CHAPTER 5

# Permutation Groups

DEFINITION (Permutation of $A$, Permutation Group of $A$). A permutation of a set $A$ is a function from $A$ to $A$ that is both 1–1 and onto.

A permutation group of a set $A$ is a set of permutations of $A$ that forms a group under function composition.

NOTE. We focus on the case where $A$ is finite. We usually take $A = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$.

NOTATION. We usually define a permutation explicitly rather than by rule: For $A = \{1, 2, 3, 4, 5\}$, define a permutation $\alpha$ by

$$\alpha(1) = 3, \quad \alpha(2) = 2, \quad \alpha(3) = 5, \quad \alpha(4) = 1, \quad \alpha(5) = 4,$$

or as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{bmatrix} \begin{matrix} \textit{domain} \\ \textit{range} \end{matrix}.$$

Suppose

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

Then

$$\beta\alpha = \begin{bmatrix} 1 & 2 & \overleftarrow{\boxed{3}} & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \underleftarrow{\boxed{3}} & 2 & 5 & 1 & 4 \end{bmatrix}$$

applies permutations from right to left, so

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

We notice that this multiplication (composition) is not commutative.

EXAMPLE. Symmetric Group $S_3$ — all permutations on $\{1, 2, 3\}$.

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

$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} (\text{note } \alpha^3 = \beta^2 = \varepsilon), \quad \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \quad \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

This is the entire group since there are $3! = 3 \cdot 2 \cdot 1 = 6$ ways to define a 1–1 and onto function on $\{1, 2, 3\}$, three possibilities for 1, two for 2, and one for 3. Note

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

so $S_3$ is not commutative. Also, using $\beta\alpha = \alpha^2\beta$ (called a relation),

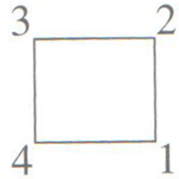
$$\beta\alpha^2 = (\beta\alpha)\alpha = (\alpha^2\beta)\alpha = \alpha^2(\beta\alpha) = \alpha^2(\alpha^2\beta) = \alpha^4\beta = \alpha\beta.$$

EXAMPLE. Symmetric Group $S_n$ — all permutations on $A = \{1, 2, \ldots, n\}$, also known as the symmtric group of degree $n$.

For $\alpha \in S_n$, $\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}$ and $|S_n| = n!$.

For $n \geq 3$, $S_n$ is non-Abelian.

EXAMPLE. Symmetries of a Square. Consider the square with number vertices:




Then, in $D_4$, $R_{90} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = \rho$ and $H = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = \phi$ generate $D_4$.

$$\rho^2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = R_{180}, \quad \rho^3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = R_{270},$$

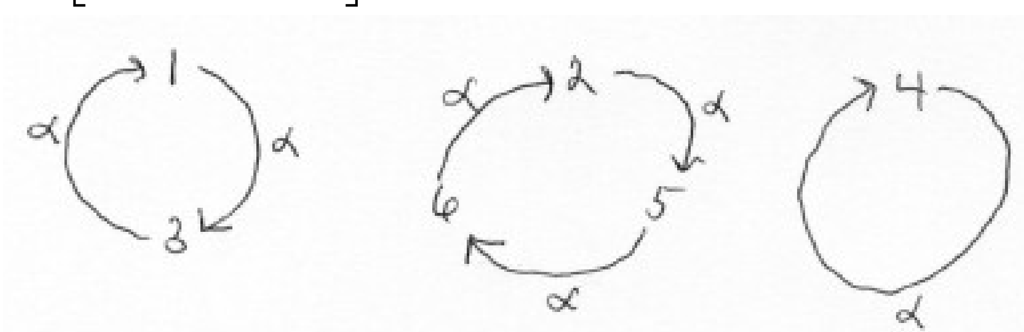
$$\rho^4 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = R_0, \quad \rho\phi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} = D',$$

$$\rho^2\phi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} = V, \quad \rho^3\phi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix} = D.$$

Thus $D_4 \leq S_4$.

Cycle Notation

Consider $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 4 & 6 & 2 \end{bmatrix}$. View schematically as follows.



Or write as $\alpha = (1\ 3)(2\ 5\ 6)(4)$ — these can be written in any order.

$(a_1\, a_2\ \cdots\ a_n)$ is a cycle of length $n$ or an $n$-cycle (use commas between integers if $n \geq 10$).

One can consider a cycle as fixing any element not apperaring in it. Thus, in $S_6$, $\beta = (1\ 3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{bmatrix}$ and $\gamma = (2\ 5\ 6) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 6 & 2 \end{bmatrix}$ can be multiplied to give

$$\alpha = \beta\gamma = \gamma\beta = (1\ 3)(2\ 5\ 6) = (2\ 5\ 6)(1\ 3).$$

Note the 4, which is fixed, no longer appears, and the multiplication is commutative since the cycles are disjoint.

Example. In $S_8$, let $\alpha = (1\ 3\ 8\ 2)(4\ 7)(5\ 6)$ and $\beta = (2\ 8\ 3)(4\ 7\ 6)$. Then

$\alpha\beta = (1\ 3\ 8\ 2)(4\ 7)(5\ 6)(2\ 8\ 3)(4\ 7\ 6) = (1\ 3)(5\ 6\ 7)$ and

$\beta\alpha = (2\ 8\ 3)(4\ 7\ 6)(1\ 3\ 8\ 2)(4\ 7)(5\ 6) = (1\ 2)(4\ 5\ 6)$. Note $\alpha\beta \neq \beta\alpha$.

Example. In $S_8$, let $\alpha = (1\ 4)(2\ 6\ 3)(5\ 8\ 7)$ and $\beta = (1\ 8)(2\ 6)(3\ 5)(4\ 7)$. Then $\alpha\beta = (1\ 7)(2\ 3\ 8\ 4\ 5)$ and $\beta\alpha = (1\ 7\ 3\ 6\ 5)(4\ 8)$.

Theorem (5.1 — Products of Disjoint Cycles). *Every permutation of a finite set can be written as a cycle or a product of disjoint cycles.*

Proof. Let $\alpha$ be a permutation on A={1,2,...,n}. Choose any $a_1 \in A$. Let $a_2 = \alpha(a_1)$, $a_3 = \alpha(\alpha(a_1)) = \alpha^2(a_1)$, etc., until $a_1 = \alpha^m(a_1)$ for some $m$. This repetition of $a_1$ is guaranteed with $m \leq n$ since $A$ is finite. Thus $(a_1\ a_2\ \cdots\ a_m)$ is a cycle of $\alpha$.

If $m < n$, choose any element $b_1 \in A$ where $b_1$ is not in the first cycle, and let $b_2 = \alpha(b_1)$, $b_3 = \alpha(\alpha(b_1)) = \alpha^2(b_1)$, until $b_1 = \alpha^k(b_1)$ for some $k \leq n$. We now have a second cycle $(b_1\ b_2\ \cdots\ b_k)$ of $\alpha$.

If $\alpha^i(a_1) = \alpha^j(b_1)$ for some $i$ and $j$, then $\alpha^{i-j}(a_1) = b_1 \Longrightarrow b_1 \in (a_1\ a_2\ \cdots\ a_m)$, contradicting how $b_1$ was chosen.

If $m + k < n$, we continue as above until there are no elements left. Thus

$$\alpha = (a_1\ a_2\ \cdots\ a_m)(b_1\ b_2\ \cdots\ b_k)\cdots(c_1\ c_2\ \cdots\ c_s).$$

□

Theorem (5.2 — Disjoint Cycles Commute).

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

Proof.

Suppose $\alpha$ and $\beta$ are permutations of

$$S = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_k\}$$

where the $c$'s are left fixed by both $\alpha$ and $\beta$.

[To show $\alpha\beta(x) = \beta\alpha(x) \forall x \in S$.]

If $x = a_i$ for some $i$, since $\beta$ fixes all $a$ elements,

$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$ (with $a_{m+1} = a_1$) and

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

so $\alpha\beta = \beta\alpha$ on the $a$ elements.

A similar argument shows $\alpha\beta = \beta\alpha$ on the $b$ elements.

Since $\alpha$ and $\beta$ both fix the $c$ elements,

$(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i$ and

$(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i$.

Thus $\alpha\beta(x) = \beta\alpha(x) \forall x \in S$. □

Question: Is there an easy way to compute the order of a permutation?

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.*

PROOF.

Suppose $\alpha$ is a permutation of a finite set $S$, $\alpha = \alpha_1\alpha_2\cdots\alpha_r$ where

$\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ are disjoint cycles of $S$. Since disjoint cycles commute,

$\alpha^m = \alpha_1^m\alpha_2^m\cdots\alpha_r^m$ for all $m \in \mathbb{Z}$. Now $\alpha^m = (1)$ (the identity) $\iff$

$\alpha_i^m = (1)\ \forall\ i = 1, \ldots, r$. For if $\alpha_i(x) \neq x$, $\alpha_j(x) = x\ \forall\ j \neq i$ (our cycles are disjoint), so $\alpha_i^m(x) = x$.

Since an $n$-cycle clearly has order $n$, by Corollary 2 of Theorem 4., $|\alpha_i|\big||\alpha|$ for $i = 1 \ldots r$. Therefore, $\mathrm{lcm}(|a_1|, \ldots, |a_r|)\big||\alpha|$. But $m = \mathrm{lcm}(|a_1|, \ldots, |a_r|)$ is the least $m$ such that $\alpha_i = (1)$ for $i = 1, \ldots, r$, so $|\alpha| = \mathrm{lcm}(|a_1|, \ldots, |a_r|)$. □

THEOREM (5.4 — Product of 2-Cycles). *Every permutation in $S_n$, $n > 1$, is a product of 2-cycles (also called transpositions).*

PROOF.

$(1) = (1\ 2)(2\ 1)$, so $(1)$ is a product of 2-cycles.

By Theorem 5.1, for $\alpha \in S_n$,

$$\alpha = (a_1\ a_2\ \cdots\ a_k)(b_1\ b_2\ \cdots\ b_t)\cdots(c_1\ c_2\ \cdots\ c_s).$$

Then

$$\alpha = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_2)(b_1\ b_t)(b_1\ b_{t-1})\cdots(b_1\ b_2)\cdots (c_1\ c_s)(c_1\ c_{s-1})\cdots(c_1\ c_2).$$

□

EXAMPLE.

$$(3\ 6\ 8\ 2\ 4) = (3\ 4)(3\ 2)(3\ 8)(3\ 6)$$
$$(1\ 3\ 7\ 2)(4\ 8\ 6) = (1\ 2)(1\ 7)(1\ 3)(4\ 6)(4\ 8)$$

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

PROOF.

$r \neq 1$, since $\varepsilon$ is not a 2-cycle. If $r = 2$, we are done. Suppose $r > 2$ and that if $\varepsilon = \beta_1\beta_2 \cdots \beta_s$ with $s < r$, then $s$ is even.

Suppose the rightmost 2-cycle is $(a\ b)$. Since $(i\ j) = (j\ i)$, the product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms shown on the right (these are 4 possibilities for $\beta_{r-1}$ if $\beta_r = (a\ b)$):

$$\varepsilon = (a\ b)(a\ b)$$
$$(a\ b)(b\ c) = (a\ c)(a\ b)$$
$$(a\ c)(c\ b) = (b\ c)(a\ b)$$
$$(a\ b)(c\ d) = (c\ d)(a\ b)$$

In the first case, we may delete $\beta_{r-1}\beta_r$ from the original product, leaving $\varepsilon = \beta_1 \cdots \beta_{r-2}$, so $r - 2$ is even by the second principle of math induction.

In the other 3 cases, We replace $\beta_{r-1}\beta_r$ by the products on the left, retaining the identity but moving the rightmost occurance of $a$ into $\beta_{r-1}$.

Repeat the above procedure with $\beta_{r-2}\beta_{r-1}$. We either obtain $\varepsilon = \beta_1 \cdots \beta_{r-2}\beta_r$, implying $r$ is even by the second principle of math induction, or obtain a new product of $r$ 2-cycles for $\varepsilon$ with the rightmost $a$ in $\beta_{r-2}$.

Continuing, if the rightmost occurrence of $a$ is in $\beta_2$, $\beta_1\beta_2 = \varepsilon$, for if $a$ was moved to $\beta_1$ as above, that would be its only occurrence, and so would not be fixed, a contradiction. Then $\varepsilon = \beta_3 \cdots \beta_r$ also, and again $r$ must be even by the second principle of math induction. $\square$

THEOREM (5.5 — Always Even or Always Odd).

*If $\alpha \in S_n$ and $\alpha = \beta_1\beta_2\cdots\beta_r = \gamma_1\gamma_2\cdots\gamma_s$ where the $\beta$'s and $\gamma$'s are 2-cycles, then $r$ and $s$ are both even or both odd.*

PROOF.

$\beta_1\beta_2\cdots\beta_r = \gamma_1\gamma_2\cdots\gamma_s \Longrightarrow \varepsilon = \gamma_1\gamma_2\cdots\gamma_s\beta_r^{-1}\cdots\beta_2^{-1}\beta_1^{-1} \Longrightarrow$

$\varepsilon = \gamma_1\gamma_2\cdots\gamma_s\beta_r\cdots\beta_2\beta_1$ since a 2-cycle is its own inverse. Then, from the lemma, $r + s$ is even $\Longrightarrow r$ and $s$ are both even or $r$ and $s$ are both odd. □

DEFINITION (Even and Odd Permutations). A permutation that can be expressed as an even number of 2-cycles is called an even permutation, and a permutation that can be expressed as an odd number of 2-cycles is called an odd permutation.

THEOREM (5.6 — Even Permutaions Form a Group). *The set of even permutations in $S_n$ forms a subgroup of $S_n$.*

PROOF.

If $\alpha, \beta \in S_n$ and are both even, then $\alpha\beta$ is also even since it is an even number of 2-cycles followed by an even number of 2-cycles. Since multiplication is closed for even permutations, we have a subgroup by Theorem 3.3 (Finite Subgroup Test). □

The above proof is Page 119 # 17.

DEFINITION (Alternating Group of Degree $n$). The group of even permutations of $n$ symbols is denoted by $A_n$ and is called the alternating group of degree $n$.

THEOREM (5.7). *For $n > 1$, $A_n$ has order $\dfrac{n!}{2}$.*

PROOF.

For each odd permutation $\alpha$, the permutation $(1\,2)\alpha$ is even and $(1\,2)\alpha \neq (1\,2)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many even permutations as odd ones.

Also, for each even permutation $\alpha$, $(1\ 2)\alpha$ is odd and $(1\ 2)\alpha \neq (1\ 2)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many odd permutations as even ones.

Therefore, there is an equal number of odd and even permutations in $S_n$. Since $|S_n| = n!$, $|A_n| = \dfrac{n!}{2}$. □

EXAMPLE (Page 111 # 8— Rotations of a Tetrahedron). The 12 rotations of a regular tetrahedron can be described with the elements of $A_4$. Table 5.1 from page 111 of the text is given below:

**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 $\alpha_k$. For example, $\alpha_3\,\alpha_8 = \alpha_6$.)

| | $\alpha_1$ | $\alpha_2$ | $\alpha_3$ | $\alpha_4$ | $\alpha_5$ | $\alpha_6$ | $\alpha_7$ | $\alpha_8$ | $\alpha_9$ | $\alpha_{10}$ | $\alpha_{11}$ | $\alpha_{12}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $(1) = \alpha_1$ | 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 |

Read the info in the text and view the graphs in Figure 5.1 on page 112.

PROBLEM (Page 119 # 15). Let $n$ be a positive integer. If $n$ is odd, is an $n$-cycle an odd or even permutation? If $n$ is even, is an $n$-cycle an odd or even permutation?

SOLUTION.

$(a_1\ a_2\ \cdots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1})\cdots(a_1\ a_2)$, so $(a_1\ a_2\ \cdots\ a_n)$ can be written as a product of $n-1$ 2-cycles.

Thus, $n$ odd $\Longrightarrow$ the $n$-cycle is even, and

$n$ even $\Longrightarrow$ the $n$-cycle is odd. □

PROBLEM (Page 119 # 9). What are the possible orders for the elements of $S_6$ and $A_6$? What about $A_7$?

SOLUTION.

We find the orders by looking at the possible products of disjoint cycle structures arranged by longest lengths left to right and denote an $n$-cycle by $(\underline{n})$.

$(\underline{6})$ has order 6 and is odd;

$(\underline{5})(\underline{1})$ has order 5 and is even;

$(\underline{4})(\underline{2})$ has order 4 and is even;

$(\underline{4})(\underline{1})(\underline{1})$ has order 4 and is odd;

$(\underline{3})(\underline{3})$ has order 3 and is even;

$(\underline{3})(\underline{2})(\underline{1})$ has order 6 and is odd;

$(\underline{3})(\underline{1})(\underline{1})(\underline{1})$ has order 3 and is even;

$(\underline{2})(\underline{2})(\underline{2})$ has order 2 and is odd;

$(\underline{2})(\underline{2})(\underline{1})(\underline{1})$ has order 2 and is even;

$(\underline{2})(\underline{1})(\underline{1})(\underline{1})(\underline{1})$ has order 2 and is odd.

So, for $S_6$, the possible orders are 1, 2, 3, 4, 5, 6; for $A_6$, the possible orders are 1, 2, 3, 4, 5.

We see from example 4 of the text (page 106) that orders of the elements of $S_7$ are 1, 2, 3, 4, 5, 6, 7, 10, and 12.

The 3-cycle with the 4-cycle and the 2-cycle with the 5-cycles are odd. Elements of $A_7$ of orders 1–5 can be created as in $S_6$. A 3-cycle with a pair of 2-cycles has order 6, and a 7-cycle has order 7. So $A_7$ has possible orders 1–7. □

**Problem** (Page 120 # 29). How many elements of order 4 does $S_6$ have? How many elements of order 2 does $S_6$ have?

**Solution.**

The possibilities for order 4 are a single 4-cycle or a 4-cycle with a two-cycle. To create a 4-cycle, there are 6 choices for the first element, 5 choices for the second, 4 for the third, and 3 for the fourth, so $6 \cdot 5 \cdot 4 \cdot 3 = 360$ choices. But since each element could be listed first, there are $\dfrac{360}{4} = 90$ possible 4-cycles. That leaves only one choice for a disjoint 2-cycle, so there are $90 \cdot 2 = 180$ elements of order 4.

Elements of order 2 could consist of 1, 2, or 3 2-cycles. Using the same reasoning as above, there are $6 \cdot 5/2 = 15$ ways to create a 2-cycle. Then there are $4 \cdot 3/2 = 6$ ways to create a second 2-cycle. Only a single way remains to create a third 2-cycle.

So there are 15 single 2-cycles, there are $15 \cdot 6/2 = 45$ pairs of disjoint 2-cycles ( divide by 2 since either 2-cycle could be listed first), and $15 \cdot 6/6 = 15$ triples of disjoint 2-cycles ($3! = 6$ ways of ordering 3 items).

Thus there are $15 + 45 + 15 = 75$ elements of order 2. □

PROBLEM (Page 122 # 66). Show that for $n \geq 3$, $Z(S_n) = \{\varepsilon\}$.

SOLUTION. Suppose $\alpha \in Z(S_n)$, $\alpha \neq \varepsilon$. Consider $\alpha$ as written in cycle form.

(1) If $\alpha$ contains an $n$-cycle $(a_1\ a_2\ \cdots\ a_n)$, $n \geq 3$:

$(a_1\ a_2)(a_1\ a_2\ \cdots\ a_n) = (a_2\ a_3\ \cdots\ a_{n-1}\ a_n)$ and

$(a_1\ a_2\ \cdots\ a_n)(a_1\ a_2) = (a_1\ a_3\ a_4\ \cdots\ a_n)$, a contradiction.

(2) If $\alpha$ contains at least two 2-cycles, say $\alpha = (a_1\ a_2)(b_1\ b_2)\cdots$:

$(a_1\ b_1)\alpha = (a_1\ b_1)(a_1\ a_2)(b_1\ b_2)\cdots = (a_1\ a_2\ b_1\ b_2)\cdots$ and

$\alpha(a_1\ b_1) = (a_1\ a_2)(b_1\ b_2)(a_1\ b_1)\cdots = (a_1\ b_2\ b_1\ a_2)$, a contradiction.

(3) $\alpha = (a_1\ a_2)$:

$(a_1\ a_3)(a_1\ a_2) = (a_1\ a_2\ a_3)$, and

$(a_1\ a_2)(a_1\ a_3) = (a_1\ a_3\ a_2)$, a contradiction.

Since this includes all possibilities, $Z(S_n) = \{\varepsilon\}$. □

MAPLE. See permutation.mw or permutation.pdf.