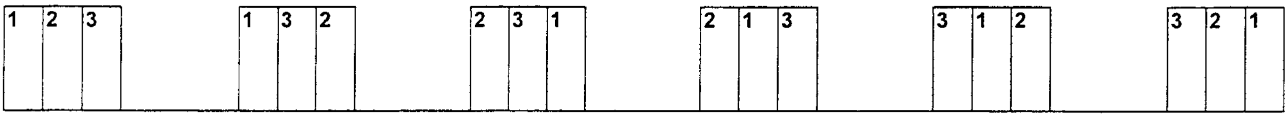
4 Permutations

4.1 Permutation Notation

We may have met permutations as 'rearrangements', for example:- how many ways can we arrange 3 books on a shelf. The answer is of course 6.



However in the context of operations involving permutations, what matters is not where each book lies after shuffling **but** what it is replaced by.

So if our 3 books started in positions 1, 2 and 3 and were rearranged to 2, 1 and 3, what is important is that 2 replaces 1, not that 2 is in the left hand position.

The notation we adopt for a permutation is $\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$, where the top row gives the initial state of the objects and the bottom row tells us what they are replaced by.

So $\begin{pmatrix}3 & 1 & 2\\ 3 & 2 & 1\end{pmatrix}$ is exactly the **same** permutation as $\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$ since the same replacements are taking place. In fact there are six ways of writing this one permutation. In general we will write permutations with numbers on the top row in ascending order.

Thus the six permutations of our three books can be written as:

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

4.2 Combining Permutations.

There is a perfectly natural way of combining permutations which gives rise to a binary operation which we will refer to as composition of permutations. We just apply one after the other.

For example: $p = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$, followed by $r = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$

p			r			combined effect of pr		
1	is replaced by	2	2	is replaced by	2	1	is replaced by	2
2		3	3		1	2		1
3		1	1		3	3		3

So we have $pr = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

However $rp = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq pr$

So combining permutations is not a commutative operation.

Exercise 4.2

In questions 1 to 4 use these permutations:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ r = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ t = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

1. Find a) ps b) pt c) pq d) qe e) et f) r^2 g) st
2. Show that $p(st) = (ps)t$
3. Which of the above elements behaves like an identity?
4. What is the inverse for p?
5. Given $e = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, x = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}, y = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}, z = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$
   - i) Find a) xy, b) yz, c) xz, d) x^2, e) ex, f) xe
   - ii) Complete a structure table for the set of permutations $\{ e, x, y, z\}$ with the binary operation composition of permutations.
   - iii) Check to see if your table demonstrates the three group axioms of closure, identity and inverse

Exercise 4.2, no 5 should be making you think that perhaps certain sets of permuations do form groups. In our exercise 5 we had a set which contained only 4 elements, had we considered all the permutations of a, b, c, d we would have been looking at a total of 24 (= 4x3x2x1 = 4!) permutations. So in number 5 above we were considering just a subset of all the possible permutations of 4 objects.

If we had permuations of 5 objects, we would be looking at a total of 5! = 120 different permuations.

It is possible to establish that when we consider the set of all the permutations for some set of objects A, together with the binary operation composition, we do in fact have a group.

The simplest way of doing this is to regard each permutation of A as a function from A to A. This function is 1-1 and onto.

4.3 Permutation Groups

You should have previously studied functions and be familiar with concepts of 1-1 and onto, together with an understanding of composite functions and inverse functions.

4.3.1 Function Notation in Algebra

The usual notation for functions is to write $f(x)$ for function f applied to x and $fg(x)$ for a composite function. This would mean the application of g first followed by f.
In algebra we use a different notation where we read from left to right. Suppose p and q are functions applied to set A and a is an element of A.
Then ap is the result of applying function p to a.
and apq is the result of applying the composite function pq to a; where the application of p is followed by the application of q.
This notation fits in with our definition of composition of permutations.

Theorem 4.3.2

Let A be a non empty set, and let S_A be the set of all permutations of A. Then S_A is a group under the binary operation composition of permutations.

Proof

Associativity
For each $a \in A$ and p, q and $r \in S_A$,
we require that $a[(pq)r] = a[p(qr)]$, ie a is mapped to the same image.

$$a[(pq)r] = [a(pq)]r = [(ap)q]r = (ap)(qr) = a[p(qr)]$$

So composition of functions is associative.

Identity
The permutation e is such that $ae = a$ for all $a \in A$. ie e is the permutation that leaves all elements unchanged.
Let p map a to a' ie $ap = a'$
Then $a(pe) = (ap)e = a'e = a' = ap$ and $a(ep) = (ae)p = ap$ So $pe = ep = p$
Hence S_A has an identity element

Inverse
Let p map a to a' ie $ap = a'$ and let p^{-1} reverse this mapping so $a'p^{-1} = a$
Then $a(pp^{-1}) = (ap)p^{-1} = a'p^{-1} = a = ae$ and $a'(p^{-1}p) = (a'p^{-1})p = ap = a' = a'e$
So $pp^{-1} = e$ and $p^{-1}p = e$ Hence each permutation has an inverse.

If p and q are permutations then they are 1-1 and onto functions. Then the composite function pq is also 1-1 and onto. So we have closure.
Hence S_A is a group under the composition of permutations.

This gives rise to a very important set of groups in group theory. These groups are called symmetric groups.
The symmetric group S_n is the group of all permutations of n objects with composition of permutations.

$$S_1 = \{\begin{pmatrix}1\\1\end{pmatrix}\} \qquad S_2 = \{\begin{pmatrix}1 & 2\\1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}\}$$

$$S_3 = \{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}\}$$

Groups S_1 and S_2 are rarely considered as they trivial groups. S_3 which is all the permutations of 3 objects contains $3! = 3 \times 2 \times 1 = 6$ elements. Similarly S_4 has $4! = 24$ elements.