Section 11

Permutations

Definition 11.1 Let X be a non-empty set. A bijective function $f\colon X \to X$ will be called a *permutation* of X.

Consider the case when X is the finite set with n elements:

$$X = \{1, 2, \dots, n\}.$$

The collection of all permutations of this set X will be called the *symmetric group* on n symbols and is denoted by S_n.

(We shall meet the definition of the term *group* in the next section.)

Observation: S_n contains $n!$ permutations.

This holds since we have n choices for the image of 1, then $n-1$ choices for the image of 2, etc. We conclude that

$$|S_n| = n(n-1)(n-2)\dots 2 \cdot 1 = n!.$$

If f is a permutation of the set X, we shall write xf for the image of the element $x \in X$ under f (rather than $f(x)$). The principal reason for doing this is that it makes composition of permutations much easier: fg will mean apply f first and then apply g rather than the other way around.

If $f \in S_n$, then we denote it as follows:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1f & 2f & 3f & \dots & nf \end{pmatrix}$$

In this two-row notation, we write the image of an element k in the second row below the occurrence of k in the first row. Thus

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

denotes the permutation of $\{1, 2, 3, 4\}$ which maps 1 to 2, 2 to 4, 3 to 1 and finally 4 to 3.

Note that as f is a bijective function, all n of the elements in $X = \{1, 2, \ldots, n\}$ must occur in the second row. It is for this reason that such functions are termed "permutations": one can think of them as simply re-ordering the elements in X.

The composite of two permutations f and g is the function obtained by applying f first and then applying g. Since we are writing maps on the right, we denote this by fg. It is easy to calculate the permutation obtained by composing two permutations written in the above two-row notation:

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

Here $1 \mapsto 2$ by the first permutation and then $2 \mapsto 2$ by the second. Thus the composite does the first then the second, so $1 \mapsto 2$. Equally the composite has the following effects:

$$2 \mapsto 4 \mapsto 1, \quad 3 \mapsto 1 \mapsto 3, \quad 4 \mapsto 3 \mapsto 4$$

Hence

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

Similarly

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

(Since $1 \mapsto 3 \mapsto 1$, $2 \mapsto 2 \mapsto 4$, $3 \mapsto 4 \mapsto 3$ and $4 \mapsto 1 \mapsto 2$.) Note this already illustrates one phenomenon: in general,

$$fg \neq gf$$

for two permutations f and g.

Cycle Notation

The above two-row notation is quite inefficient and also difficult to understand the permutations in great detail. For example, the permutation

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

fixes both 1 and 3, while swaps round 2 and 4. It would be nice to have a more efficient way to describe this element (ideally one which misses out 1 and 3 since they are not moved by the permutation).

Definition 11.2 Let x_1, x_2, $\ldots$, x_r be r distinct elements of $\{1, 2, \ldots, n\}$ (so $1 \leqslant r \leqslant n$). The *$r$-cycle* $(x_1\, x_2 \ldots x_r)$ is the permutation in S_n which maps

$$x_1 \mapsto x_2, \quad x_2 \mapsto x_3, \quad \ldots, \quad x_{r-1} \mapsto x_r, \quad x_r \mapsto x_1$$

and fixes all other points in $\{1, 2, \ldots, n\}$.

Such a cycle may be described by drawing the points x_i in a circular picture. Thus the cycle could also be written as

$$(x_2\, x_3 \ldots x_r\, x_1), \quad \text{or} \quad (x_3\, x_4 \ldots x_r\, x_1\, x_2), \quad \text{etc.}$$

For example, the above permutation

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

could be written more simply as

$$(2\,4) \qquad \text{or} \qquad (4\,2).$$

This tells us that this permutation fixes both 1 and 3.

What about the identity permutation? This is the permutation

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

This is often written as the cycle (1). (Such a cycle fixes all elements except 1 and moves 1 to 1: so it really is the identity.) Of course, it could also be written (x) for any $x \in \{1, 2, \ldots, n\}$, but to avoid confusion its probably best to stick to $x = 1$.

Definition 11.3 Two cycles $(x_1\, x_2 \ldots x_r)$ and $(y_1\, y_2 \ldots y_s)$ in S_n are *disjoint* if no element in $\{1, 2, \ldots, n\}$ is moved by both cycles.

If these cycles are non-identity (i.e., if $r \geqslant 2$ and $s \geqslant 2$) then this condition can be expressed as

$$\{x_1, x_2, \ldots, x_r\} \cap \{y_1, y_2, \ldots, y_s\} = \varnothing.$$

The crucial observation that will enable us to make use of cycles is the following:

Theorem 11.4 *Every permutation (of n points) can be written as a product of disjoint cycles.*

The proof is omitted. A proof is not too hard, but it is more helpful to give an example to illustrate and this should be fairly convincing of the truth of the theorem.

Example 11.5

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

To calculate this one starts with 1, follow the images round until we get back to 1. Then we start again with the next symbol not accounted for.

It should be reasonably clear that we can follow this process with any permutation and consequently the truth of the above theorem is assured (if not proved in careful detail).

Example 11.6

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

We can use the same method used to calculate the composite of two permutations when these permutations are expressed as products of cycles:

Example 11.7 $(4\,5\,3) \circ (1\,2\,3\,4\,5) = (1\,2\,3\,5\,4)$
[Can be done by following images.]

Definition 11.8 We say two permutations f and g *commute* if $fg = gf$.

We have noticed that we cannot expect two permutations commute. Of course, a permutation f always commutes with itself. The following is easy to establish:

Lemma 11.9 *Disjoint cycles commute.*

(This may simply be described: the effect of a product of disjoint cycles is the same no matter which was around it is calculated.)

This has the consequence that

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

etc. Note that $(2\,5)$ commutes with this permutation:

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

since disjoint cycles commute. Similar calculations can be done for other examples.

Definition 11.10 The *order* of a permutation f is the smallest positive integer m such that f^m is the identity.

The idea here is that the order of f is the number of permutations we can produce by taking powers of f. Once we have reached the identity, any further powers just produce ones we already have calculated.

How do we calculate the order of f? One method is just to calculate powers (f, f^2, f^3, ...) and wait until we hit the identity. The problem is that this can be laborious. Instead we can exploit the way we can write permutations as products of disjoint cycles.

First consider a cycle $f = (x_1\, x_2 \ldots x_r)$. Note that powers of f first map x_1 to x_2, then to x_3, then to x_4, and so on. Hence to produce the identity, we need to use f^r. (So the order of an r-cycle is r.)

Now consider any permutation f and write it as a product of disjoint cycles:

$$f = f_1 f_2 \ldots f_s.$$

Since disjoint cycles commute, we find

$$f^m = f_1^m f_2^m \ldots f_s^m.$$

To obtain the identity we therefore need to take the m which makes the power of each cycle the identity. We thus have:

Theorem 11.11 *The order of a permutation is equal to the lowest common multiple of the lengths of the cycles occurring in its decomposition into disjoint cycles.*

Example 11.12 Take

$$\begin{aligned} f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 7 & 9 & 5 & 10 & 8 & 1 & 2 & 6 \end{pmatrix} \\ &= (1\ 3\ 7\ 8)(2\ 4\ 9)(6\ 10). \end{aligned}$$

We need fourth powers to make the first cycle the identity, cubes to make the second cycle the identity, and squares for the final cycle. Thus the order of σ is $4 \times 3 = 12$.

We give a special name to the following very short cycles.

Definition 11.13 A 2-cycle (that is, a cycle of length 2) is also called a *transposition.*

Thus a transposition is a permutation $(x\, y)$ which simply swaps round the two elements x and y. Transpositions are useful for the following reason:

Theorem 11.14 *Every permutation can be expressed as a product of transpositions.*

PROOF: We can express every permutation as a product of disjoint cycles. The next step is to express any cycle as a product of transpositions. For example,

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

does what we want for a 5-cycle. Analogous calculations establish the same for other lengths. □

The final thing we can do with permutations is *invert* them:

Definition 11.15 If f is a permutation of the set X, then the *inverse* f^{-1} of f is the permutation that undoes the effect of applying f; i.e., if $f\colon x \mapsto y$, then $f^{-1}\colon y \mapsto x$.

Calculating Inverses, Method 1: If f is written in two-row notation, then interchanging the rows produces its inverse:

e.g., if

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

then

$$\begin{aligned} f^{-1} &= \begin{pmatrix} 2 & 4 & 3 & 5 & 1 & 6 & 8 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 3 & 2 & 4 & 6 & 8 & 7 \end{pmatrix}. \end{aligned}$$

Calculating Inverses, Method 2: If g is a cycle, say $g = (x_1\,x_2\ldots x_r)$, so

$$g\colon x_1 \mapsto x_2, \quad x_2 \mapsto x_3, \quad \ldots, \quad x_{r-1} \mapsto x_r, \quad x_r \mapsto x_1,$$

then

$$g^{-1}\colon x_r \mapsto x_{r-1}, \quad x_{r-1} \mapsto x_{r-2}, \quad \ldots, \quad x_2 \mapsto x_1, \quad x_1 \mapsto x_r.$$

That is,

$$g^{-1} = (x_r\,x_{r-1}\ldots x_2\,x_1),$$

i.e., we write the cycle for g backwards.

Hence for $f = (1\,2\,4\,5)(7\,8)$, we have

$$\begin{aligned} f^{-1} &= (5\,4\,2\,1)(8\,7) \\ &= (1\,5\,4\,2)(7\,8). \end{aligned}$$

(Note this agrees with the answer obtained by Method 1!)