\ 5\ 7)$.

Solution. Let $\sigma = (1\ 4\ 5)(7\ 8)(2\ 5\ 7)$.
Then $\sigma = (1\ 4\ 5\ 8\ 7\ 2)$. □

Exercise 24. Compute the product of the cycles below in S_8.
$(1\ 3\ 2\ 7)(4\ 8\ 6)$.

Solution. Let $\sigma = (1\ 3\ 2\ 7)(4\ 8\ 6)$.
Then σ is a product of disjoint cycles. □

Exercise 25. Compute the product of the cycles below in S_8.
$(1\ 2)(4\ 7\ 8)(2\ 1)(7\ 2\ 8\ 1\ 5)$.

Solution. Let $\sigma = (1\ 2)(4\ 7\ 8)(2\ 1)(7\ 2\ 8\ 1\ 5)$.
Then

$$\begin{aligned}
\sigma &= (1\ 2)(4\ 7\ 8)(2\ 1)(7\ 2\ 8\ 1\ 5) \\
&= (1\ 2)(2\ 1)(4\ 7\ 8)(7\ 2\ 8\ 1\ 5) \\
&= (1\ 2)(1\ 2)(4\ 7\ 8)(7\ 2\ 8\ 1\ 5) \\
&= id(4\ 7\ 8)(7\ 2\ 8\ 1\ 5) \\
&= (4\ 7\ 8)(7\ 2\ 8\ 1\ 5) \\
&= (1\ 5\ 8)(2\ 4\ 7).
\end{aligned}$$

□

Exercise 26. Compute the order of the cycle below in S_8.
$(1\ 4\ 5\ 7)$.

Solution. Let $\sigma = (1\ 4\ 5\ 7)$.
Then $\sigma^2 = (1\ 5)(4\ 7)$ and
$\sigma^3 = (1\ 7\ 5\ 4) = (1\ 5)(1\ 7)(4\ 5)$ and

$\sigma^4 = (1) = id$.

Thus, $|\sigma| = 4$.

Since the length of σ is 4, then the order of σ is 4. □

Exercise 27. Compute the order of the permutation below in S_8.

(4 5)(2 3 7).

Solution. Let $\sigma = (4\ 5)(2\ 3\ 7) = (2\ 3\ 7)(4\ 5)$.

Then $\sigma^2 = (2\ 7\ 3)$ and

$\sigma^3 = (4\ 5)$ and

$\sigma^4 = (2\ 3\ 7)$ and

$\sigma^5 = (2\ 7\ 3)(4\ 5)$ and

$\sigma^6 = (1) = id$.

Thus, $|\sigma| = 6$.

The order of σ is the least common multiple of the orders of its disjoint cycles.

Therefore, $|\sigma| = lcm(3, 2) = 6$. □

Exercise 28. Compute the order of the permutation below in S_8.

(1 4)(3 5 7 8).

Solution. Let $\tau = (1\ 4)(3\ 5\ 7\ 8)$.

Then $\tau^2 = (3\ 7)(5\ 8)$ and

$\tau^3 = (1\ 4)(3\ 8\ 7\ 5)$ and

$\tau^4 = (1) = id$.

Thus, $|\tau| = 4$.

The order of τ is the least common multiple of the orders of its disjoint cycles.

Therefore, $|\tau| = lcm(2, 4) = 4$. □

Exercise 29. Compute the order of the permutation below in S_8.

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

Solution. Since $\sigma = (1\ 8)(3\ 6\ 4)(5\ 7)$, then

$\sigma^2 = (3\ 4\ 6)$ and

$\sigma^3 = (1\ 8)(5\ 7)$ and

$\sigma^4 = (3\ 6\ 4)$ and

$\sigma^5 = (1\ 8)(3\ 4\ 6)(5\ 7)$ and

$\sigma^6 = (1) = id$.

Thus, $|\sigma| = 6$.

The order of σ is the least common multiple of the orders of its disjoint cycles.

Therefore, $|\sigma| = lcm(2, 3, 2) = 6$. □

Exercise 30. Compute the order of the permutation below in S_8.

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

Solution. Since $\sigma = (1\ 3\ 4)(2\ 6)(5\ 8\ 7)$, then
$\sigma^2 = (1\ 4\ 3)(5\ 7\ 8)$ and
$\sigma^3 = (2\ 6)$ and
$\sigma^4 = (1\ 3\ 4)(5\ 8\ 7)$ and
$\sigma^5 = (1\ 4\ 3)(2\ 6)(5\ 7\ 8)$ and
$\sigma^6 = (1) = id$.
Thus, $|\sigma| = 6$.

The order of σ is the least common multiple of the orders of its disjoint cycles.

Therefore, $|\sigma| = lcm(3, 2, 3) = 6$. □

Exercise 31. Compute the order of the permutation below in S_8.

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

Solution. Since $\sigma = (1\ 3\ 4\ 7\ 8\ 6\ 5\ 2)$, then
$\sigma^2 = (1\ 4\ 8\ 5)(2\ 3\ 7\ 6)$ and
$\sigma^3 = (1\ 7\ 5\ 3\ 8\ 2\ 4\ 6)$ and
$\sigma^4 = (1\ 8)(2\ 7)(3\ 6)(4\ 5)$ and
$\sigma^5 = (1\ 6\ 4\ 2\ 8\ 3\ 5\ 7)$ and
$\sigma^6 = (1\ 5\ 8\ 4)(2\ 6\ 7\ 3)$ and
$\sigma^7 = (1\ 2\ 5\ 6\ 8\ 7\ 4\ 3)$ and
$\sigma^8 = (1) = id$.
Thus, $|\sigma| = 8$.

Since σ is a cycle of length 8, then the order of σ is 8.

Therefore, $|\sigma| = 8$. □

Exercise 32. Compute the permutation product below and analyze results.
$(1\ 3\ 4\ 5)(2\ 3\ 4)$.

Solution. Let $\sigma = (1\ 3\ 4\ 5)(2\ 3\ 4)$.

Then $\sigma = (1\ 3\ 4\ 5)(2\ 3\ 4) = (1\ 3\ 5)(2\ 4) = (2\ 4)(1\ 3\ 5)$.

The order of σ is the least common multiple of the orders of its disjoint cycles, so $|\sigma| = lcm(2, 3) = 6$. □

Exercise 33. Compute the permutation product below in S_5 and analyze results.
$(1\ 2)(1\ 2\ 5\ 3)$.

Solution. Let $\sigma = (1\ 2)(1\ 2\ 5\ 3)$.

Then $\sigma = (2\ 5\ 3)$.

Since σ is a cycle of length 3, then the order of σ is $|\sigma| = 3$. □

Exercise 34. Compute the permutation product below in S_5 and analyze results.
$(1\ 4\ 3)(2\ 3)(2\ 4)$.

Solution. Let $\sigma = (1\ 4\ 3)(2\ 3)(2\ 4)$.

Then $\sigma = (1\ 4)(2\ 3)$.

The order of σ is the least common multiple of the orders of its disjoint cycles, so $|\sigma| = lcm(2, 2) = 2$. □

Exercise 35. Compute the permutation product below in S_6 and analyze results.

$(1\ 4\ 2\ 3)(3\ 4)(5\ 6)(1\ 3\ 2\ 4)$.

Solution. Let $\sigma = (1\ 4\ 3)(2\ 3)(2\ 4)$.

Then $\sigma = (1\ 2)(5\ 6)$.

The order of σ is the least common multiple of the orders of its disjoint cycles, so $|\sigma| = lcm(2, 2) = 2$. □

Exercise 36. Compute the permutation product below in S_5 and analyze results.

$(1\ 2\ 5\ 4)(1\ 3)(2\ 5)$.

Solution. Let $\sigma = (1\ 2\ 5\ 4)(1\ 3)(2\ 5)$.

Then $\sigma = (1\ 3\ 2\ 4)$.

Since σ is a cycle of length 4, then the order of σ is $|\sigma| = 4$. □

Exercise 37. Compute the permutation product below in S_5 and analyze results.

$(1\ 2\ 5\ 4)(1\ 3)(2\ 5)^2$.

Solution. Let $\sigma = (1\ 2\ 5\ 4)(1\ 3)(2\ 5)^2$.

Then $\sigma = (1\ 3\ 2\ 5\ 4)$.

Since σ is a cycle of length 5, then the order of σ is $|\sigma| = 5$. □

Exercise 38. Compute the permutation product below in S_5 and analyze results.

$(1\ 2\ 5\ 4)^{-1}(1\ 2\ 3)(4\ 5)(1\ 2\ 5\ 4)$.

Solution. Let $\sigma = (1\ 2\ 5\ 4)^{-1}(1\ 2\ 3)(4\ 5)(1\ 2\ 5\ 4)$.

Then $\sigma = (1\ 3\ 4)(2\ 5)$.

The order of σ is the least common multiple of the orders of its disjoint cycles, so $|\sigma| = lcm(3, 2) = 6$. □

Exercise 39. Compute the permutation product below in S_5 and analyze results.

$(1\ 2\ 5\ 4)^2(1\ 2\ 3)(4\ 5)$.

Solution. Let $\sigma = (1\ 2\ 5\ 4)^2(1\ 2\ 3)(4\ 5)$.

Then $\sigma = (1\ 4)(2\ 3\ 5)$.

The order of σ is the least common multiple of the orders of its disjoint cycles, so $|\sigma| = lcm(2, 3) = 6$. □

Exercise 40. Compute the permutation product below in S_5 and analyze results.

$(1\ 2\ 3)(4\ 5)(1\ 2\ 5\ 4)^{-2}$.

Solution. Let $\sigma = (1\ 2\ 3)(4\ 5)(1\ 2\ 5\ 4)^{-2}$.

Then $\sigma = (1\ 4\ 3)(2\ 5)$.

The order of σ is the least common multiple of the orders of its disjoint cycles, so $|\sigma| = lcm(3, 2) = 6$. □

Exercise 41. Compute the permutation product below in S_5 and analyze results.

$(1\ 2\ 5\ 4)^{100}$.

Solution. Let $\sigma = (1\ 2\ 5\ 4)^{100}$.

Let $\alpha = (1\ 2\ 5\ 4)$.

Since α is a cycle of length 4, then the order of α is 4, so $\alpha^4 = id$.

Observe that

$$\begin{aligned}\sigma &= (1\ 2\ 5\ 4)^{100} \\ &= \alpha^{100} \\ &= \alpha^{4\cdot 25} \\ &= (\alpha^4)^{25} \\ &= id^{25} \\ &= id \\ &= (1).\end{aligned}$$

Therefore, $\sigma = (1)$ is the identity permutation. □

Exercise 42. Compute the permutation product below in S_5 and analyze results.

$(1\ 2\ 5\ 4)^2$.

Solution. Let $\sigma = (1\ 2\ 5\ 4)^2$.

Then $\sigma = (1\ 5)(2\ 4)$.

The order of σ is the least common multiple of the orders of its disjoint cycles, so $|\sigma| = lcm(2, 2) = 2$. □

Exercise 43. Compute the permutation product below in S_7 and analyze results.

$(1\ 2\ 5\ 3\ 7)^{-1}$.

Solution. Let $\sigma = (1\ 2\ 5\ 3\ 7)^{-1}$.

Then $\sigma = (7\ 3\ 5\ 2\ 1)$.

Since σ is a cycle of length 5, then the order of σ is $|\sigma| = 5$. □

Exercise 44. Compute the permutation product below in S_7 and analyze results.

$[(1\ 2)(3\ 4)(1\ 2)(4\ 7)]^{-1}$.

Solution. Let $\sigma = [(1\ 2)(3\ 4)(1\ 2)(4\ 7)]^{-1}$.

Then $\sigma = (3\ 7\ 4)$.

Since σ is a cycle of length 3, then the order of σ is $|\sigma| = 3$. □

Exercise 45. Compute the permutation product below in S_7 and analyze results.

$[(1\ 2\ 3\ 5)(4\ 6\ 7)]^{-1}$.

Solution. Let $\sigma = [(1\ 2\ 3\ 5)(4\ 6\ 7)]^{-1}$.

Observe that

$$\begin{aligned}\sigma &= [(1\ 2\ 3\ 5)(4\ 6\ 7)]^{-1} \\ &= (4\ 6\ 7)^{-1}(1\ 2\ 3\ 5)^{-1} \\ &= (7\ 6\ 4)(5\ 3\ 2\ 1) \\ &= (4\ 7\ 6)(1\ 5\ 3\ 2).\end{aligned}$$

The order of σ is the least common multiple of the orders of its disjoint cycles, so $|\sigma| = lcm(3, 4) = 12$. □

Parity of a permutation

Exercise 46. Express the below permutation in S_5 as a product of transpositions:

$(1\ 3\ 5)(2\ 4)$.

Solution. Let $\sigma = (1\ 3\ 5)(2\ 4)$.

We start with the identity permutation id and swap 2 and 4.

Then swap 3 and 5.

Finally, swap 1 and 3.

Therefore, $\sigma = (1\ 3)(3\ 5)(2\ 4)$.

Another approach is to breakdown the 3 cycle $(1\ 3\ 5)$ by letting the first element 1 swap with each element beginning with $3, 5$.

Then $(1\ 3\ 5) = (1\ 5)(1\ 3)$.

Hence, $\sigma = (1\ 5)(1\ 3)(2\ 4)$. □

Exercise 47. A permutation has no unique representation as a product of transpositions.

Express the below permutation in S_6 as a product of transpositions in several different ways:

$(1\ 6)(2\ 5\ 3)$.

Solution. Let $\sigma = (1\ 6)(2\ 5\ 3)$.

We start with the identity permutation id and swap 2 and 5.

Then swap 2 and 3.

Finally, swap 1 and 6.

Therefore, $\sigma = (1\ 6)(2\ 3)(2\ 5)$.

Another approach is:

We start with the identity permutation id and swap 3 and 5.

Then swap 2 and 5.

Finally, swap 1 and 6.

Therefore, $\sigma = (1\ 6)(2\ 5)(3\ 5)$.

Another approach is:

We start with the identity permutation id and perform the following actions.

1. Swap 2 and 5.
2. Swap 4 and 5.
3. Swap 2 and 3.
4. Swap 4 and 5.
5. Swap 1 and 6.

Therefore, $\sigma = (1\ 6)(4\ 5)(2\ 3)(4\ 5)(2\ 5)$.

Since our convention is to apply function composition in right to left order, we write the swap actions in reverse order. □

Exercise 48. Write the permutation in S_7 below as a product of transpositions and analyze results:

$(1\ 4\ 3\ 2\ 6\ 7\ 5)$.

Solution. Let $\sigma = (1\ 4\ 3\ 2\ 6\ 7\ 5)$.

We let the first element 1 cycle all the way through this 7 cycle, so have 6 swaps of 1 with each element of this cycle, beginning with $4, 3, 2, 6, 7, 5$.

Thus, $\sigma = (1\ 5)(1\ 7)(1\ 6)(1\ 2)(1\ 3)(1\ 4)$ is a product of 6 transpositions, so σ is an even permutation. □

Exercise 49. Let $H = \{f \in S_5 : f(1) = 1\}$.

Then $(H, \circ)$ is a subgroup of $(S_5, \circ)$.

Proof. We prove $H \subset S_5$.

Since $H = \{f \in S_5 : f(1) = 1\}$, then $H \subset S_5$.

We prove $H \neq \emptyset$.

The identity function defined by

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

is an element of S_5 and $id(1) = 1$, so $id \in H$.

Therefore, $H \neq \emptyset$.

We prove H is a finite set.

Since $|S_5| = 5! = 120$, then S_5 is a finite set.

Every subset of a finite set is finite.

Since S_5 is a finite set and H is a subset of S_5, then we conclude H is finite.

Since $H \subset S_5$ and $H \neq \emptyset$ and H is finite, then H is a non-empty finite subset of S_5.

We prove H is closed under function composition.

Let $g, h \in H$.

Since $g \in H$, then $g \in S_5$ and $g(1) = 1$.

Since $h \in H$, then $h \in S_5$ and $h(1) = 1$.

Since $(S_5, \circ)$ is a group, then S_5 is closed under function composition.

Since $g \in S_5$ and $h \in S_5$, then the function $g \circ h$ defined by $(g \circ h)(x) = g(h(x))$ for all $x \in \{1, 2, 3, 4, 5\}$ is an element of S_5, so $g \circ h \in S_5$.

Since $(g \circ h)(1) = g(h(1)) = g(1) = 1$, then $(g \circ h)(1) = 1$.

Since $g \circ h \in S_5$ and $(g \circ h)(1) = 1$, then $g \circ h \in H$, so H is closed under function composition.

Since H is a non-empty finite subset of S_5 and H is closed under function composition, then by the finite subgroup test, H is a subgroup of S_5, so $(H, \circ) < (S_5, \circ)$. $\square$

Exercise 50. Find a subgroup of S_7 that contains 12 elements.

Solution. Let $\sigma = (1, 2, 3, 4)(5, 6, 7)$.

Then $|\sigma| = lcm(4, 3) = 12$, so $\langle \sigma \rangle$ is a cyclic subgroup of order 12 generated by σ. $\square$

Exercise 51. Let $H = \{\sigma \in S_5 : \sigma(5) = 5\}$.

Show that $H < S_5$ and compute $|H|$.

Solution. Let $\sigma \in H$.

Then $\sigma \in S_5$ and $\sigma(5) = 5$.

Thus, $\sigma : X \to X$ is a permutation of 5 letters, where $X = \{1, 2, 3, 4, 5\}$.

Since $\sigma(5) = 5$, then there are 4 choices for $\sigma(1)$ and for each choice there are then 3 choices for $\sigma(2)$ which then leaves 2 choices for $\sigma(3)$ and then leaves just 1 choice for $\sigma(4)$.

Hence, there are 4! different permutations, so $|H| = 4! = 24$.

To prove $H < S_5$, we use the finite subgroup test.

Since S_5 is finite and $H \subset S$, then H is finite.

Since $(1) \in H$, then H is not empty.

Let $\alpha, \beta \in H$.

Then $\alpha, \beta \in S_5$ and $\alpha(5) = 5 = \beta(5)$.

By closure of S_5, $\alpha\beta \in S_5$.

Observe that

$$\begin{aligned}(\alpha\beta)(5) &= \alpha(\beta(5)) \\ &= \alpha(5) \\ &= 5.\end{aligned}$$

Since $\alpha\beta \in S_5$ and $(\alpha\beta)(5) = 5$, then $\alpha\beta \in H$.

Therefore, H is closed under permutation multiplication.

Hence, $H < S_5$. $\square$

Exercise 52. List all subgroups of S_4.

Solution. Let $X = \{1, 2, 3, 4\}$.

Let $(S_4, \circ)$ be the symmetric group of degree 4.

Then $|S_4| = 4! = 24$, so there are 24 permutations in S_4.

We first list all 24 permutations of X.

We enumerate each choice as a branching tree to obtain:

$1234, 1243, 1324, 1342, 1423, 1432$ and
$2134, 2143, 2314, 2341, 2413, 2431$ and
$3124, 3142, 3214, 3241, 3412, 3421$ and
$4123, 4132, 4213, 4231, 4312, 4321$.

Now, we need to write these in cycle notation:

The elements in S_4 are:

$id, (34), (23), (234), (243), (24),$
$(12), (12)(34), (123), (1234), (1243), (124),$
$(132), (1342), (13), (134), (13)(24), (1324),$
$(1432), (142), (143), (14), (1423), (14)(23)$.

The element of order 1 is id, so the subgroup of order 1 is the trivial subgroup $\{id\}$.

The elements of order 2 are: $(34), (23), (24), (12), (12)(34), (13), (13)(24), (14), (14)(23)$.

Each of these elements generates a cyclic subgroup of S_4 of order 2 and all of these subgroups are the same up to isomorphism.

Thus, we have the following subgroups of order 2:

$\{id, (34)\}$
$\{id, (23)\}$
$\{id, (24)\}$
$\{id, (12)\}$
$\{id, (12)(34)\}$
$\{id, (13)\}$
$\{id, (13)(24)\}$
$\{id, (14)\}$
$\{id, (14)(23)\}$

The elements of order 3 are: $(234), (243), (123), (124), (132), (134), (142), (143)$.

Each of these elements generates a cyclic subgroup of S_4 of order 3 and all of these subgroups are the same up to isomorphism.

Thus, we have the following subgroups of order 3:

$\{id, (234), (243)\}$
$\{id, (123), (132)\}$
$\{id, (124), (142)\}$
$\{id, (134), (143)\}$

The elements of order 4 are: $(1234), (1243), (1342), (1324), (1432), (1423)$.

Each of these elements generates a cyclic subgroup of S_4 of order 4 and all of these subgroups are the same up to isomorphism.

Thus, we have the following subgroups of order 4:

$\{id, (1234), (13)(24), (4321)\}$
$\{id, (1243), (14)(23), (3421)\}$

$\{(1324), (12)(34), (1423), id\}$ □

Exercise 53. Let $\alpha, \beta \in S_n$.
Then $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.

Proof. The permutations α and β are each either even or odd.
There are 4 cases to consider.
Case 1: Suppose α, β are both even.
Then α and β have the same parity.
The parity of a permutation is the same as the parity of its inverse.
Hence, α^{-1} is even and β^{-1} is even, so α^{-1} and β^{-1} have the same parity.
The composition of two permutations of the same parity is even.
Hence, $\alpha\beta$ is even and $\alpha^{-1}\beta^{-1}$ is even.
Therefore, $\alpha\beta$ and $\alpha^{-1}\beta^{-1}$ have the same parity.
Thus, $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.
Case 2: Suppose α, β are both odd.
Then α and β have the same parity.
The parity of a permutation is the same as the parity of its inverse.
Hence, α^{-1} is odd and β^{-1} is odd, so α^{-1} and β^{-1} have the same parity.
The composition of two permutations of the same parity is even.
Hence, $\alpha\beta$ is even and $\alpha^{-1}\beta^{-1}$ is even.
Therefore, $\alpha\beta$ and $\alpha^{-1}\beta^{-1}$ have the same parity.
Thus, $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.
Case 3: Suppose α is even and β is odd.
Then α and β have opposite parity.
The parity of a permutation is the same as the parity of its inverse.
Hence, α^{-1} is even and β^{-1} is odd, so α^{-1} and β^{-1} have opposite parity.
The composition of two permutations of opposite parity is odd.
Hence, $\alpha\beta$ is odd and $\alpha^{-1}\beta^{-1}$ is odd.
Therefore, $\alpha\beta$ and $\alpha^{-1}\beta^{-1}$ have the same parity.
The composition of two permutations of the same parity is even.
Hence, $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.
Case 4: Suppose α is odd and β is even.
Then α and β have opposite parity.
The parity of a permutation is the same as the parity of its inverse.
Hence, α^{-1} is odd and β^{-1} is even, so α^{-1} and β^{-1} have opposite parity.
The composition of two permutations of opposite parity is odd.
Hence, $\alpha\beta$ is odd and $\alpha^{-1}\beta^{-1}$ is odd.
Therefore, $\alpha\beta$ and $\alpha^{-1}\beta^{-1}$ have the same parity.
The composition of two permutations of the same parity is even.
Hence, $\alpha^{-1}\beta^{-1}\alpha\beta$ is even.
Therefore, in all cases $\alpha^{-1}\beta^{-1}\alpha\beta$ is even, as desired. □

Exercise 54. If $\tau \in S_n$ has order m, then $\sigma\tau\sigma^{-1}$ has order m for all $\sigma \in S_n$.

Proof. Suppose $\tau \in S_n$ and $|\tau| = m$.
Then m is the least positive integer such that $\tau^m = (1)$.
Hence, for every $s \in \mathbb{Z}^+$ such that $\tau^s = (1)$, $m \leq s$.

Let $\sigma \in S_n$.

Since S_n is a finite group, then the element $\sigma\tau\sigma^{-1} \in S_n$ has finite order.

Let k be the order of $\sigma\tau\sigma^{-1}$.

Then k is the least positive integer such that $(\sigma\tau\sigma^{-1})^k = (1)$.

Observe that

$$\begin{aligned}(\sigma\tau\sigma^{-1})^m &= \sigma\tau^m\sigma^{-1} \\ &= \sigma(1)\sigma^{-1} \\ &= (1).\end{aligned}$$

Since $(\sigma\tau\sigma^{-1})^m = (1)$ iff $k|m$, then $k|m$.

Since $k, m \in \mathbb{Z}^+$, then this implies $k \leq m$.

Observe that

$$\begin{aligned}(1) &= (\sigma\tau\sigma^{-1})^k \\ &= \sigma\tau^k\sigma^{-1}.\end{aligned}$$

Hence, $\sigma = \sigma\tau^k$, so $\sigma(1) = \sigma\tau^k$.

By cancellation, $(1) = \tau^k$.

Thus, $m \leq k$.

Since $k \leq m$ and $m \leq k$, then $m = k$.

Therefore, $|\sigma\tau\sigma^{-1}| = m$. ∎

Exercise 55. Let $n \geq 1$.

Let $\sigma \in S_n$.

Then σ can be written as a product of at most $n - 1$ transpositions.

Proof. Either σ is the identity permutation or it is not.

We consider these cases separately.

Case 1: Suppose $\sigma = id$.

Since the identity permutation has no 2 cycles, then id can be written as a product of zero transpositions.

Thus, σ can be written as a product of zero transpositions and $0 \leq n - 1$.

Case 2: Suppose $\sigma \neq id$.

Any permutation of a nonempty finite set can be written as a finite product of disjoint cycles.

Since S_n is nonempty and finite, then σ can be written as a finite product of disjoint cycles.

Thus, there exist k disjoint cycles $c_1, c_2, ..., c_k$ such that $\sigma = c_1c_2 \cdots c_k$ and $k > 0$.

Let l_i be the length of the cycle c_i for each $i = 1, 2, ..., k$.

Since the sum of the cycle lengths of all the disjoint cycles cannot exceed n, then $0 \leq l_1 + l_2 + ... + l_k \leq n$.

Hence, $0 \leq \sum_{i=1}^{k} l_i \leq n$.

If d is a cycle of length m, then $d = (d_1, d_2, ..., d_m) = (d_1, d_m)(d_1, d_{m-1}), ...(d_1, d_2)$.

Hence d is a product of $m - 1$ transpositions.

Thus, any cycle of length m is a product of $m - 1$ transpositions.

The number of transpositions of σ is the sum of the number of transpositions of each disjoint cycle.

Let t be the number of transpositions of σ.

Then $t = (l_1 - 1) + (l_2 - 1) + ... + (l_k - 1) = (l_1 + l_2 + ... + l_k) - k * 1 = \sum_{i=1}^{k} l_i - k$.

The maximum value for t occurs when $\sum_{i=1}^{k} l_i$ is maximum and k is minimum.

Let T be the maximum of t.

Then T is the value when $\sum_{i=1}^{k} l_i = n$ and $k = 1$.

Thus, $T = n - 1$.

Hence, the maximum number of transpositions is $n - 1$. □

Exercise 56. If σ is a cycle of odd length, then σ^2 is a cycle.

Proof. Let σ be a k cycle of odd length.

Then k is odd and $\sigma = (a_1, a_2, ..., a_k)$.

Observe that $\sigma^2(a_1) = \sigma(\sigma(a_1)) = \sigma(a_2) = a_3$.

Observe that $\sigma^2(a_2) = \sigma(\sigma(a_2)) = \sigma(a_3) = a_4$.

Observe that $\sigma^2(a_3) = \sigma(\sigma(a_3)) = \sigma(a_4) = a_5$.

We continue this process.

Observe that $\sigma^2(a_{k-1}) = \sigma(\sigma(a_{k-1})) = \sigma(a_k) = a_1$.

Observe that $\sigma^2(a_k) = \sigma(\sigma(a_k)) = \sigma(a_1) = a_2$.

Observe that $a_1 \mapsto a_3 \mapsto a_5 \mapsto a_7 \mapsto ... \mapsto a_k \mapsto a_2 \mapsto a_4 \mapsto a_6 ... \mapsto a_{k-1} \mapsto a_1$.

Therefore, $\sigma^2 = (a_1, a_3, a_5, ..., a_k, a_2, a_4, a_6, ..., a_{k-1})$.

Hence, σ^2 is a cycle of length k. □

Exercise 57. If $H < S_n$, then either all members of H are even or exactly half of the members of H are even.

Solution. We compute some examples.

Let $n = 1$.

Then $S_1 = \{id\}$.

Since id is an even permutation, then all members of S_1 are even.

Therefore, all members of S_1 are even.

Since there is only 1 group of order 1 up to isomorphism, then in any group of order 1 all of its members are even.

The only subgroups of S_1 is S_1 itself since S_1 is the trivial group.

Let $n = 2$.

Then $S_2 = \{id, (12)\}$.

Since id is even and (12) is odd (b/c any transposition is odd), then exactly 1/2 of its members are even.

Therefore, exactly 1/2 of the members of S_2 are even.

Since there is only 1 group of order 2 up to isomorphism, then in any group of order 2 exactly $1/2$ of its members are even.

The only subgroups of S_2 are the trivial subgroup and S_2 itself.

Let $n = 3$.

Then $S_3 = \{id, (12), (13), (14), (123), (132)\}$.

Since $id, (123), (132)$ are all even and the transpositions $(12), (13), (14)$ are all odd, then exactly $1/2$ of its members are even.

Therefore, exactly $1/2$ of the members of S_3 are even.

What are all the subgroups of S_3?

They are: $\{id\}, \{(12), id\}$, $\{(13), id\}$, $\{(23), id\}$, $\{(123), (132), id\}, S_3$.

The trivial subgroup is a group of order 1, so all of its members are even.

S_3 has 3 groups of order 2.

We know that in any subgroup of order 2 exactly $1/2$ of its members are even.

S_3 has 1 group of order 3, namely S_3 itself.

In S_3 the even permutations are $id, (123), (132)$ and the odd permutations are $(12), (13), (23)$. Hence exactly $1/2$ of its members are even and $1/2$ are odd.

Therefore, in S_3 exactly $1/2$ of its members are even.

Since there is only 1 group of order 3 up to isomorphism, then in any group of order 3 exactly $1/2$ of its members are even.

Let $n = 4$.

Then S_4 consists of $4! = 24$ permutations.

One example of a permutation of S_4 that has order 4 is the cycle (1234).

Every element generates a cyclic subgroup, so the cycle (1234) generates a cyclic subgroup of S_4 of order 4.

This particular group of order 4 is $G_4 = \{id, (1234), (13)(24), (1432)\}$.

The even permutations are $id, (13)(24)$ and the odd permutations are $(1234), (1432)$.

Hence, the number of even permutations equals the number of odd permutations, so exactly $1/2$ of the members of G_4 are even.

Any group of order 4 that is cyclic is isomorphic to $(\mathbb{Z}_4, +)$, so $(G_4, \circ) \cong (\mathbb{Z}_4, +)$.

There is also a subgroup of S_4 that is not cyclic by Cayley's theorem.

Let $H < S_4$ be a noncyclic subgroup of order 4.

Then H is isomorphic to Klein 4 group.

An example is $H = \{id, (13)(24), (14)(23), (12)(34)\}$.

Note that $H < A_4$ since all elements of H are even permutations.

Hence a group of order 4 is either cyclic or not cyclic.

If a group of order 4 is cyclic, then it is isomorphic to $\mathbb{Z}_4$ and exactly $1/2$ of its members are even permutations.

If a group of order 4 is not cyclic, then it is isomorphic to Klein 4 group and all of its members are even permutations.

To prove this assertion, let $H < S_n$.

P : All members of H are even permutations.

Q : Exactly $1/2$ of the members of H are even permutations.

We must prove $P \vee Q$.

Since $\neg P \rightarrow Q \Leftrightarrow \neg(\neg P) \vee Q \Leftrightarrow P \vee Q$, we may prove $P \vee Q$ by proving its logically equivalent form $\neg P \rightarrow Q$.

Thus, we assume Not all members of H are even permutations.

We must prove exactly $1/2$ of the members of H are even. $\square$

Proof. Let n be a positive integer.

Let $H < S_n$.

Suppose not all members of H are even permutations.

Then there exists at least one member of H that is not even.

Hence, there exists at least one member of H that is odd.

Let σ be some odd permutation of H.

Then $\sigma \in H$ and σ is odd.

Let A be the set of all even permutations of H.

Let B be the set of all odd permutations of H.

Then $A = \{h \in H : h \text{ is even}\}$ and $B = \{h \in H : h \text{ is odd}\}$.

Let $P = \{A, B\}$.

We prove P is a partition of H.

Since H is a group, then there exists an identity in H.

Let id be the identity of H.

Since id is even, then $id \in A$.

Thus, $A \neq \emptyset$.

Since $\sigma \in H$ and σ is odd, then $\sigma \in B$.

Hence, $B \neq \emptyset$.

Since $A \subset H$ and $B \subset H$, then $A \cup B \subset H$.

Let $x \in H$.

Since $H \subset S_n$, then $x \in S_n$.

Thus, x is a permutation on n symbols.

By the parity theorem, any permutation is either even or odd, but not both.

Hence, x is either even or odd, but not both.

Thus, either x is even or x is odd and x is not both even and odd.

Hence, either $x \in A$ or $x \in B$ and $x \notin A \cap B$.

Therefore, $x \in A \cup B$ and $x \notin A \cap B$.

Thus, $x \in H$ implies $x \in A \cup B$, so $H \subset A \cup B$.

Since $A \cup B \subset H$ and $H \subset A \cup B$, then $H = A \cup B$.

Since x is arbitrary, then $x \notin A \cap B$ for all $x \in H$.

Hence, there does not exist $x \in H$ such that $x \in A \cap B$.

Therefore, $A \cap B = \emptyset$.

Therefore, P is a partition of H.

Observe that

$$\begin{aligned} |H| &= |A \cup B| \\ &= |A| + |B| - |A \cap B| \\ &= |A| + |B| - |\emptyset| \\ &= |A| + |B| - 0 \\ &= |A| + |B|. \end{aligned}$$

To prove exactly $1/2$ of the members of H are even, we prove $|A| = |B|$.
Hence, we must prove there exists a bijection from A to B.
Let $f : A \to B$ be a binary relation defined by $f(\alpha) = \alpha\sigma$.
Let $\alpha \in A$.
Then $\alpha \in H$ and α is even.

Let $\alpha\sigma$ be the composition of α and σ.
Since $\alpha \in H$ and $\sigma \in H$, then by closure of H under $\circ$, $\alpha\sigma \in H$.
Since $\circ$ is a binary operation of H, then the product $\alpha\sigma$ is unique.
Since α is even and σ is odd, then α and σ have opposite parity.
The composition of two permutations of opposite parity is odd.
Hence, $\alpha\sigma$ is odd.
Since $\alpha\sigma \in H$ and $\alpha\sigma$ is odd, then $\alpha\sigma \in B$.
Since $f(\alpha) = \alpha\sigma$, then $f(\alpha) \in B$ and $f(\alpha)$ is unique.
Thus, $\alpha \in A$ implies $f(\alpha) \in B$ and $f(\alpha)$ is unique.
Therefore, f is a function.

We prove f is injective.
Suppose there exist $\alpha_1, \alpha_2 \in A$ such that $f(\alpha_1) = f(\alpha_2)$.
Then $\alpha_1 \in H$ and $\alpha_2 \in H$ and $\alpha_1\sigma = \alpha_2\sigma$.
Thus, $\alpha_1, \alpha_2, \sigma \in H$.
Since H is a group, we apply the cancellation law for groups to obtain $\alpha_1 = \alpha_2$.
Hence, $f(\alpha_1) = f(\alpha_2)$ implies $\alpha_1 = \alpha_2$, so f is injective.

We prove f is surjective.
Let $\beta \in B$.
Then $\beta \in H$ and β is odd.
Let $\alpha = \beta\sigma^{-1}$.
Since H is a group and $\sigma \in H$, then $\sigma^{-1} \in H$.
By closure of H, $\beta\sigma^{-1} \in H$, so $\alpha \in H$.

The parity of σ^{-1} is the same as the parity of its inverse.
Hence, the parity of σ^{-1} is the same as the parity of $(\sigma^{-1})^{-1} = \sigma$.
Thus, the parity of σ^{-1} is the same as the parity of σ.
Since the parity of σ is odd, then this implies that σ^{-1} is odd.

Thus, β and σ^{-1} have the same parity.
The composition of two permutations of the same parity is even.
Hence, α is even.
Since $\alpha \in H$ and α is even, then $\alpha \in A$. Observe that

$$\begin{aligned} f(\alpha) &= f(\beta\sigma^{-1}) \\ &= (\beta\sigma^{-1})\sigma \\ &= \beta(\sigma^{-1}\sigma) \\ &= \beta(id) \\ &= \beta. \end{aligned}$$

Hence, there exists $\alpha \in A$ such that $f(\alpha) = \beta$.
Therefore, f is surjective.
Hence, f is bijective, so $|A| = |B|$.
Thus, $|H| = |A| + |B| = |A| + |A| = 2|A|$, so $|A| = \frac{|H|}{2}$.
Therefore, the number of even permutations in H is $\frac{|H|}{2}$.
Hence, exactly 1/2 of the members of H are even. □

Exercise 58. Let $\alpha \in S_n$ for $n \geq 3$.
If $\alpha\beta = \beta\alpha$ for all $\beta \in S_n$, then $\alpha = id$.

Solution. We must prove: $(\forall \beta \in S_n)(\alpha\beta = \beta\alpha) \to (\alpha = id)$.

To get a complete picture, we try S_2.

When we compute S_2, we find that both id and (12) each commute with all elements of S_2, so that α could be either id or (12).

When we try S_3, we compute and find that id commutes with all elements of S_3 and that all non-identity elements do not.

We find that each non identity element α has at least one β such that $\alpha\beta \neq \beta\alpha$.

In fact, we also observe that such a β is not the identity.

The same observation applies when we compute S_4.

Thus, to prove this statement we can consider whether α is identity or not.

This suggests proof by contrapositive because we can then assume α is not identity and hopefully deduce our result.

The contrapositive is:
$(\alpha \neq id) \to (\exists \beta \in S_n)(\alpha\beta \neq \beta\alpha)$.
Thus, we assume $\alpha \neq id$.
We must construct a suitable $\beta \in S_n$ such that $\alpha\beta \neq \beta\alpha$. □

Proof. Let $X = \{1, 2, 3, ..., n\}$.

Suppose $\alpha \neq id$.

Since $\alpha = id$ iff $\alpha(x) = x$ for all $x \in X$, then $\alpha \neq id$ iff there exists $x \in X$ such that $\alpha(x) \neq x$.

Thus, there exists $x \in X$ such that $\alpha(x) \neq x$.
Without loss of generality, we may let $x = 1$.
Then $\alpha(1) \neq 1$.

Let $a = \alpha(1)$.
Then $a \neq 1$.
Since α is a permutation, then α is a bijective function, so α is surjective.
Hence, there exists $b \in X$ such that $\alpha(b) = 1$.
Suppose $b = 1$.
Then $\alpha(1) = 1$.
Thus, $\alpha(1) = 1$ and $\alpha(1) \neq 1$, so $\alpha(1)$ is not unique.
Since α is a function, then $\alpha(x)$ is unique for all $x \in X$.
Hence, in particular, $\alpha(1)$ is unique.
Thus, we have $\alpha(1)$ is not unique and $\alpha(1)$ is unique, a contradiction.
Therefore, $b \neq 1$.
Let $\beta \in S_n$ such that $\beta(1) = b$ and $\beta(a) = a$.
Since $\beta(1) = b$ and $b \neq 1$, then $\beta(1) \neq 1$.
Hence, $\beta \neq id$.

Suppose $a = b$.
Then $\beta(a) = a = b = \beta(1)$, so $\beta(a) = \beta(1)$.
Since β is a permutation, then β is a bijective function, so β is injective.
Hence, $\beta(a) = \beta(1)$ implies $a = 1$, so $a = 1$.
Thus, we have $a = 1$ and $a \neq 1$, a contradiction.
Therefore, $a \neq b$.
Hence, $1, a, b$ are distinct elements of X.
Observe that

$$\begin{aligned} (\alpha\beta)(1) &= \alpha(\beta(1)) \\ &= \alpha(b) \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} (\beta\alpha)(1) &= \beta(\alpha(1)) \\ &= \beta(a) \\ &= a \\ &\neq 1. \end{aligned}$$

Hence, $(\alpha\beta)(1) \neq (\beta\alpha)(1)$, so $\alpha\beta \neq \beta\alpha$.
Therefore, if $\alpha \neq id$, then there exists a $\beta \in S_n$ such that $\alpha\beta \neq \beta\alpha$.
Thus, if $\alpha\beta = \beta\alpha$ for all $\beta \in S_n$, then $\alpha = id$. □

Exercise 59. How many transpositions exist in S_n?

Solution. Let $n \in \mathbb{Z}^+$.
Let S_n be the symmetric group on n letters.
Let $X = \{1, ..., n\}$ be a set of n letters.
Then S_n is the set of all permutations of X.

Let $\tau \in S_n$ be a transposition.
Then there exist $a, b \in X$ such that $\tau = (a, b)$.
Thus, τ is a particular combination of n letters taken 2 at a time.
Thus, the number of transpositions is

$$\begin{aligned}\binom{n}{2} &= \frac{n!}{(n-2)!2!} \\ &= \frac{n(n-1)(n-2)!}{2(n-2)!} \\ &= \frac{n(n-1)}{2}.\end{aligned}$$

□