Chapter 6

Permutation Groups

6.1 Definitions and Array Notation

In this chapter, we will study transformations which reshuffle the elements of a set. Mathematically, these transformations are bijections from a set to itself. Such bijections are called **permutations**. More precisely, we have the following definition.

Definition 224 *Let A be a nonempty set.*

1. *A **permutation** of the set A is a bijection from A to itself in other words a function $\alpha : A \to A$ such that α is a bijection (one-to-one and onto).*

2. *A **permutation group** of a set A is a set of permutations of A that forms a group under composition of functions.*

3. *The **symmetric group** of a set A, denoted S_A, is the set of all permutations of A. It can be shown that such a set, with composition of functions, forms a group. In the case A is finite, that is $A = \{1, 2, 3, 4, ..., n\}$, then we denote the symmetric group by S_n.*

Symmetric groups were used in mathematics before the abstract concept of a group had been formulated. In particular, they were used to obtain important results about the solutions of polynomial equations. Their study is partly responsible for the development of the abstract concept of a group. It can also be shown (Cayley's theorem) that every group can be thought of as a subgroup of some symmetric group. For now, we will focus on permutations on a finite set $A = \{1, 2, ..., n\}$.

Let $\alpha \in S_n$, that is α is a permutation on $A = \{1, 2, ..., n\}$. Then, α shuffles the elements of A. We can represent α explicitly in array notation by writing

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix}$$

where the top row represent the original elements and the bottom row represents what each element is mapped to. Note that some texts use square brackets. This is one of the notations of a permutation. Below, we will see there is another way to represent permutations. Let us look at some specific examples.

Example 225 *Let* $A = \{1,2,3,4\}$ *and suppose that* $\alpha(1) = 3$, $\alpha(2) = 1$, $\alpha(3) = 4$ *and* $\alpha(4) = 2$ *then we would write*

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

and to indicate the action of α *on an element, say* 2*, we would write*

$$\alpha(2) = \begin{pmatrix} 1 & \mathbf{2} & 3 & 4 \\ 3 & \mathbf{1} & 4 & 2 \end{pmatrix}(2) = 1$$

Similarly

$$\alpha(1) = \begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ \mathbf{3} & 1 & 4 & 2 \end{pmatrix}(1) = 3$$

Example 226 *The identity permutation on* $A = \{1,2,3,4\}$ *is*

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

in other words, it does not change anything.

6.2 Operations on Permutations

Above we said that S_n was a group under composition. Let us look in more detail at composition of permutations. Composition of permutations written in array notation is performed from right to left, that is the permutation on the right is performed first.

Example 227 *Let* $A = \{1,2,3,4\}$ *and suppose that* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ *and* $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ *then*

1. *We can find how* $\alpha\beta$ *acts on any element.*

$$\begin{aligned} \alpha\beta(1) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}\begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ \mathbf{3} & 2 & 4 & 1 \end{pmatrix}(1) \\ &= \begin{pmatrix} 1 & 2 & \mathbf{3} & 4 \\ 2 & 4 & \mathbf{1} & 3 \end{pmatrix}(3) \\ &= 1 \end{aligned}$$

2. We can also find what permutation $\alpha\beta$ is.

$$\begin{aligned}\alpha\beta &= \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}\\ &= \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}\end{aligned}$$

Example 228 *What is the order of* $\alpha = \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$*?*

We are looking for the smallest positive integer n *such that* $\alpha^n = e$ *remembering that the operation is composition so* α^2 *means* $\alpha\alpha$*.*

$$\begin{aligned}\alpha^2 &= \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\\ &= \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\end{aligned}$$

$$\begin{aligned}\alpha^3 &= \alpha^2\alpha\\ &= \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\\ &= \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\end{aligned}$$

$$\begin{aligned}\alpha^4 &= \alpha^3\alpha\\ &= \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\\ &= \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\\ &= e\end{aligned}$$

So $|\alpha| = 4$

Example 229 *Let's find the elements of* S_3*, the set of all permutations on* $\{1,2,3\}$*. Let* α *be such a permutation . Then, there are* 3 *possibilities for* $\alpha(1)$*. Once* $\alpha(1)$ *is chosen, then there are only* 2 *possibilities for* $\alpha(2)$ *then* 1 *possibility for* $\alpha(3)$*. Thus there are* $3\cdot 2\cdot 1 = 3! = 6$ *possible permutations. They are:*

- *First, we have the identity:*

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

- *Next, with* $1 \to 1$*, we can have* $2 \to 3$*. Let's call it* β*. We have:*

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

- *We have exhausted all the possibilities for* $1 \to 1$*, so we now look at* $1 \to 2$*. We have two choices* $2 \to 3$ *or* $2 \to 1$*. Let's call* α *the one for which* $2 \to 3$*. We have:*

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

- *With* $1 \to 2$*, we can also have* $2 \to 1$*. It turns out the permutation we get is* $\alpha\beta$*. We have:*

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

- *Finally, we look at the permutations for which* $1 \to 3$*. Here again, there are two possibilities.* $2 \to 1$ *and* $2 \to 2$*. It turns out that the permutation for which* $2 \to 1$ *is* α^2*. So, we have:*

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

- *It also turns out that the permutation for which* $2 \to 2$ *is* $\alpha^2\beta$*. So, we have*

$$\alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

- *In conclusion, the* 6 *permutations of* S_3 *are:*

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

  We can see that the distinct elements of S_3 *are* $S_3 = \{e, \alpha, \beta, \alpha^2, \alpha\beta, \alpha^2\beta\}$*. In particular,* $|\alpha| = 3$ *and* $|\beta| = 2$*.*

- *As a final remark, note that* $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *but* $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$*. So* S_3 *is not Abelian.*

Example 230 *Similarly, we can show that the order of* S_n *is* $|S_n| = n!$*. It can be shown that* S_n *is not Abelian for* $n \geq 3$*.*

6.3 Cycle Notation

There is a more compact way to write permutations. This notation is due to Augustin Cauchy. We now present this notation.

Definition 231 *Let $x_1, x_2, ..., x_r$ with $1 \leq r \leq n$ be r distinct elements of $\{1, 2, 3, ..., n\}$. The **r-cycle** $(x_1, x_2, ..., x_r)$ is the element of S_n that maps*

$$x_1 \to x_2 \to x_3 \to ... \to x_r \to x_1$$

In particular, the 1-cycle (x_i) maps $x_i \to x_i$. 1-cycles are usually omitted.

Example 232 *Find $\alpha(1)$, $\alpha(2)$ and $\alpha(4)$ if $\alpha = (1, 4, 3, 2)$.*

- $\alpha(1) = 4$
- $\alpha(2) = 1$
- $\alpha(4) = 3$

The operation on cycles is also composition. They are composed from right to left.

Example 233 *What will 3 be mapped to by $(1, 2)(3)(4, 5)(1, 5, 3)(2, 4)$?*
We proceed from right to left. $(2, 4)$ has no action on 3. $(1, 5, 3)$ maps 3 to 1. So, now we have 1. $(4, 5)$ has no action on 1. (3) has no action on 1. $(1, 2)$ maps 1 to 2. So, the result is $3 \to 2$.

Definition 234 *When two cycles have no elements in common, they are said to be **disjoint**.*

We now illustrate how permutations can be represented by cycles with examples.

Example 235 *The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ can be represented $(1)(2, 4)(3)$ or $(2, 4)$ if we omit the 1-cycles with the understanding that the elements missing are mapped to themselves.*

Remark 236 *The cycle notation is not unique. For example $(2, 4)$ is the same as $(4, 2)$.*

Example 237 *The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$ can be represented by $(1, 2)(3, 4, 6)(5)$ or $(1, 2)(3, 4, 6)$ if we omit the 1-cycle.*

Remark 238 *You will note that $(1, 2)(3, 4, 6)$ is the same as $(3, 4, 6)(1, 2)$. This is a specific case of a more general result we will see and prove below, which states that disjoint cycles commute.*

Example 239 *Write the permutation $(1, 3)(2, 7)(4, 5, 6)(8)$ in array form.*

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

Example 240 *Let* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ *and* $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$. *Write* α *and* β *in cycle notation. Then, write* $\alpha\beta$ *in cycle notation. Finally, write* $\alpha\beta$ *so that the cycles which appear are disjoint.*

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

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

Thus

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

We can see that $\alpha\beta$ *is written as a product of cycles which are not disjoint. We see that* $\alpha\beta(1) = 4$, $\alpha\beta(2) = 5$, $\alpha\beta(3) = 2$, $\alpha\beta(4) = 1$ *and* $\alpha\beta(5) = 3$. *Hence,* $\alpha\beta = (1,4)(2,5,3)$

Example 241 *As noticed above, 1-cycles are usually omitted in a product of cycles with the understanding that they map the omitted element to itself. However, if the permutation is the identity as in* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ *then we have to write something. We can represented by* (1) *or* (2) *or* (i) *for* $i = 1, 2, ..., 5$.

Example 242 *What is the inverse of* $(1,2,3)$*?*
Since the composition of a cycle and its inverse must give the identity, if a cycle maps i *into* j*, then its inverse must map* j *back to* i. *So,* $(1,2,3)^{-1} = (3,2,1)$. *We can verify that* $(1,2,3)(3,2,1) = e$.

Example 243 *Our last example will be the elements of* S_3 *we derived above. We rewrite them in cycle notation.*

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1) = (2) = (3)$$

Recall that we usually omit 1-cycles. However when all the cycles in the permutation are 1-cycles, we do need to write something down.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$$

$$a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,2,3)$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$$

$$\alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$$

We finish this section by stating an obvious result.

Lemma 244 *The order of an r-cycle is r.*
Proof. *See problems.* ■

Example 245 *The order of $\alpha = (1,3,5)$ is 3. Recall that the order is the smallest positive integer n such that $\alpha^n = e$. To get the identity, each element must be mapped to itself. In a cycle, an element is mapped to the one next to it on the right. So, we must compose the cycle until each element is mapped back to itself. So, we must compose the cycle as many times as the cycle has elements.*

We now look at important properties of permutations.

6.4 Properties of Permutations

Theorem 246 *Every permutation of a finite set can be written as a product of disjoint cycles.*
Proof. *Let α be a permutation on $A = \{1,2,...,n\}$. Pick any element of A, say a_1. Compute $a_2 = \alpha(a_1)$, $a_3 = \alpha(a_2) = \alpha^2(a_1)$ and so on. Because A is finite , the sequence $a_1, \alpha(a_1), \alpha^2(a_1), ...$ must also be finite, thus there is a repetition, that is there exist $i < j$ for which $\alpha^i(a_1) = \alpha^j(a_1)$ and hence $a_1 = \alpha^m(a_1)$ with $m = j - i$. So we can write $\alpha = (a_1, a_2, ..., a_m)...$ where the dots indicate we may not have exhausted all the elements of A. If we did not, we pick b_1 among the elements of A which do not appear in $(a_1, a_2, ..., a_m)$ and repeat the same process to get a cycle $(b_1, b_2, ..., b_k)$. First, we note that the two cycles $(a_1, a_2, ..., a_m)$ and $(b_1, b_2, ..., b_k)$ are disjoint. If they had elements in common, then for some i and j we would have $\alpha^i(a_1) = \alpha^j(b_1)$ that is $b_1 = \alpha^{i-j}(a_1)$ but this would imply b_1 is an element of the cycle $(a_1, a_2, ..., a_m)$ which contradicts the way b_1 was chosen. We now have $\alpha = (a_1, a_2, ..., a_m)(b_1, b_2, ..., b_k)...$ where the cycles appearing so far are disjoint and the dots indicate we may not have exhausted all the elements of A. If there are elements of A left, we repeat the procedure. We know this must end since A has a finite number of elements.* ■

We illustrate the technique used in the proof with an example.

Example 247 *Write $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 4 & 2 & 8 & 1 & 6 \end{pmatrix}$ as a product of disjoint cycles.*
We pick an element and apply α to it until we get the element we had picked. If we have not exhausted all the elements, we pick an element not appearing in the cycle we just wrote and repeat the process. We get:

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

Being able to write a permutation as a product of disjoint cycles has several advantages:

- When finding the image of an element, we just need to find the cycle which contains it. If the cycles are disjoint, that element will only appear once.
- Disjoint cycles commute.
- It is easy to find the order of a product of disjoint cycles.

The last two statements are made more precise in the next few theorems.

Theorem 248 *Disjoint cycles commute in other words, if* $\alpha = (a_1, a_2, ..., a_m)$ *and* $\beta = (b_1, b_2, ..., b_n)$ *have no element in common, then* $\alpha\beta = \beta\alpha$.
Proof. *We show* $\alpha\beta = \beta\alpha$ *by showing that* $\alpha\beta(x) = \beta\alpha(x)$ *for every* x *in* A*, the set on which our permutations are defined. We can write* A *as* $A = \{a_1, a_2, ..., a_m, b_1, b_2, ..., b_n, c_1, c_2, ..., c_k\}$ *where the* $c's$ *are the elements of* S *left untouched by* α *and* β*. To prove* $\alpha\beta(x) = \beta\alpha(x)$ *for every* x *in* A *we prove it is true for the* $a's$*, the* $b'a$ *and the* $c's$.

$$\begin{aligned} \alpha\beta(a_i) &= \alpha(\beta(a_i)) \\ &= \alpha(a_i) \text{ since } \beta \text{ leaves the } a's \text{ untouched} \\ &= a_{i+1} \end{aligned}$$

with the understanding that $a_{i+1} = a_1$ *if* $i = m$*. Similarly*

$$\begin{aligned} \beta\alpha(a_i) &= \beta(\alpha(a_i)) \\ &= \beta(a_{i+1}) \\ &= a_{i+1} \text{ since } \beta \text{ leaves the } a's \text{ untouched} \end{aligned}$$

Thus, we see that $\alpha\beta(a_i) = \beta\alpha(a_i)$*. Similarly, we prove that* $\alpha\beta(b_i) = \beta\alpha(b_i)$*. For the* $c's$*, it is even easier. Since both* α *and* β *leave the* $c's$ *untouched, we have*

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

and

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

■

Theorem 249 *The order of a permutation of a finite set written as a product of disjoint cycles is the least common multiple of the length of the cycles.*

Example 250 *The order of* $(1,3,5)(2,4)$ *is* $\operatorname{lcm}(3,2) = 6$.

Example 251 *What is the order of* $(1,2,4)(3,4,5)$*?*
First, we must write it as a product of disjoint cycles.

$$(1,2,4)(3,4,5) = (1,2,4,5,3)$$

Hence, the order is 5*.*

Example 252 *We illustrate the power of this theorem by looking at* S_7*. Though* S_7 *has* $7! = 5040$ *elements, we will use the theorem to quickly find all the possible order the elements of* S_7 *can have. From the theorem, it is enough to consider the possible disjoint cycle structures. Using the notation* $(\underline{n})$ *to denote an n-cycle, the possible disjoint cycles are, writing them from left to right with decreasing length:*

$(\underline{7})$
$(\underline{6})(\underline{1})$
$(\underline{5})(\underline{2})$
$(\underline{5})(\underline{1})(\underline{1})$
$(\underline{4})(\underline{3})$
$(\underline{4})(\underline{2})(\underline{1})$
$(\underline{4})(\underline{1})(\underline{1})(\underline{1})$
$(\underline{3})(\underline{3})(\underline{1})$
$(\underline{3})(\underline{2})(\underline{2})$
$(\underline{3})(\underline{2})(\underline{1})(\underline{1})$
$(\underline{3})(\underline{1})(\underline{1})(\underline{1})(\underline{1})$
$(\underline{2})(\underline{2})(\underline{2})(\underline{1})$
$(\underline{2})(\underline{2})(\underline{1})(\underline{1})(\underline{1})$
$(\underline{2})(\underline{1})(\underline{1})(\underline{1})(\underline{1})(\underline{1})$
$(\underline{1})(\underline{1})(\underline{1})(\underline{1})(\underline{1})(\underline{1})(\underline{1})$

Computing the least common multiple of the various lengths, we see that the possible orders are $7, 6, 10, 5, 12, 4, 3, 2$*.*

Next, we look at 2-cycles. They play an important role and have a special name.

Definition 253 *A 2-cycle is called a* ***transposition****.*

Example 254 $(1,2)$*,* $(1,5)$*,* $(2,4)$ *are examples of transpositions.*

Example 255 *What is the inverse of a transposition?*
A transposition on S_n *is of the form* (a_i, a_j) *It is easy to see that* $(a_i, a_j)(a_i, a_j) = e$*, so every transposition is its own inverse.*

Theorem 256 *Any cycle in S_n with $n > 1$ can be written as the product of transpositions.*
Proof. *A 1-cycle is the identity hence can be written as $(a_i) = (a_i, a_{i+1})(a_{i+1}, a_i)$. For a r-cycle with $r \geq 2$, we have*

$$(a_1, a_2, ..., a_r) = (a_1, a_r)(a_1, a_{r-1}) ... (a_1, a_3)(a_1, a_2)$$

■

Example 257 $(1, 3, 7) = (1, 7)(1, 3)$

Example 258 $(1, 2, 3, 4, 5) = (1, 5)(1, 4)(1, 3)(1, 2)$

Combining the last two theorems, we have:

Theorem 259 *Every permutation in S_n with $n > 2$ can be written as a product of transpositions.*
Proof. *We know that every permutation can be written as a product of disjoint cycles. Then, every cycle can be written as a product of transpositions.* ■

Example 260 $(1, 6, 3, 2)(4, 5, 7) = (1, 2)(1, 3)(1, 6)(4, 7)(4, 5)$

Example 261 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 4 & 2 & 8 & 1 & 6 \end{pmatrix} = (1, 3, 7)(2, 5)(4)(6, 8) = (1, 7)(1, 3)(2, 5)(4, 5)(5, 4)(6$

Every permutation can be written as a product of transpositions. Whether that number is odd or even is important. We investigate this next.

6.5 Even and Odd Permutations

Definition 262 *A permutation is said to be **even** if it can be written as an even number of transpositions. It is said to be odd if it can be written as an **odd** number of transpositions.*

Example 263 *Is $(1, 3, 7)$ even or odd?*
From an example above, $(1, 3, 7) = (1, 7)(1, 3)$ hence it is even.

Example 264 *Is $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 3 & 7 & 5 \end{pmatrix}$ odd or even?*
We decompose α as a product of transpositions by first writing it as a product of disjoint cycles.

$$\begin{aligned} \alpha &= (1, 2, 4)(3, 6, 7, 5) \\ &= (1, 4)(1, 2)(3, 5)(3, 7)(3, 6) \end{aligned}$$

hence α is odd.

Of course, in view of the fact that there are many ways to write a permutation, the reader may wonder if a permutation can be both even and odd. That would not be good. It turns out it cannot happen. Before we prove it, we state a lemma without proof.

Lemma 265 *The identity permutation on S_n is even.*

Theorem 266 *No permutation is both even and odd.*
Proof. *Suppose that α is both even and odd that is $\alpha = \beta_1\beta_2...\beta_l = \gamma_1\gamma_2...\gamma_k$ where k is even and l odd. Since every transposition is its own inverse, this would imply that $e = \beta_1\beta_2...\beta_l\gamma_k\gamma_{k-1}...\gamma_1$. Since $l+k$ is odd, this contradicts the lemma.* ■

The set of even permutations is an important set.

Definition 267 *The set of even permutations in S_n is denoted A_n.*

Theorem 268 *A_n is a subgroup of S_n*
Proof. *See homework.* ■

Definition 269 *A_n is called the alternating group of degree n.*

Theorem 270 *For $n \geq 2$, A_n has order $\frac{n!}{2}$.*
Proof. *We prove that the number of even permutations is the same as the number of odd permutations. Since $|S_n| = n!$, the result will follow. For each odd permutation α in S_n, $(1,2)\alpha$ is even and if $\alpha \neq \beta$ then $(1,2)\alpha \neq (1,2)\beta$. So, there are at least as many even permutations as odd ones. Similarly, we can prove that there are at least as many odd permutations as even ones. Hence there is the same number of both.* ■

6.6 Problems

Do the following problems:

1. Prove that S_n is a group under function composition.
2. Prove that A_n is a subgroup of S_n.
3. Prove that the order of an r-cycle is r.
4. Find a general formula for the inverse of a cycle. Then, prove your formula is the right formula. You may want to try some specific examples first with cycles of various length to get an idea of what is happening.
5. Do # 1, 2, 3, 4, 5, 7, 9, 11, 15, 17, 19, 21 at the end of Chapter 5.