2.2 Supplement to Chapter 2: even and odd permutations

Definition 2.2.1. *The group consisting of all permutations of a set of* n *elements is called the* symmetric group of degree n *and denoted* S_n.

REMARKS

1. The order of S_n is $n!$, the number of permutations of n objects (read this as "n factorial").
2. We often think of the n elements being permuted as the first n positive integers $1, 2, \ldots, n$, but this is not intrinsic to the definition of S_n. It doesn't really matter what these elements are called as long as they have distinct labels.
3. Although the terminology is potentially problematic, it is important not to confuse the term "symmetric group" with groups of symmetries of (for example) regular polygons.

This section is mostly about how to represent permutations and how to do calculations with them. Later in the chapter we will use this information to deduce some nice properties of the symmetric groups.

An element of S_4 is a permutation of the set $\{1, 2, 3, 4\}$; this means a function from that set to itself that sends each element to a different image, and hence shuffles the four elements. In S_4, a basic way to represent the permutation $1 \to 1,\ 2 \to 4,\ 3 \to 2,\ 4 \to 3$ is by the array

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

Representing permutations like this we can practise multiplying (or composing) them. In these notes we will use the convention that for permutations σ and τ, the product $\sigma\tau$ means "σ after τ or $\sigma \circ \tau$, i.e. that the factor that is written on the right is applied first. This is not a universally agreed convention and people use both possible interpretations. For this course it is probably a good idea that we all share the same interpretation to avoid confusion, but in general all that is important is that you state in which order you are considering the composition to take place and that you are consistent.

Example 2.2.2. *In* S_5, *suppose that*

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

Calculate the products $\sigma\tau$ *and* $\tau\sigma$.

Solution: To calculate $\sigma\tau$, we apply τ first and then σ. Remember that this is just a composition of functions.

- τ sends 1 to 4, then σ sends 4 to 4. So $\sigma\tau$ sends 1 to 4.
- τ sends 2 to 2, then σ sends 2 to 3. So $\sigma\tau$ sends 2 to 3.
- τ sends 3 to 3, then σ sends 3 to 5. So $\sigma\tau$ sends 3 to 5.
- τ sends 4 to 5, then σ sends 5 to 1. So $\sigma\tau$ sends 4 to 1.
- τ sends 5 to 1, then σ sends 1 to 2. So $\sigma\tau$ sends 5 to 2.

We conclude that

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

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

This array format is not the only way of representing a permutation and not always the most useful way. Another way of thinking about a permutation π is by thinking about how it moves the elements of the set around, by starting with a single element and looking at the sequence of images when you repeatedly apply π to it. Eventually you will have to get back to the original element. Consider the following example in S_{14}.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 9 & 8 & 2 & 5 & 1 & 12 & 14 & 6 & 7 & 3 & 13 & 10 & 4 \end{pmatrix}$$

Start with the element 1 and look at what happens to it when you repeatedly apply π.

- First you get $1 \to 11$;
- Then $11 \to 3$;
- Then $3 \to 8$;
- Then $8 \to 14$;
- Then $14 \to 4$;
- Then $4 \to 2$;
- Then $2 \to 9$;
- Then $9 \to 6$;
- Then $6 \to 1$.

After nine applications of π we arrive back at 1 and this is the first time we have a repetition in the list. This will happen every time: the list can't continue indefinitely without repetition because there are only finitely many elements being permuted. Suppose that after starting at 1 the first repetition occurs at Step k, after k applications of π. Then we have

$$1 \to a_1 \to a_2 \to \cdots \to a_{k-1} \to$$

where $1, a_1, \ldots, a_{k-1}$ are distinct. The next element (a_k) is a repeat of one of these. However it can't be a repeat of a_1, because 1 is the only element whose image under π is a_1, and $a_{k-1} \neq 1$. The same applies to $a_2, \ldots, a_{k-1}$. So it must be that 1 (the element where we started) is the first element to be repeated, and that we close the circle that started with 1. In our example above there were nine distinct elements in the sequence that started at 1. So the permutation π produces the following *cycle*:

$$1 \to 11 \to 3 \to 8 \to 14 \to 4 \to 2 \to 9 \to 6 \to 1$$

This cycle is often written using the following notation:

$$(1\ 11\ 3\ 8\ 14\ 4\ 2\ 9\ 6).$$

Note that 1 is not written at the end here. The above notation means the permutation (of 14 elements in this case) that sends 1 to 11, 11 to 3, etc, and sends 6 back to 1. There is nothing in the notation to indicate that we are talking about an element of S_{14} - this has to be clear from the context. Also, it is understood that elements that are not mentioned in the above notation are fixed by the permutation that it denotes. The permutation $(1\ 11\ 3\ 8\ 14\ 4\ 2\ 9\ 6)$ is an example of a *cycle of length 9* in S_{14}. It is not the same as the permutation π that we started with, but it does coincide with π on the set of nine elements that can be obtained by starting at 1 and repeatedly applying π. This set is called the *orbit* of 1 under π.

The point of this discussion is that π can be written as a product (or composition) of *disjoint* cycles in S_{14}. The next step towards doing so is to look for the first element (in the natural order)

of our set that is not involved in the first cycle. This is 5. Go back to π and see what happens to 5 under repeated application of π. We find that

$$5 \to 5,$$

so 5 is fixed by π. We could think of this as a cycle of length 1.

There are still some elements unaccounted for. The first one is 7. Looking at the orbit of 7 under π, we find

$$7 \to 12 \to 13 \to 10 \to 7$$

so we get the cycle $(7\ \ 12\ \ 13\ \ 10)$ of length 4. Note that this has no intersection with the previous cycles.

Our conclusion is that π can be written as the product of these disjoint cycles:

$$\pi = (1\ \ 11\ \ 3\ \ 8\ \ 14\ \ 4\ \ 2\ \ 9\ \ 6)(7\ \ 12\ \ 13\ \ 10).$$

If you like you can explicitly include (5) as a third factor, but the usual convention is not to bother including elements that are fixed in expressions of this nature, if an element does not appear it is understood to be fixed.

Notes

1. The representation of π in "array" format can easily be read from its representation as a product of disjoint cycles. For example if you want to know the image of 8 under π, just look at the cycle where 8 appears - its image under π is the next element that appears after it in that cycle, 14 in this example. If your element is written at the end of a cycle, like 10 in this example, then its image under π is the number that is written in the first position of that same cycle (so $10 \to 7$ here). An element that does not appear in any of the cycles is fixed by the permutation.

2. The statement above says that π can be effected by first applying the cycle $(7\ \ 12\ \ 13\ \ 10)$ (which only moves the elements $7, 12, 13, 10$) and then applying the cycle $(1\ 11\ 3\ 8\ 14\ 4\ 2\ 9\ 6)$ (which only moves the elements $1, 11, 3, 8, 14, 4, 2, 9, 6$). Since these two cycles operate on disjoint sets of elements and do not interfere with each other, they commute with each other under composition - it does not matter which is written first in the expression for π as a product of the two of them. So we could equally well write

$$\pi = (7\ \ 12\ \ 13\ \ 10)(1\ \ 11\ \ 3\ \ 8\ \ 14\ \ 4\ \ 2\ \ 9\ \ 6).$$

3. The expression for a permutation as a product of disjoint cycles is unique up to the order in which the cycles are written. This means that the same cycles must appear in any such expression for a given permutation, but they can be written in different orders.

   It might also be worth mentioning that a given cycle can be written in slightly different ways, since it doesn't matter which element is taken as the "starting point". For example $(7\ \ 12\ \ 13\ \ 10)$ and $(13\ \ 10\ \ 7\ \ 12)$ represent the same cycle.

Definition 2.2.3. *The expression of an element of S_n as a product of disjoint cycles partitions the set $\{1, 2, \ldots, n\}$ into disjoint* orbits. *In the above example there are three orbits:*

$$\{1, 2, 3, 4, 6, 8, 9, 11, 14\},\ \{5\},\ \{7, 10, 12, 13\}.$$

If two elements belong to the same orbit for a permutation π, it means that some power of π takes one of those elements to the other. Note that fixed points *do* count as orbits. So the identity element of S_n has n orbits each consisting of a single element. A permutation in S_n has just one orbit if it is a single cycle involving all n elements.

It is good idea to practise moving between the "array representation" and "disjoint cycle representation" of a permutation. There is another way of representing permutations that is sometimes

useful. We could think of the "simplest" type of non-identity permutation as being one that just swaps two elements and leaves the rest fixed. Such a permutation is called a transposition. The transposition that (for example) interchanges 1 and 2 and leaves all the other elements fixed is denoted, in typical cycle notation, as $(1\ 2)$.

Theorem 2.2.4. *Every element of S_n can be expressed as a product of transpositions.*

Rather than giving a formal general proof of Theorem 2.2.4, we will look at a way of expressing a given permutation as a product of transpositions. This contains all that would be required for a fully detailed proof, without having to worry about setting up cumbersome general notation.

Example 2.2.5. *In S_8 (for example), the cycle $(2\ 4\ 7\ 6\ 8)$ can be written as the product*

$$(2\ 8)(2\ 6)(2\ 7)(2\ 4)$$

of four transpositions.
To see this, just look at what happens to each element under the proposed composition of transpositions. Start with 2. We have:

$$2 \to 4.$$

Move on to 4:

$$4 \to 2 \to 7.$$

Then 7:

$$7 \to 2 \to 6.$$

Then 6:

$$6 \to 2 \to 8.$$

Finally 8:

$$8 \to 2.$$

So overall our composition of transpositions amounts to the cycle

$$2 \to 4 \to 7 \to 6 \to 8 \to 2,$$

as we wanted.

Note: The expression for a given cycle (or permutation) as a product of transpositions is *not unique*. For example we could write the 4-cycle above equally well as $(4\ 7\ 6\ 8\ 2)$, then using the same technique to write it as a product of transpositions would result in

$$(4\ 2)(4\ 8)(4\ 6)(4\ 7),$$

which does not involve the same transpositions as our example above, although it is the same permutation.

Example 2.2.6. *In S_{12}, write the element*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 4 & 6 & 1 & 10 & 7 & 8 & 12 & 9 & 3 & 2 & 5 \end{pmatrix}$$

as a product of transpositions.

Solution: First write it as a product of disjoint cycles.

$$(1\ 11\ 2\ 4)(3\ 6\ 7\ 8\ 12\ 5\ 10).$$

Then as a product of transpositions:

$$(1\ 4)(1\ 2)(1\ 11)(3\ 10)(3\ 5)(3\ 12)(3\ 8)(3\ 7)(3\ 6).$$

This expression involves nine transpositions.

Exercise 2.2.7. *How many of the* $n!$ *elements of* S_n *are transpositions? How many are* 3*-cycles? (i.e. cycles of length 3, like* $(1\ 2\ 3)$*).*

The number of transpositions involved in an expression for a permutation as a product of transpositions is not uniquely determined either, since for example $(2\ 3)$ and $(1\ 3)(2\ 3)(1\ 2)$ are the same permutation (check this). However, it *is* true that no permutation can be written both as the product of an even number and an odd number of permutations. To prove this is not difficult but involves a bit of fussing. This is our next task.

Theorem 2.2.8. *A permutation in* S_n *cannot be expressed both as the product of an even number and an odd number of transpositions.*

Proof. Let $\pi \in S_n$, and suppose that π can be written as a product of s transpositions, i.e.

$$\pi = \tau_s \tau_{s-1} \dots \tau_2 \tau_1,$$

where each τ_i is a transposition. Let r be the number of orbits of π (i.e. the number of cycles in the expression for π as a product of disjoint cycles, including fixed points). Then r is fully determined by π and so is $n - r$ (this means that the numbers r and $n - r$ do not depend on any choice about how π is represented). We will show that the numbers s and $n - r$ are either both even or both odd.

We will do this by induction on s, the starting point being $s = 0$. If $s = 0$ then π is the identity permutation, $r = n$ and $n - r = 0$. So in this case s and $n - r$ are both zero, they are both even.

The case $s = 1$ is also manageable. If $s = 1$, then π is a single transposition, so it has one cycle of length 2 and $n - 2$ fixed points. In this case $r = n - 1$ and $n - r = 1$, so s and $n - r$ are both equal to 1, they are both odd.

Now suppose that s and $n-r$ have the same parity for all values of s up to $s = k$, and consider the case $s = k + 1$. This means

$$\pi = \tau_{k+1} \tau_k \dots \tau_2 \tau_1,$$

where each τ_i is a transposition. Let $\tau_{k+1} = (1\ 2)$ (there is no loss of generality here since we can relabel the elements that are being permuted if necessary), let π' be the element of S_n given by

$$\pi' = \tau_k \dots \tau_2 \tau_1,$$

and let r' be the number of orbits of π'. We will show that the number r of orbits of π differs from r' by 1.

Case 1: Suppose first that 1 and 2 belong to the same orbit in π', and write the cycle corresponding to this orbit as $(1\ a_2 \dots a_l\ 2\ a_{l+m} \dots a_m)$. Then we have (check this)

$$(1\ 2)(1\ a_1 \dots\ a_l\ 2\ a_{l+1} \dots a_m) = (1\ a_1 \dots a_1)(2\ a_{l+1} \dots a_m).$$

So the orbit of π' that contained the elements 1 and 2 is split into two separate orbits by the multiplication by τ_{k+1}. Other orbits of π' are unaffected since they do not involve 1 or 2. So in the case where 1 and 2 belong to the same orbit of π', we have $r = r' + 1$.

Case 2: Suppose that 1 and 2 belong to different orbits of π', and write the cycles corresponding to these orbits as

$$(1\ a_1 \dots a_l),\ \ (2\ b_1 \dots b_m)$$

where none of the a_i is equal to any of the b_j. Then (check that)

$$(1\ 2)(1\ a_1 \dots a_l)(2\ b_1 \dots b_m) = (1\ a_1 \dots a_l\ 2\ b_1 \dots b_m),$$

so the effect of the multiplication by $(1\ 2)$ is to combine these two orbits into one. As in Case 1 there is no effect on the other orbits of π'. So in the case where 1 and 2 belong to different orbits of π', we have $r = r' - 1$.

By our induction hypothesis, $n-r'$ has the same parity as k. The above argument above shows that $n - r$ differs from $n - r'$ by 1, and hence it must have the same parity as $k + 1$ which is the number of transpositions in π.

We have proved that the parity (oddness or evenness) of the number of transpositions in any expression for π as a product of transpositions is the same as the parity of $n - r$. In particular, for a given π, this number of transpositions is always even or always odd. □

Definition 2.2.9. *An element of S_n is called* even *if it can be written as the product of an even number of transpositions, and* odd *if it can be written as the product of an odd number of transpositions. Every element of S_n is either even or odd (not both).*

Note that the inverse of an even permutation is again even (it involves the same transpositions listed in the opposite order), and that the product of two even permutations is even. Moreover, the identity permutation is even, since it can be written as the "product of zero transpositions" or as the square of any transposition. Thus the set of *even permutations* of n objects is a subgroup of S_n. This is known as the *alternating group* of degree n and denoted by A_n. Directly counting the even permutations of a set of n elements is a more difficult task than counting *all* the permutations. However, by showing that the even permutations can be put in one-to-one correspondence with the odd permutations, we can show that exactly half of all the elements of S_n are even.

Theorem 2.2.10. *The order of the alternating group A_n is $\frac{n!}{2}$.*

Proof. Let the numbers of even and odd permutations in S_n be k_1 and k_2 respectively, and let τ denote the transposition $(1\ 2)$. For every even permutation π, we have a corresponding odd permutation $\pi\tau$. Thus there are at least as many odd permutations as even permutations, $k_1 \leqslant k_2$.

On the other hand, for every *odd* permutation σ we have the corresponding *even* permutation $\sigma\tau$. So there are at least as many even permutations as odd permutations, $k_2 \leqslant k_1$.

It follows that $k_1 = k_2$ and hence that the even permutations and odd permutations each account for half of all permutations. Thus

$$|A_n| = \frac{n!}{2}.$$

□