Wigner’s discovery about the electron permutation group was just the beginning. He and others found many similar applications and nowadays group theoretical methods—especially those involving characters and representations—pervade all branches of quantum mechanics.

*George Mackey, Proceedings of the American Philosophical Society*

**Definition and Notation**

In this chapter, we study certain groups of functions, called permutation groups, from a set $A$ to itself. In the early and mid-19th century, groups of permutations were the only groups investigated by mathematicians. It was not until around 1850 that the notion of an abstract group was introduced by Cayley, and it took another quarter century before the idea firmly took hold.

**Definitions**

**Permutation of $A$, Permutation Group of $A$**

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

Although groups of permutations of any nonempty set $A$ of objects exist, we will focus on the case where $A$ is finite. Furthermore, it is customary, as well as convenient, to take $A$ to be a set of the form \( \{1, 2, 3, \ldots, n\} \) for some positive integer $n$. Unlike in calculus, where most functions are defined on infinite sets and are given by formulas, in algebra, permutations of finite sets are usually given by an explicit listing of each element of the domain and its corresponding functional value. For example, we define a permutation $\alpha$ of the set $\{1, 2, 3, 4\}$ by specifying

\[
\alpha(1) = 2, \quad \alpha(2) = 3, \quad \alpha(3) = 1, \quad \alpha(4) = 4.
\]
A more convenient way to express this correspondence is to write $\alpha$ in array form as

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

Here $\alpha(j)$ is placed directly below $j$ for each $j$. Similarly, the permutation $\beta$ of the set $\{1, 2, 3, 4, 5, 6\}$ given by

$$\beta(1) = 5, \quad \beta(2) = 3, \quad \beta(3) = 1, \quad \beta(4) = 6, \quad \beta(5) = 2, \quad \beta(6) = 4$$

is expressed in array form as

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

Composition of permutations expressed in array notation is carried out from right to left by going from top to bottom, then again from top to bottom. For example, let

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

and

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

then

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

On the right we have 4 under 1, since $(\gamma\sigma)(1) = \gamma(\sigma(1)) = \gamma(2) = 4$, so $\gamma\sigma$ sends 1 to 4. The remainder of the bottom row $\gamma\sigma$ is obtained in a similar fashion.

We are now ready to give some examples of permutation groups.

**EXAMPLE 1 Symmetric Group $S_3$** Let $S_3$ denote the set of all one-to-one functions from $\{1, 2, 3\}$ to itself. Then $S_3$, under function composition, is a group with six elements. The six elements are

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

Note that \( \beta \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \alpha^2 \beta \neq \alpha \beta \), so that \( S_3 \) is non-Abelian.

The relation \( \beta \alpha = \alpha^2 \beta \) can be used to compute other products in \( S_3 \) without resorting to the arrays. For example, \( \beta \alpha^2 = (\beta \alpha) \alpha = (\alpha^2 \beta) \alpha = \alpha^2 (\beta \alpha) = \alpha^2 (\alpha^2 \beta) = \alpha^4 \beta = \alpha \beta. \)

Example 1 can be generalized as follows.

**EXAMPLE 2 Symmetric Group \( S_n \)** Let \( A = \{1, 2, \ldots, n\} \). The set of all permutations of \( A \) is called the symmetric group of degree \( n \) and is denoted by \( S_n \). Elements of \( S_n \) have the form

\[ \alpha = \begin{bmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{bmatrix}. \]

It is easy to compute the order of \( S_n \). There are \( n \) choices of \( \alpha(1) \). Once \( \alpha(1) \) has been determined, there are \( n - 1 \) possibilities for \( \alpha(2) \) [since \( \alpha \) is one-to-one, we must have \( \alpha(1) \neq \alpha(2) \)]. After choosing \( \alpha(2) \), there are exactly \( n - 2 \) possibilities for \( \alpha(3) \). Continuing along in this fashion, we see that \( S_n \) has \( n(n-1) \cdots 3 \cdot 2 \cdot 1 = n! \) elements. We leave it to the reader to prove that \( S_n \) is non-Abelian when \( n \geq 3 \) (Exercise 45).

The symmetric groups are rich in subgroups. The group \( S_4 \) has 30 subgroups, and \( S_5 \) has well over 100 subgroups.

**EXAMPLE 3 Symmetries of a Square** As a third example, we associate each motion in \( D_4 \) with the permutation of the locations of each of the four corners of a square. For example, if we label the four corner positions as in the figure below and keep these labels fixed for reference, we may describe a 90° counterclockwise rotation by the permutation

\[ \rho = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}. \]
whereas a reflection across a horizontal axis yields
\[ \phi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}. \]
These two elements generate the entire group (that is, every element is some combination of the \( \rho \)'s and \( \phi \)'s).

When \( D_4 \) is represented in this way, we see that it is a subgroup of \( S_4 \).

**Cycle Notation**

There is another notation commonly used to specify permutations. It is called *cycle notation* and was first introduced by the great French mathematician Cauchy in 1815. Cycle notation has theoretical advantages in that certain important properties of the permutation can be readily determined when cycle notation is used.

As an illustration of cycle notation, let us consider the permutation
\[ \alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}. \]
This assignment of values could be presented schematically as follows.

Although mathematically satisfactory, such diagrams are cumbersome. Instead, we leave out the arrows and simply write \( \alpha = (1, 2) \)
\( (3, 4, 6)(5) \). As a second example, consider
\[ \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}. \]
In cycle notation, \( \beta \) can be written \( (2, 3, 1, 5)(6, 4) \) or \( (4, 6)(3, 1, 5, 2) \), since both of these unambiguously specify the function \( \beta \). An expression of the form \( (a_1, a_2, \ldots, a_m) \) is called a *cycle of length m* or an *m-cycle*. 
A multiplication of cycles can be introduced by thinking of a cycle as a permutation that fixes any symbol not appearing in the cycle. Thus, the cycle (4, 6) can be thought of as representing the permutation $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{bmatrix}$. In this way, we can multiply cycles by thinking of them as permutations given in array form. Consider the following example from $S_8$. Let $\alpha = (13)(27)(456)(8)$ and $\beta = (1237)(648)(5)$. (When the domain consists of single-digit integers, it is common practice to omit the commas between the digits.) What is the cycle form of $\alpha \beta$? Of course, one could say that $\alpha \beta = (13)(27)(456)(8)(1237)(648)(5)$, but it is usually more desirable to express a permutation in a disjoint cycle form (that is, the various cycles have no number in common). Well, keeping in mind that function composition is done from right to left and that each cycle that does not contain a symbol fixes the symbol, we observe that (5) fixes 1; (648) fixes 1; (1237) sends 1 to 2; (8) fixes 2; (456) fixes 2; (27) sends 2 to 7; and (13) fixes 7. So the net effect of $\alpha \beta$ is to send 1 to 7. Thus, we begin $\alpha \beta = (17 \cdots) \cdots$. Now, repeating the entire process beginning with 7, we have, cycle by cycle, right to left,

$7 \to 7 \to 7 \to 1 \to 1 \to 1 \to 1 \to 3$,

so that $\alpha \beta = (173 \cdots) \cdots$. Ultimately, we have $\alpha \beta = (1732)(48)(56)$. The important thing to bear in mind when multiplying cycles is to “keep moving” from one cycle to the next from right to left. (Warning: Some authors compose cycles from left to right. When reading another text, be sure to determine which convention is being used.)

To be sure you understand how to switch from one notation to the other and how to multiply permutations, we will do one more example of each.

If array notations for $\alpha$ and $\beta$, respectively, are $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$, then, in cycle notation, $\alpha = (12)(3)(45)$, $\beta = (153)(24)$, and $\alpha \beta = (12)(3)(45)(153)(24)$.

To put $\alpha \beta$ in disjoint cycle form, observe that (24) fixes 1; (153) sends 1 to 5; (45) sends 5 to 4; and (3) and (12) both fix 4. So, $\alpha \beta$ sends 1 to 4. Continuing in this way we obtain $\alpha \beta = (14)(253)$. One can convert $\alpha \beta$ back to array form without converting each cycle of $\alpha \beta$ into array form by simply observing that (14) means 1 goes to 4 and 4 goes to 1; (253) means 2 $\to$ 5, 5 $\to$ 3, 3 $\to$ 2.
One final remark about cycle notation: Mathematicians prefer not to write cycles that have only one entry. In this case, it is understood that any missing element is mapped to itself. With this convention, the permutation \( \alpha \) above can be written as \((12)(45)\). Similarly, 

\[
\alpha = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 \\
3 & 2 & 4 & 1 & 5 
\end{bmatrix}
\]

can be written \( \alpha = (134) \). Of course, the identity permutation consists only of cycles with one entry, so we cannot omit all of these! In this case, one usually writes just one cycle. For example, 

\[
\epsilon = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 
\end{bmatrix}
\]

can be written as \( \epsilon = (5) \) or \( \epsilon = (1) \). Just remember that missing elements are mapped to themselves.

## Properties of Permutations

We are now ready to state several theorems about permutations and cycles. The proof of the first theorem is implicit in our discussion of writing permutations in cycle form.

### 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** Let \( \alpha \) be a permutation on \( A = \{1, 2, \ldots, n\} \). To write \( \alpha \) in disjoint cycle form, we start by choosing any member of \( A \), say \( a_1 \), and let 

\[
a_2 = \alpha(a_1), \quad a_3 = \alpha(\alpha(a_1)) = \alpha^2(a_1),
\]

and so on, until we arrive at \( a_i = \alpha^m(a_1) \) for some \( m \). We know that such an \( m \) exists because the sequence \( a_1, \alpha(a_1), \alpha^2(a_1), \ldots \) must be finite; so there must eventually be a repetition, say \( \alpha^i(a_1) = \alpha^j(a_1) \) for some \( i \) and \( j \) with \( i < j \). Then \( a_1 = \alpha^m(a_1) \), where \( m = j - i \). We express this relationship among \( a_1, a_2, \ldots, a_m \) as

\[
\alpha = (a_1, a_2, \ldots, a_m) \cdot \cdot \cdot
\]

The three dots at the end indicate the possibility that we may not have exhausted the set \( A \) in this process. In such a case, we merely choose any element \( b_1 \) of \( A \) not appearing in the first cycle and proceed to
create a new cycle as before. That is, we let $b_2 = \alpha(b_1)$, $b_3 = \alpha^2(b_1)$, and so on, until we reach $b_1 = \alpha^k(b_1)$ for some $k$. This new cycle will have no elements in common with the previously constructed cycle. For, if so, then $\alpha'(a_i) = \alpha'(b_1)$ for some $i$ and $j$. But then $\alpha^{i-j}(a_i) = b_1$, and therefore $b_1 = a_t$ for some $t$. This contradicts the way $b_1$ was chosen. Continuing this process until we run out of elements of $A$, our permutation will appear as

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

In this way, we see that every permutation can be written as a product of disjoint cycles.

**Theorem 5.2** Disjoint Cycles Commute

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

**Proof** For definiteness, let us say that $\alpha$ and $\beta$ are permutations of the set

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

where the $c$’s are the members of $S$ left fixed by both $\alpha$ and $\beta$ (there may not be any $c$’s). To prove that $\alpha \beta = \beta \alpha$, we must show that $(\alpha \beta)(x) = (\beta \alpha)(x)$ for all $x$ in $S$. If $x$ is one of the $a$ elements, say $a_i$, then

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

since $\beta$ fixes all $a$ elements. (We interpret $a_{i+1}$ as $a_1$ if $i = m$.) For the same reason,

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

Hence, the functions of $\alpha \beta$ and $\beta \alpha$ agree on the $a$ elements. A similar argument shows that $\alpha \beta$ and $\beta \alpha$ agree on the $b$ elements as well. Finally, suppose that $x$ is a $c$ element, say $c_i$. Then, since both $\alpha$ and $\beta$ fix $c$ elements, we have

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

and

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

This completes the proof.
In demonstrating how to multiply cycles, we showed that the product \((13)(27)(456)(8)(1237)(648)(5)\) can be written in disjoint cycle form as \((1732)(48)(56)\). Is economy in expression the only advantage to writing a permutation in disjoint cycle form? No. The next theorem shows that the disjoint cycle form has the enormous advantage of allowing us to “eyeball” the order of the permutation.

**Theorem 5.3** Order of a Permutation (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.

**Proof** First, observe that a cycle of length \(n\) has order \(n\). (Verify this yourself.) Next, suppose that \(\alpha\) and \(\beta\) are disjoint cycles of lengths \(m\) and \(n\), and let \(k\) be the least common multiple of \(m\) and \(n\). It follows from Theorem 4.1 that both \(\alpha^k\) and \(\beta^k\) are the identity permutation \(e\) and, since \(\alpha\) and \(\beta\) commute, \((\alpha\beta)^k = \alpha^k\beta^k\) is also the identity. Thus, we know by Corollary 2 to Theorem 4.1 \((\alpha^k = e\) implies that \(|\alpha|\) divides \(k\)) that the order of \(\alpha\beta\)—let us call it \(t\)—must divide \(k\). But then \((\alpha\beta)^t = \alpha^t\beta^t = e\), so that \(\alpha^t = \beta^{-t}\). However, it is clear that if \(\alpha\) and \(\beta\) have no common symbol, the same is true for \(\alpha^t\) and \(\beta^{-t}\), since raising a cycle to a power does not introduce new symbols. But, if \(\alpha^t\) and \(\beta^{-t}\) are equal and have no common symbol, they must both be the identity, because every symbol in \(\alpha^t\) is fixed by \(\beta^{-t}\) and vice versa (remember that a symbol not appearing in a permutation is fixed by the permutation). It follows, then, that both \(m\) and \(n\) must divide \(t\). This means that \(k\), the least common multiple of \(m\) and \(n\), divides \(t\) also. This shows that \(k = t\).

Thus far, we have proved that the theorem is true in the cases where the permutation is a single cycle or a product of two disjoint cycles. The general case involving more than two cycles can be handled in an analogous way.

Theorem 5.3 is an enormously powerful tool for calculating the orders of permutations and the number of permutations of a particular order. We demonstrate this in the next two examples.

**Example 4** To determine the orders of the \(7! = 5040\) elements of \(S_7\), we need only consider the possible disjoint cycle structures of the elements of \(S_7\). For convenience, we denote an \(n\)-cycle by \((\eta)\). Then, arranging all possible disjoint cycle structures of elements of \(S_7\) according to longest cycle lengths left to right, we have
Now, from Theorem 5.3 we see that the orders of the elements of $S_7$ are 7, 6, 10, 5, 12, 4, 3, 2, and 1. To do the same for the 10! = 3628800 elements of $S_{10}$ would be nearly as simple.

**EXAMPLE 5** We determine the number of elements of $S_7$ of order 3. By Theorem 5.3, we need only count the number of permutations of the forms $(a_1a_2a_3)$ and $(a_4a_5a_6)$ $(a_1a_2a_3)$. In the first case consider the triple $a_1a_2a_3$. Clearly there are $7 \cdot 6 \cdot 5$ such triples. But this product counts the permutation $(a_1a_2a_3)$ three times (for example, it counts 134, 341, 413 as distinct triples whereas the cycles (134), (341), and (413) are the same group element). Thus, the number of permutations in $S_7$ for the form $(a_1a_2a_3)$ is $(7 \cdot 6 \cdot 5)/3 = 70$. For elements of $S_7$ of the form $(a_1a_2a_3) (a_4a_5a_6)$ there are $(7 \cdot 6 \cdot 5)/3$ ways to create the first cycle and $(4 \cdot 3 \cdot 2)/3$ to create the second cycle but the product of $(7 \cdot 6 \cdot 5)/3$ and $(4 \cdot 3 \cdot 2)/3$ counts $(a_1a_2a_3) (a_4a_5a_6)$ and $(a_4a_5a_6)(a_1a_2a_3)$ as distinct when they are equal group elements. Thus, the number of elements in $S_7$ for the form $(a_1a_2a_3) (a_4a_5a_6)$ is $(7 \cdot 6 \cdot 5)(4 \cdot 3 \cdot 2)/(3 \cdot 3 \cdot 2) = 280$. This gives us 350 elements of order 3 in $S_7$.

As we will soon see, it is often greatly advantageous to write a permutation as a product of cycles of length 2—that is, as permutations of the form $(ab)$ where $a \neq b$. Many authors call these permutations transpositions, since the effect of $(ab)$ is to interchange or transpose $a$ and $b$.

Example 6 and Theorem 5.4 show how this can always be done.
Theorem 5.4 Product of 2-Cycles

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

**Proof** First, note that the identity can be expressed as $(12)(12)$, and so it is a product of 2-cycles. By Theorem 5.1, we know that every permutation can be written in the form

$$\left( a_1a_2\cdots a_k \right) \left( b_1b_2\cdots b_l \right) \left( c_1c_2\cdots c_m \right).$$

A direct computation shows that this is the same as

$$\left( a_1a_k \right) \left( a_1a_{k-1} \right) \cdots \left( a_1a_2 \right) \left( b_1b_b \right) \left( b_1b_{b-1} \right) \cdots \left( b_1b_2 \right) \cdots \left( c_1c_s \right) \left( c_1c_{s-1} \right) \cdots \left( c_1c_2 \right).$$

This completes the proof.

The decomposition of a permutation into a product of 2-cycles given in Example 6 and in the proof of Theorem 5.4 is not the only way a permutation can be written as a product of 2-cycles. Although the next example shows that even the number of 2-cycles may vary from one decomposition to another, we will prove in Theorem 5.5 (first proved by Cauchy) that there is one aspect of a decomposition that never varies.

**Example 7**

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


We isolate a special case of Theorem 5.5 as a lemma.

**Lemma**

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

**Proof** Clearly, $r \neq 1$, since a 2-cycle is not the identity. If $r = 2$, we are done. So, we suppose that $r > 2$, and we proceed by induction.
Suppose that the rightmost 2-cycle is $(ab)$. Then, since $(ij) = (ji)$, the product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms shown on the right:

\[
\begin{align*}
\varepsilon &= (ab)(ab), \\
(ab)(bc) &= (ac)(ab), \\
(ac)(cb) &= (bc)(ab), \\
(ab)(cd) &= (cd)(ab).
\end{align*}
\]

If the first case occurs, we may delete $\beta_{r-1}\beta_r$ from the original product to obtain $\varepsilon = \beta_1\beta_2 \cdots \beta_{r-2}$, and therefore, by the Second Principle of Mathematical Induction, $r - 2$ is even. In the other three cases, we replace the form of $\beta_{r-1}\beta_r$ on the right by its counterpart on the left to obtain a new product of $r$ 2-cycles that is still the identity, but where the rightmost occurrence of the integer $a$ is in the second-from-the-rightmost 2-cycle of the product instead of the rightmost 2-cycle. We now repeat the procedure just described with $\beta_{r-2}\beta_{r-1}$, and, as before, we obtain a product of $(r - 2)$ 2-cycles equal to the identity or a new product of $r$ 2-cycles, where the rightmost occurrence of $a$ is in the third 2-cycle from the right. Continuing this process, we must obtain a product of $(r - 2)$ 2-cycles equal to the identity, because otherwise we have a product equal to the identity in which the only occurrence of the integer $a$ is in the leftmost 2-cycle, and such a product does not fix $a$, whereas the identity does. Hence, by the Second Principle of Mathematical Induction, $r - 2$ is even, and $r$ is even as well.

**Theorem 5.5 Always Even or Always Odd**

If a permutation $\alpha$ can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of $\alpha$ into a product of 2-cycles must have an even (odd) number of 2-cycles. In symbols, if

\[
\alpha = \beta_1\beta_2 \cdots \beta_r \quad \text{and} \quad \alpha = \gamma_1\gamma_2 \cdots \gamma_s,
\]

where the $\beta$'s and the $\gamma$'s are 2-cycles, then $r$ and $s$ are both even or both odd.

**Proof** Observe that $\beta_1\beta_2 \cdots \beta_r = \gamma_1\gamma_2 \cdots \gamma_s$ implies

\[
\varepsilon = \gamma_1\gamma_2 \cdots \gamma_s\beta_r^{-1} \cdots \beta_2^{-1}\beta_1^{-1} = \gamma_1\gamma_2 \cdots \gamma_s\beta_r \cdots \beta_2\beta_1,
\]

since a 2-cycle is its own inverse. Thus, the lemma on page 108 guarantees that $s + r$ is even. It follows that $r$ and $s$ are both even or both odd.

**Theorem 5.5 Always Even or Always Odd**

If a permutation $\alpha$ can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of $\alpha$ into a product of 2-cycles must have an even (odd) number of 2-cycles. In symbols, if

\[
\alpha = \beta_1\beta_2 \cdots \beta_r \quad \text{and} \quad \alpha = \gamma_1\gamma_2 \cdots \gamma_s,
\]

where the $\beta$'s and the $\gamma$'s are 2-cycles, then $r$ and $s$ are both even or both odd.

**Proof** Observe that $\beta_1\beta_2 \cdots \beta_r = \gamma_1\gamma_2 \cdots \gamma_s$ implies

\[
\varepsilon = \gamma_1\gamma_2 \cdots \gamma_s\beta_r^{-1} \cdots \beta_2^{-1}\beta_1^{-1} = \gamma_1\gamma_2 \cdots \gamma_s\beta_r \cdots \beta_2\beta_1,
\]

since a 2-cycle is its own inverse. Thus, the lemma on page 108 guarantees that $s + r$ is even. It follows that $r$ and $s$ are both even or both odd.
**Definition** Even and Odd Permutations
A permutation that can be expressed as a product of an even number of 2-cycles is called an *even* permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an *odd* permutation.

Theorems 5.4 and 5.5 together show that every permutation can be unambiguously classified as either even or odd. The significance of this observation is given in Theorem 5.6.

**Theorem 5.6** Even Permutations Form a Group

The set of even permutations in $\mathcal{S}_n$ forms a subgroup of $\mathcal{S}_n$.

**Proof** This proof is left to the reader (Exercise 17).

The subgroup of even permutations in $\mathcal{S}_n$ arises so often that we give it a special name and notation.

**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 $n$*.

The next result shows that exactly half of the elements of $\mathcal{S}_n$ ($n > 1$) are even permutations.

**Theorem 5.7**

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

**Proof** For each odd permutation $\alpha$, the permutation $(12)\alpha$ is even and, by the cancellation property in groups, $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many even permutations as there are odd ones. On the other hand, for each even permutation $\alpha$, the permutation $(12)\alpha$ is odd and $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many odd permutations as there are even ones. It follows that there are equal numbers of even and odd permutations. Since $|\mathcal{S}_n| = n!$, we have $|A_n| = n!/2$.