# Chapter 6
# Symmetric and Alternating Groups


We have seen the definition of the symmetric group $S_n$, but so far, we do not have too much experience with it. In this chapter, we will introduce the notions of cycles and, in particular, transpositions, which are important elements of the symmetric group. These will help us to understand the group.

We will also construct a subgroup of the symmetric group called the alternating group. If $n \geq 5$, then the alternating group is very special in that it has no nontrivial proper normal subgroups.

## 6.1 The Symmetric Group and Cycle Notation

Let $n$ be a positive integer. Then we recall that the set of permutations of the set $\{1, 2, \ldots, n\}$ is a group of order $n!$ under composition of functions. It is called the symmetric group and denoted $S_n$. Why is this group of sufficient interest to merit a chapter on its own? In the earliest years of group theory, the abstract definition of a group had not been written down. Instead, mathematicians worked with groups of permutations. As it turns out, they were not losing much by doing so! If $A$ is any nonempty set, write $P(A)$ for the set of all permutations of $A$. Then just as we saw that $S_n$ is a group under composition of functions, so is $P(A)$. The following famous result is due to Arthur Cayley.

**Theorem 6.1 (Cayley's Theorem).** *Let $G$ be any group. Then $G$ is isomorphic to a subgroup of $P(G)$.*

*Proof.* For each $a \in G$, define $\rho_a : G \to G$ via $\rho_a(g) = ag$, for all $g \in G$. We claim that $\rho_a \in P(G)$. Certainly $\rho_a(g) \in G$. If $\rho_a(g_1) = \rho_a(g_2)$, for $g_1, g_2 \in G$, then $ag_1 = ag_2$, so $g_1 = g_2$. Thus, $\rho_a$ is one-to-one. If $g \in G$, then $\rho_a(a^{-1}g) = g$, so $\rho_a$ is also onto. The claim is proved.

© Springer International Publishing AG, part of Springer Nature 2018

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_6

Now, define $\rho : G \to P(G)$ via $\rho(a) = \rho_a$. We claim that $\rho$ is a homomorphism. If $a, b \in G$, then $\rho(ab)(g) = \rho_{ab}(g) = abg$ and $(\rho(a) \circ \rho(b))(g) = \rho_a(\rho_b(g)) = \rho_a(bg) = abg$, for all $g \in G$. Thus, $\rho(ab) = \rho(a) \circ \rho(b)$, proving the claim. Also, if $a \in \ker(\rho)$, then $\rho_a$ is the identity permutation. In particular, $\rho_a(e) = e$, and therefore $ae = e$. Thus, $a = e$, and $\rho$ is one-to-one. It now follows that $G$ is isomorphic to $\rho(G)$, which is a subgroup of $P(G)$. □

**Corollary 6.1.** *Let $G$ be a group of order $n < \infty$. Then $G$ is isomorphic to a subgroup of $S_n$.*

*Proof.* We know that $G$ is isomorphic to a subgroup of $P(G)$, but replacing $G$ with $\{1, 2, \ldots, n\}$ is just a relabelling. Thus, $G$ is isomorphic to a subgroup of $S_n$. □

The notation we have been using for elements of $S_n$ is rather cumbersome and tends to hide the properties of the permutations. It is time to introduce something better.

**Definition 6.1.** Let $k$ be a positive integer. A permutation $\sigma \in S_n$ is called a **$k$-cycle** if there exist distinct elements $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$ such that $\sigma(a_i) = a_{i+1}$, for $1 \leq i < k$, $\sigma(a_k) = a_1$ and if $a \notin \{a_1, \ldots, a_k\}$, then $\sigma(a) = a$. We use the **cycle notation** $\sigma = (a_1\ a_2\ \cdots\ a_k)$. A **cycle** means a $k$-cycle for some $k$.

*Example 6.1.* Let us work in $S_5$. Then $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$ is a 3-cycle; as $\sigma(2) = 5$, $\sigma(5) = 4$, $\sigma(4) = 2$ and everything else is fixed, we have $\sigma = (2\ 5\ 4)$. Note that it would be just as correct to write $\sigma = (5\ 4\ 2)$ or $(4\ 2\ 5)$ (but not $(2\ 4\ 5)$). Similarly, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$ satisfies $\tau(1) = 3$, $\tau(3) = 2$, $\tau(2) = 5$, $\tau(5) = 4$, $\tau(4) = 1$, and there are no other values to consider, so $\tau$ is the 5-cycle $(1\ 3\ 2\ 5\ 4)$ (or $(3\ 2\ 5\ 4\ 1)$, and so on).

Note that the only 1-cycle in $S_n$ is the identity permutation, denoted $(1)$.

**Theorem 6.2.** *Any $k$-cycle in $S_n$ has order $k$.*

*Proof.* Simply note that if $\sigma = (a_1\ \cdots\ a_k)$, then $\sigma(a_1) = a_2$, $\sigma^2(a_1) = \sigma(a_2) = a_3$, and so on. It takes $k$ steps to reach $a_1$ again. Similarly for all other $a_i$. □

**Definition 6.2.** We say that cycles $\sigma_1, \ldots, \sigma_r$ are **disjoint** if, whenever $\sigma_i(a) \neq a$, we have $\sigma_j(a) = a$ for all $j \neq i$. If $\sigma \in S_n$ and we write $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$, where the $\sigma_i$ are disjoint cycles, then we have a **disjoint cycle decomposition** for $\sigma$.

*Example 6.2.* Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}$ in $S_6$. Then noting that $\sigma(1) = 5$, $\sigma(5) = 4$ and $\sigma(4) = 1$, we have a cycle $(1\ 5\ 4)$. Also, $\sigma(2) = 6$ and $\sigma(6) = 2$, so we have another cycle $(2\ 6)$. The remaining number, 3, is fixed by $\sigma$, so a disjoint cycle decomposition for $\sigma$ is $\sigma = (1\ 5\ 4)(2\ 6)$.

*Example 6.3.* Similarly, consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 6 & 8 & 4 & 3 & 7 \end{pmatrix}$. Using the same procedure as above, we find that $\sigma = (1\ 2)(3\ 5\ 8\ 7)(4\ 6)$ is a disjoint cycle decomposition.

In fact, we can always apply the procedure from the last two examples.

**Theorem 6.3.** *Every element of $S_n$ is a product of disjoint cycles.*

*Proof.* Take any $\sigma \in S_n$. If $\sigma$ is the identity, then $\sigma = (1)$ and there is nothing to do. Assume otherwise, and take $a_1 \in \{1, \ldots, n\}$ such that $\sigma(a_1) = a_2 \neq a_1$. If $\sigma(a_2) = a_1$, then we have a 2-cycle, $(a_1\ a_2)$. Otherwise, let $\sigma(a_2) = a_3$. Continue until we find $a_k$ such that $\sigma(a_k) \in \{a_1, \ldots, a_k\}$. Now, if $\sigma(a_k) = a_i$, with $1 < i \leq k$, then $\sigma^k(a_1) = \sigma^{i-1}(a_1)$. Thus, $\sigma^{k-i+1}(a_1) = a_1$. In other words, $a_{k-i+2} = a_1$. But this is a contradiction. Therefore, $\sigma(a_k) = a_1$, and we have a $k$-cycle, $(a_1\ a_2\ \cdots\ a_k)$.

If $\sigma = (a_1\ a_2\ \cdots\ a_k)$, then we are done. Otherwise, take $b_1$ which is not in $\{a_1, \ldots, a_k\}$ such that $\sigma(b_1) = b_2 \neq b_1$. Now repeat the same procedure, obtaining an $l$-cycle, $(b_1\ b_2\ \cdots\ b_l)$. We must make sure that these cycles are disjoint; that is, we cannot have $b_m \in \{a_1, \ldots, a_k\}$, for any $m$. By choice, $b_1 \notin \{a_1, \ldots, a_n\}$. If $b_2 = \sigma(b_1) = a_t$, then since $a_t = \sigma(a_s)$, for some $s$, we have $\sigma(b_1) = \sigma(a_s)$, and as $\sigma$ is one-to-one, $b_1 = a_s$, which is impossible. Proceeding in this way, we see that the cycles are disjoint.

If $\sigma = (a_1\ \cdots\ a_k)(b_1\ \cdots\ b_l)$, then we are done. Otherwise, take any $c_1$ that does not lie in $\{a_1, \ldots, a_k, b_1, \ldots, b_l\}$ such that $\sigma(c_1) \neq c_1$ and repeat. As there are only $n$ entries in $\{1, \ldots, n\}$, this procedure must stop eventually. □

We were not too concerned about the order in which we wrote the cycles in the last proof. But this is ok.

**Theorem 6.4.** *In $S_n$, disjoint cycles commute.*

*Proof.* Let $\sigma = (a_1\ \cdots\ a_k)$ and $\tau = (b_1\ \cdots\ b_m)$ be disjoint cycles. We will show that $\sigma\tau = \tau\sigma$. Take $c \in \{1, \ldots, n\}$. If $c \in \{a_1, \ldots, a_k\}$, then as $\sigma$ and $\tau$ are disjoint, $\tau$ fixes $c$. Thus, $\sigma\tau(c) = \sigma(c)$. But $\sigma(c) \in \{a_1, \ldots, a_k\}$ as well. Thus, $\tau$ fixes $\sigma(c)$ too, so $\tau\sigma(c) = \sigma(c)$. By a similar argument, if $c \in \{b_1, \ldots, b_m\}$, then $\sigma\tau(c) = \tau\sigma(c) = \tau(c)$. If $c$ is not among the $a_i$ or $b_i$, then both $\sigma$ and $\tau$ fix $c$, so $\sigma\tau(c) = \tau\sigma(c) = c$. We are done. □

*Example 6.4.* It makes no difference if we write $(1\ 5)(2\ 6\ 4)$ or $(2\ 6\ 4)(1\ 5)$. Both are the same permutation.

However, it would be wrong to try to extend this to cycles that are not disjoint!

*Example 6.5.* In $S_3$, let $\sigma = (1\ 2)$ and $\tau = (1\ 3)$. Let us compute $\sigma\tau$. Now, $\tau(1) = 3$ and $\sigma(3) = 3$, so $\sigma\tau(1) = 3$. Also, $\tau(3) = 1$ and $\sigma(1) = 2$, so $\sigma\tau(3) = 2$. Finally, $\tau(2) = 2$ and $\sigma(2) = 1$, so $\sigma\tau(2) = 1$. There are no other values to consider, so $\sigma\tau$ is the 3-cycle $(1\ 3\ 2)$. But proceeding in the same way, we find that $\tau\sigma$ is a different 3-cycle, $(1\ 2\ 3)$.

*Example 6.6.* Let us find a disjoint cycle decomposition for (2 4)(2 5 3 4)(1 3)(1 5). We see (working from right to left) that 1 is mapped by (1 5) to 5, which is fixed by (1 3), which then goes to 3, which is fixed by (2 4). So, 1 goes to 3. Next, 3 is fixed by (1 5), then goes to 1, which is fixed by the other cycles, so we have a 2-cycle (1 3). Next, 2 is fixed by (1 3)(1 5), it then goes to 5, which is fixed by (2 4), so 2 goes to 5. Now, 5 goes to 1 which goes to 3 which goes to 4 and then back to 2. Thus, we have another 2-cycle, (2 5). Finally, 4 goes to 2 then back to 4, so 4 is fixed. Therefore, we have (2 4)(2 5 3 4)(1 3)(1 5) = (1 3)(2 5).

We can use the disjoint cycle decomposition to find the order of a permutation. Recall that the **least common multiple** of positive integers $a_1, a_2, \ldots, a_r$ is the smallest positive integer $m$ such that $a_i | m$ for all $i$.

**Theorem 6.5.** *If $\sigma_1, \ldots, \sigma_r$ are disjoint cycles in $S_n$, then the order of $\sigma_1 \cdots \sigma_r$ is the least common multiple of the lengths of the $\sigma_i$.*

*Proof.* Let $k$ be a positive integer. Then since the $\sigma_i$ commute, by Theorem 6.4, we have $(\sigma_1 \cdots \sigma_r)^k = \sigma_1^k \cdots \sigma_r^k$. As the $\sigma_i$ move disjoint subsets of $\{1, \ldots, n\}$, we have $\sigma_1^k \cdots \sigma_r^k = (1)$ if and only if each $\sigma_i^k = (1)$. In view of Theorem 6.2, this occurs if and only if the length of each $\sigma_i$ divides $k$. □

## Exercises

**6.1.** Write each of the following permutations as a product of disjoint cycles.

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

**6.2.** Write each of the following permutations as a product of disjoint cycles.

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

**6.3.** Find the inverse of each of the following permutations. Write the answer as a product of disjoint cycles.

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

**6.4.** Find all possible orders of elements of $S_7$.

**6.5.** How many elements of order 3 are there in $S_9$?

**6.6.** Let $\sigma$ be a $k$-cycle. If $m$ is a positive integer, show that $\sigma^m$ is a $k$-cycle if and only if $(k, m) = 1$.

**6.7.** Let $\sigma \in S_n$ be a $k$-cycle. Show that there exists a $k$-cycle $\tau \in S_n$ such that $\tau^2 = \sigma$ if and only if $k$ is odd.

**6.8.** If $n \neq 2$, show that $Z(S_n) = \{(1)\}$.

**6.9.** Find the smallest positive integers $m$ and $n$ such that $S_m$ has an element of order 105 and $S_n$ has an element of order 125.

**6.10.** Find a subgroup of order 120 in $S_8$.

## 6.2 Transpositions and the Alternating Group

While a disjoint cycle decomposition gives us the clearest picture of the action of a permutation, it is often useful to write the permutation as a different sort of product.

**Definition 6.3.** A **transposition** is a 2-cycle.

**Theorem 6.6.** *If $n \geq 2$, then every permutation in $S_n$ is a product of transpositions.*

*Proof.* In view of Theorem 6.3, it is sufficient to show that every cycle is a product of transpositions. The identity is $(1) = (1\ 2)(1\ 2)$. Let us take a $k$-cycle $\sigma$; without loss of generality, say $\sigma = (1\ 2\ 3\ \cdots\ k)$. We claim that $\sigma = (1\ k)(1\ (k-1))\cdots(1\ 2)$. Our proof is by induction on $k$. If $k = 2$, there is nothing to do. Otherwise, assume that $(1\ 2\ \cdots\ k) = (1\ k)(1\ (k-1))\cdots(1\ 2)$. Then

$$(1\ (k+1))(1\ k)\cdots(1\ 2) = (1\ (k+1))(1\ 2\ \cdots\ k),$$

and performing the calculation, we see that this is $(1\ 2\ \cdots\ (k+1))$, as required. □

*Example 6.7.* Let us write $(1\ 4\ 5)(1\ 3\ 6\ 4\ 5)$ as a product of transpositions. Using the method described in the above proof,

$$(1\ 4\ 5) = (1\ 5)(1\ 4)$$

and

$$(1\ 3\ 6\ 4\ 5) = (1\ 5)(1\ 4)(1\ 6)(1\ 3),$$

so

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

It is worth noting that the expression of a permutation as a product of transpositions is by no means unique. For instance, we have seen that $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$. But also, $(1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4)$. In fact, the number of transpositions involved does not have to be the same, as both of these are equal to $(5\ 6)(1\ 2)(2\ 3)(3\ 4)(5\ 6)$.

Nevertheless, we note that all of the products we have just calculated involve an odd number of transpositions. It is a very useful fact that this parity is always preserved; that is, a permutation will be a product of either an even or an odd number of transpositions, not both. The following lemma does most of the work in proving this fact.

**Lemma 6.1.** *In $S_n$, the identity permutation cannot be written as a product of an odd number of transpositions.*

*Proof.* Suppose that the lemma is false, and let $k$ be the smallest odd number such that $(1) = \sigma_1\sigma_2\cdots\sigma_k$, where each $\sigma_i$ is a transposition. Now, choose an element of $\{1, \ldots, n\}$ that is not fixed by all of the $\sigma_i$. Without loss of generality, let us say that some $\sigma_i(1) \neq 1$. Let $j$ be such that $\sigma_j(1) \neq 1$ but $\sigma_r(1) = 1$ for all $r > j$. Among all expressions of (1) as a product of $k$ transpositions such that at least one does not fix 1, we proceed by induction on $j$. If $j = 1$, then we note that $\sigma_2\cdots\sigma_k$ fixes 1, but $\sigma_1$ does not, so $\sigma_1\cdots\sigma_k$ does not fix 1, which is a contradiction.

Therefore, assume that $j > 1$ and that our result holds for expressions with a smaller $j$ value. Without loss of generality, say that $\sigma_j = (1\ 2)$. We have four cases to consider for $\sigma_{j-1}$. If $\sigma_{j-1} = (1\ 2)$, then since $(1\ 2)(1\ 2)$ is the identity, we can cancel it from our expression. But this contradicts the minimality of $k$.

Suppose that $\sigma_{j-1}$ fixes 1 but not 2. Without loss of generality, say $\sigma_{j-1} = (2\ 3)$. Then notice that $(2\ 3)(1\ 2) = (1\ 3\ 2) = (1\ 3)(2\ 3)$. Thus, replacing $\sigma_{j-1}\sigma_j$ with $(1\ 3)(2\ 3)$, we see that the $j$ value has now decreased to $j - 1$. By our inductive hypothesis, it is impossible to write the identity as a product in this way.

Suppose that $\sigma_{j-1}$ fixes 2 but not 1. Without loss of generality, say $\sigma_{j-1} = (1\ 3)$. Then we see that $(1\ 3)(1\ 2) = (1\ 2\ 3) = (1\ 2)(2\ 3)$. Again, replacing $\sigma_{j-1}\sigma_j$ with $(1\ 2)(2\ 3)$, the $j$ value decreases, and we have a contradiction.

Finally, suppose that $\sigma_{j-1}$ fixes both 1 and 2. Without loss of generality, say $\sigma_{j-1} = (3\ 4)$. Then by Theorem 6.4, $(3\ 4)(1\ 2) = (1\ 2)(3\ 4)$, so we can once again decrease the $j$ value. Our proof is complete. □

**Theorem 6.7.** *No permutation in $S_n$ can be written as a product of both an even and an odd number of transpositions.*

*Proof.* Suppose that

$$\sigma_1\sigma_2\cdots\sigma_k = \tau_1\tau_2\cdots\tau_m,$$

where each $\sigma_i$ and $\tau_i$ is a transposition, $k$ is even and $m$ is odd. Then

$$(1) = \sigma_k^{-1}\cdots\sigma_1^{-1}\tau_1\cdots\tau_m = \sigma_k\cdots\sigma_1\tau_1\cdots\tau_m,$$

since each $\sigma_i$ has order 2 (by Theorem 6.2) and is therefore its own inverse. Thus, we have written the identity as a product of $k + m$ transpositions. But $k + m$ is odd, contradicting the preceding lemma. □

**Definition 6.4.** We say that a permutation in $S_n$ is **even** (respectively, **odd**) if it is the product of an even (respectively, odd) number of transpositions.

*Example 6.8.* In $S_5$, we note that $(1\ 2\ 3)(4\ 5)$ is odd, as $(1\ 2\ 3)(4\ 5) = (1\ 3)(1\ 2)(4\ 5)$.

**Theorem 6.8.** *A $k$-cycle is even if and only if $k$ is odd.*

*Proof.* If $k = 1$, then we know that the identity is even. If $k > 1$, then refer to the proof of Theorem 6.6, where we wrote a $k$-cycle as a product of $k - 1$ transpositions. □

Thus, to determine if a particular permutation is even or odd, we can look at its disjoint cycle decomposition. The preceding theorem tells us whether each cycle is a product of an even or odd number of transpositions, so we can easily determine the answer for the entire permutation.

**Definition 6.5.** The **alternating group** $A_n$ is the set of all even permutations in $S_n$.

*Example 6.9.* We note that $S_3$ consists of the identity (which is even), three transpositions (which are odd) and two 3-cycles (which are even). Thus,

$$A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Similarly $S_4$ consists of the identity (even), six transpositions (odd), eight 3-cycles (even), six 4-cycles (odd) and three elements that are products of two disjoint transpositions (even). Thus,

$$\begin{aligned} A_4 = \{&(1), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), \\ &(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}. \end{aligned}$$

**Theorem 6.9.** *Let $n \geq 2$. Then $A_n$ is a normal subgroup of $S_n$, and $[S_n : A_n] = 2$.*

*Proof.* Define $\alpha : S_n \to \mathbb{Z}_2$ as follows. Let $\alpha(\sigma) = 0$ if $\sigma$ is even and 1 if $\sigma$ is odd. We claim that $\alpha$ is a homomorphism. Indeed, as the product of two even or two odd permutations is even, and the product of an even and an odd is odd, this follows immediately. By definition, the kernel is $A_n$, so $A_n$ is a normal subgroup. Furthermore, $\alpha((1)) = 0$ and $\alpha((1\ 2)) = 1$, so $\alpha$ is onto. Thus, by the First Isomorphism Theorem, $S_n/A_n$ is isomorphic to $\mathbb{Z}_2$. That is, $|S_n/A_n| = 2$, so $A_n$ has index 2. □

**Exercises**

**6.11.** Decide if each of the following permutations is even or odd.

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

**6.12.** Write each of the following permutations as a product of transpositions.

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

**6.13.** Find every possible order of the product of two transpositions.

**6.14.** Let $n \geq 2$ and $H \leq S_n$. Show that either every element of $H$ is even, or exactly half of the elements of $H$ are even.

**6.15.** For which $n \geq 2$ does $A_n$ have a subgroup of order 4? What if we insist that the subgroup be cyclic?

**6.16.** Find the orders of all the elements of $A_8$.

**6.17.** If $n \geq 2$, show that every element of odd order in $S_n$ lies in $A_n$.

**6.18.** Show that every permutation other than the identity in $S_n$ is the product of at most $n - 1$ transpositions.

**6.19.** For which positive integers $n$ does $S_n$ have

1. more elements of even order than odd order;
2. more elements of odd order than even order;
3. the same number of elements of odd order as even order?

**6.20.** For which integers $n \geq 2$ does there exist a $\sigma \in A_n$ such that $|\sigma| > n$?

## 6.3 The Simplicity of the Alternating Group

Why are we so interested in the group $A_n$? In order to explain this, we must start with a definition.

**Definition 6.6.** A group is **simple** if it is nontrivial and has no nontrivial proper normal subgroups.

If $G$ is abelian, then every subgroup is normal, so we are looking for groups whose only subgroups are $G$ and $\{e\}$. But these were determined in Exercise 3.52. Indeed, we saw that these were precisely the cyclic groups of prime order. By Theorem 4.14, we have the following result.

**Theorem 6.10.** *Let $G$ be an abelian group. Then $G$ is simple if and only if $G$ is isomorphic to $\mathbb{Z}_p$, for some prime $p$.*

That was pretty painless! However, the nonabelian case is much much more difficult. Much! The classification of all of the finite simple groups was one of the biggest mathematical projects of the twentieth century. Over one hundred mathematicians contributed to the solution, and the proof consists of many thousands of pages of journal articles. For obvious reasons, we will not be discussing this classification here.

We will content ourselves with proving one of the earliest results on the subject; namely, if $n \geq 5$ then $A_n$ is a nonabelian simple group. (Actually, $A_5$ is the smallest nonabelian simple group.) The $n = 5$ case was established by Évariste Galois in the early nineteenth century. Decades later, M.E. Camille Jordan provided a proof for all $n \geq 5$.

Why are finite simple groups so interesting? Let us look at it this way. Suppose that $G$ is a nontrivial finite group. Let $N_1$ be a proper normal subgroup of largest order in $G$. (If $G$ is simple, this will be $\{e\}$. Otherwise, it will be something larger.) Now, we claim that $G/N_1$ is simple. Indeed, by Theorem 4.8, the normal subgroups of $G/N_1$ are precisely of the form $H/N_1$, where $H$ is a normal subgroup of $G$ containing $N_1$. But by definition of $N_1$, $H = N_1$ or $G$. Thus, $G/N_1$ has no nontrivial proper normal subgroups, so it is simple.

Now, suppose that $N_1 \neq \{e\}$. Then in the same way, take a proper normal subgroup $N_2$ of $N_1$ of largest possible order. Then $N_1/N_2$ is simple. We can repeat this procedure and obtain

$$G = N_0 \geq N_1 \geq N_2 \geq N_3 \geq \cdots \geq N_{k-1} \geq N_k = \{e\},$$

where each $N_{i+1}$ is normal in $N_i$ and $N_i/N_{i+1}$ is simple. We know the process must end, as each $N_{i+1}$ is properly contained in $N_i$, and the original group is finite. In a way, then, finite groups can be built up using simple groups.

Let us begin the process of proving that $A_n$ is simple, for $n \geq 5$. We start with a general fact about the conjugation of cycles.

**Lemma 6.2.** *Let $\sigma = (a_1\ a_2\ \cdots\ a_k)$ be a $k$-cycle in $S_n$. If $\tau \in S_n$, then $\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \cdots\ \tau(a_k))$.*

*Proof.* Suppose that $b = \tau(a_i)$. Then $\tau^{-1}(b) = a_i$; hence, $\sigma(\tau^{-1}(b)) = \sigma(a_i) = a_{i+1}$ (or $a_1$, if $i = k$). Therefore, $\tau\sigma\tau^{-1}(b) = \tau(a_{i+1})$ (or $\tau(a_1)$, if $i = k$). That is, $\tau\sigma\tau^{-1}$ permutes the $\tau(a_i)$ as described. If $b$ is not among the $\tau(a_i)$, then $\tau^{-1}(b)$ is not equal to any $a_i$, which means that it is fixed by $\sigma$. Thus, $\tau\sigma\tau^{-1}(b) = \tau\tau^{-1}(b) = b$. Therefore, $\tau\sigma\tau^{-1}$ is the $k$-cycle described in the statement of the lemma. □

**Corollary 6.2.** *Let $n$ and $k$ be positive integers with $n \geq k$. Then*

1. *any two $k$-cycles are conjugate in $S_n$; and*
2. *if $k$ is odd and $n \geq k + 2$, then any two $k$-cycles are conjugate in $A_n$.*

*Proof.* (1) Let $\sigma = (a_1\ \cdots\ a_k)$ and $\delta = (b_1\ \cdots\ b_k)$ be any two $k$-cycles. The preceding lemma tells us that in order to show that $\sigma$ and $\delta$ are conjugate, we need only find $\tau \in S_n$ such that $\tau(a_i) = b_i$ for all $i$; in this case, $\tau\sigma\tau^{-1} = \delta$. But $S_n$ contains every possible permutation of $\{1, \ldots, n\}$. Thus, we can certainly assign $\tau(a_i) = b_i$, and for the $j \notin \{a_1, \ldots, a_k\}$, let the $\tau(j)$ be any distinct values not in $\{b_1, \ldots, b_k\}$.

(2) As $k$ is odd, the $k$-cycles are even, and therefore lie in $A_n$. Let $\sigma$ and $\delta$ be any $k$-cycles. Without loss of generality, let us say that $\delta = (1\ 2\ \cdots\ k)$. Then just as in (1), we can find $\tau \in S_n$ such that $\tau\sigma\tau^{-1} = \delta$. If $\tau \in A_n$, then we are done. Otherwise, $\tau$ is odd, so $((k+1)\ (k+2))\tau$ is even. (Note that this is valid, as $n \geq k + 2$.) Thus, letting $\eta = ((k+1)\ (k+2))\tau \in A_n$, we have

$$\begin{aligned}\eta\sigma\eta^{-1} &= ((k+1)\ (k+2))\tau\sigma\tau^{-1}((k+1)\ (k+2)) \\ &= ((k+1)\ (k+2))(1\ 2\ \cdots\ k)((k+1)\ (k+2)).\end{aligned}$$

But disjoint cycles commute, so this is

$$((k+1)\ (k+2))((k+1)\ (k+2))\delta = \delta.$$

We are done. □

*Example 6.10.* The preceding lemma tells us that (1 2 3) and (1 3 2) are conjugate in $S_3$, and the proof suggests how we might demonstrate it. We need to find $\tau$ such that $\tau(1) = 1$, $\tau(2) = 3$ and $\tau(3) = 2$; that is, $\tau = (2\ 3)$. Then $(1\ 3\ 2) = \tau(1\ 2\ 3)\tau^{-1}$. However, (1 2 3) and (1 3 2) are not conjugate in $A_3$; this is obvious, as $A_3$ is abelian, having order 3, so different elements are not conjugate. It is less obvious that they are not conjugate in $A_4$ either; however, it is possible to try conjugating (1 2 3) by all of the elements of $A_4$. None of these conjugates will equal (1 3 2). However, the preceding lemma tells us that (1 2 3) and (1 3 2) are indeed conjugate in $A_5$, and the proof tells us that if we take $\eta = (4\ 5)\tau$, then $\eta \in A_5$, and we find that $\eta(1\ 2\ 3)\eta^{-1} = (1\ 3\ 2)$.

We can now simplify our task by showing that if we have a 3-cycle in a normal subgroup of $A_n$, then we have all of $A_n$.

**Corollary 6.3.** *Let $n \geq 3$. Then*

1. *every element of $A_n$ is a product of 3-cycles; and*
2. *if a normal subgroup $N$ of $A_n$ contains any 3-cycle, then $N = A_n$.*

*Proof.* (1) We know that an element of $A_n$ is a product of an even number of transpositions. Thus, it is sufficient to show that every product of two transpositions is a product of 3-cycles. (As $(1) = (1\ 2\ 3)(1\ 3\ 2)$, we need not worry about the identity.) If the two transpositions are equal, then their product is the identity, with which we have just dealt. Suppose they have one number in common. Without loss of generality, say $(1\ 2)(1\ 3)$. Then note that $(1\ 2)(1\ 3) = (1\ 3\ 2)$, which is a 3-cycle. Finally, suppose they have no numbers in common. Without loss of generality, say $(1\ 2)(3\ 4)$. Then we observe that $(1\ 2)(3\ 4) = (1\ 4\ 3)(1\ 2\ 3)$, which is a product of 3-cycles.

(2) In view of (1), it is sufficient to show that $N$ contains all of the 3-cycles. But it contains one 3-cycle, so as $N$ is normal, it contains all of its conjugates. If $n \geq 5$, then Corollary 6.2 tells us that these conjugates are all of the 3-cycles, and we are done. If $n = 3$, there is little to do, as the only 3-cycles are (1 2 3) and (1 3 2), and they are squares of each other; thus, if $N$ contains one, it contains the other. The $n = 4$ case requires a little more work, and we leave it as Exercise 6.24. □

And now, our main result for this section.

**Theorem 6.11.** *If $n \geq 5$, then $A_n$ is a nonabelian simple group.*

*Proof.* The fact that $(1\ 2\ 3)(1\ 2\ 4) \neq (1\ 2\ 4)(1\ 2\ 3)$ shows that $A_n$ is nonabelian, so we can focus on the simplicity. Let $N$ be a nontrivial normal subgroup of $A_n$. We

must prove that $N = A_n$. In view of Corollary 6.3, it is sufficient to show that $N$ contains a 3-cycle.

Take any $(1) \neq \sigma \in N$, and consider the disjoint cycle decomposition of $\sigma$. Suppose, first of all, that there are two or more transpositions in this decomposition. Without loss of generality, say $\sigma = (1\ 2)(3\ 4)\delta$, where $\delta$ is a product of disjoint cycles which also fix everything in $\{1, 2, 3, 4\}$ (and $\delta = (1)$ is possible). Let $\tau = (1\ 2\ 4) \in A_n$. Then as $N$ is normal in $A_n$, we have $\tau\sigma\tau^{-1} \in N$. That is,

$$(1\ 2\ 4)(1\ 2)(3\ 4)\delta(1\ 4\ 2) \in N.$$

(It is easy to check that $(1\ 2\ 4)^{-1} = (1\ 4\ 2)$.) As the cycles in $\delta$ are disjoint from all the other cycles in the product, we see from Theorem 6.4 that $N$ contains

$$(1\ 2\ 4)(1\ 2)(3\ 4)(1\ 4\ 2)\delta = (1\ 3)(2\ 4)\delta.$$

But $N$ also contains $\sigma^{-1}$, and therefore

$$\sigma^{-1}(1\ 3)(2\ 4)\delta = \delta^{-1}(3\ 4)(1\ 2)(1\ 3)(2\ 4)\delta \in N.$$

Again, $\delta$ commutes with these other cycles, so we have

$$\delta^{-1}\delta(3\ 4)(1\ 2)(1\ 3)(2\ 4) = (1\ 4)(2\ 3) \in N.$$

Let $\eta = (1\ 4\ 5) \in A_n$ (since $n \geq 5$). Then $N$ must contain

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

Thus, $N$ also contains

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

But when $N$ contains a 3-cycle, we know that $N = A_n$. Thus, from this point on, we may assume that the disjoint cycle decomposition of $\sigma$ contains at most one transposition.

Now, let us consider the length $k$ of the longest cycle appearing in the disjoint cycle decomposition of $\sigma$. If $k = 2$, then $\sigma$ is a product of an even number of disjoint transpositions, and we have already dealt with this case.

Suppose that $k = 3$. Then $\sigma$ is a product of some 3-cycles and, possibly, some transpositions. But the product of some 3-cycles and a single transposition is odd, and therefore not in $A_n$. Furthermore, multiple transpositions are not allowed. Therefore, we may assume that $\sigma$ is a product of one or more 3-cycles. If it is just one 3-cycle, then we are done. So assume that it is a product of two or more disjoint 3-cycles. Without loss of generality, say $\sigma = (1\ 2\ 3)(4\ 5\ 6)\delta$, where either $\delta = (1)$ or $\delta$ is a product of disjoint 3-cycles, all of which fix everything in $\{1, 2, 3, 4, 5, 6\}$. Let $\tau = (3\ 4\ 5) \in A_n$. Then as $N$ is normal, it contains

$$\tau\sigma\tau^{-1} = (3\ 4\ 5)(1\ 2\ 3)(4\ 5\ 6)\delta(3\ 5\ 4) = (1\ 2\ 4)(3\ 6\ 5)\delta,$$

since $\delta$ commutes with the other cycles. But $N$ also contains $\sigma^{-1}$, so we have

$$\sigma^{-1}(1\ 2\ 4)(3\ 6\ 5)\delta = \delta^{-1}(4\ 6\ 5)(1\ 3\ 2)(1\ 2\ 4)(3\ 6\ 5)\delta = (2\ 6\ 4\ 3\ 5) \in N,$$

again, since $\delta$ is disjoint from the other cycles. Replacing $\sigma$ with $(2\ 6\ 4\ 3\ 5)$, we can move to our final case.

Let us suppose that $k \geq 4$. Then without loss of generality, we may write $\sigma = (1\ 2\ 3\ \cdots\ k)\delta$, where $k \geq 4$ and $\delta$ is some product of disjoint cycles, all of which fix everything in $\{1, 2, \ldots, k\}$. Let $\tau = (1\ 2\ 3) \in A_n$. Then by normality, $N$ contains

$$\tau\sigma\tau^{-1} = (1\ 2\ 3)(1\ 2\ 3\ \cdots\ k)\delta(1\ 3\ 2) = (1\ 4\ 5\ \cdots\ k\ 2\ 3)\delta.$$

But $N$ also contains $\sigma^{-1}$, so noting that $(1\ 2\ 3\ \cdots\ k)^{-1} = (1\ k\ (k-1)\ \cdots\ 2)$, we have

$$\sigma^{-1}(1\ 4\ 5\ \cdots\ k\ 2\ 3)\delta = \delta^{-1}(1\ k\ (k-1)\ \cdots\ 2)(1\ 4\ 5\ \cdots\ k\ 2\ 3)\delta = (1\ 3\ k) \in N,$$

again using the fact that $\delta$ commutes with everything else. Thus, $N$ contains a 3-cycle, and the proof is complete. □

We might well ask about $A_n$ when $n < 5$. For $n = 2$, $A_2$ is the trivial group; hence, by definition, not simple. When $n = 3$, $A_3$ has order 3 and by Corollary 4.2, it is isomorphic to $\mathbb{Z}_3$. By Theorem 6.10, it is an abelian simple group. The big exception is the $n = 4$ case, as illustrated in the following example.

*Example 6.11.* The alternating group $A_4$ is not simple. To see, this let

$$N = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

It simply requires some computation to see that $N$ is a nontrivial proper normal subgroup of $A_4$.

With the exception of $S_2$, which is abelian of order 2, and hence isomorphic to $\mathbb{Z}_2$, the symmetric groups are not simple. Indeed, $A_n$ is a nontrivial proper normal subgroup of $S_n$, whenever $n \geq 3$. However, we can state the following result.

**Corollary 6.4.** *If $n \geq 5$, then the only nontrivial proper normal subgroup of $S_n$ is $A_n$.*

*Proof.* Let $N$ be a normal subgroup of $S_n$. Then $N \cap A_n$ is a normal subgroup of $A_n$. As $A_n$ is simple, this means that $N \cap A_n = A_n$ or $\{(1)\}$. If $N \cap A_n = A_n$, then $A_n \leq N$. But by Lagrange's theorem, this implies that $|A_n|$ divides $|N|$ and $|N|$ divides $|S_n|$. As $|S_n| = 2|A_n|$ (because $A_n$ is of index 2), this can only mean that $|N| = |A_n|$ or $|S_n|$. Thus, $N = A_n$ or $S_n$, as desired.

On the other hand, suppose that $N \cap A_n = \{(1)\}$. Then by Theorem 4.4, $|NA_n| = |N||A_n|$. As $|A_n| = |S_n|/2$ and $|NA_n| \leq |S_n|$, we see that $|N| = 1$ or 2. If $|N| = 1$, we are done, so suppose that $|N| = 2$. But by Exercise 4.3, a normal subgroup of order 2 in a group is central. However, Exercise 6.8 tells us that the centre of $S_n$ is trivial. Thus, we have a contradiction, and the proof is complete. □

**Exercises**

**6.21.** Show that $A_5$ has no subgroup of order 30.

**6.22.** In $S_7$, describe the conjugates of $(1\ 2)(3\ 4\ 5)$.

**6.23.** Can a nonabelian simple group have a nonabelian simple proper subgroup? Either prove that it cannot, or construct an explicit example.

**6.24.** Let $N$ be a normal subgroup of $A_4$ containing a 3-cycle. Show that $N = A_4$.

**6.25.** Show that the only nontrivial proper normal subgroup of $A_4$ is the one exhibited in Example 6.11.

**6.26.** Let $n \geq 2$. Show that every element of $S_n$ can be written as a product of transpositions of the form $(1\ i)$, for various $i$.

**6.27.** If $n \geq 2$, show that every element of $S_n$ can be written as a product of the transpositions $(1\ 2), (2\ 3), \ldots, ((n-1)\ n)$.

**6.28.** If $n \geq 2$, let $\sigma = (1\ 2)$ and $\tau = (1\ 2\ 3\ \cdots\ n)$. Show that every element of $S_n$ can be written in the form $\sigma^{i_1}\tau^{j_1}\sigma^{i_2}\tau^{j_2}\cdots\sigma^{i_k}\tau^{j_k}$, where the exponents are any integers and $k \in \mathbb{N}$.