CHAPTER I.

ON PERMUTATIONS.

1. AMONG the various notations used in the following pages, there is one of such frequent recurrence that a certain readiness in its use is very desirable in dealing with the subject of this treatise. We therefore propose to devote a preliminary chapter to explaining it in some detail.

2. Let $a_1, a_2, \ldots, a_n$ be a set of n distinct letters. The operation of replacing each letter of the set by another, which may be the same letter or a different one, when carried out under the condition that no two distinct letters are replaced by one and the same letter, is called a *permutation* performed on the n letters. Such a permutation will change any given arrangement

$$a_1, a_2, \ldots, a_n$$

of the n letters into a definite new arrangement

$$b_1, b_2, \ldots, b_n$$

of the same n letters.

3. One obvious form in which to write the permutation is

$$\begin{pmatrix} a_1, & a_2, \ldots\ldots, & a_n \\ b_1, & b_2, \ldots\ldots, & b_n \end{pmatrix},$$

thereby indicating that each letter in the upper line is to be replaced by the letter standing under it in the lower. The disadvantage of this form is its unnecessary complexity, each of the n letters occurring twice in the expression for the permutation; by the following process, the expression of the permutation may be materially simplified.

Let p be any one of the n letters, and q the letter in the lower line standing under p in the upper. Suppose now that r is the letter in the lower line that stands under q in the upper, and so on. Since the number of letters is finite, we must arrive at last at a letter s in the upper line under which p stands. If the set of n letters is not thus exhausted, take any letter p' in the upper line, which has not yet occurred, and let $q', r', \ldots$ follow it as $q, r, \ldots$ followed p, till we arrive at s' in the upper line with p' standing under it. If the set of n letters is still not exhausted, repeat the process, starting with a letter p'' which has not yet occurred. Since the number of letters is finite, we must in this way at last exhaust them; and the n letters are thus distributed into a number of sets

$$p,\ q,\ r, \ldots,\ s;$$
$$p',\ q',\ r', \ldots,\ s';$$
$$p'',\ q'',\ r'', \ldots,\ s'';$$
$$\ldots\ldots\ldots\ldots;$$

such that the permutation replaces each letter of a set by the one following it in that set, the last letter of each set being replaced by the first of the same set.

If now we represent by the symbol

$$(pqr \ldots s)$$

the operation of replacing p by q, q by $r, \ldots$, and s by p, the permutation will be completely represented by the symbol

$$(pqr \ldots s)\,(p'q'r' \ldots s')\,(p''q''r'' \ldots s'')\ldots\ldots.$$

The advantage of this mode of expressing the permutation is that each of the letters occurs only once in the symbol.

4. The separate components of the above symbol, such as $(pqr \ldots s)$, are called the *cycles* of the permutation. In particular cases, one or more of the cycles may contain a single letter; when this happens, the letters so occurring singly are unaltered by the permutation. The brackets enclosing single letters may clearly be omitted without risk of ambiguity, as also may the unaltered letters themselves. Thus the permutation

$$\begin{pmatrix} a, & b, & c, & d, & e \\ c, & b, & d, & a, & e \end{pmatrix}$$

may be written $(acd)(b)(e)$, or $(acd)\,be$, or simply (acd). If for any reason it were desirable to indicate that permutations of the five letters a, b, c, d, e were under consideration, the second of these three forms would be used.

5. The form thus obtained for a permutation is not unique. The symbol $(qr\ldots sp)$ clearly represents the same permutation as $(pqr\ldots s)$, if the letters that occur between r and s in the two symbols are the same and occur in the same sequence; so that, as regards the letters inside the bracket, any one may be chosen to stand first so long as the cyclical order is preserved unchanged.

Moreover the order in which the brackets are arranged is clearly immaterial, since the operation denoted by any one bracket has no effect on the letters contained in the other brackets. This latter property is characteristic of the particular expression that has been obtained for a permutation; it depends upon the fact that the expression contains each of the letters once only.

6. When we proceed to consider the effect of performing two or more permutations successively, it is seen at once that the order in which the permutations are carried out in general affects the result. Thus to give a very simple instance, the permutation (ab) followed by (ac) changes a into b, since b is unaltered by the second permutation. Again, (ab) changes b into a and (ac) changes a into c, so that the two permutations performed successively change b into c. Lastly, (ab) does not affect c and (ac) changes c into a. Hence the two permutations performed successively change a into b, b into c, c into a, and affect no other symbols. The result of the two permutations performed successively is therefore equivalent to the permutation (abc); and it may be similarly shewn that (ac) followed by (ab) gives (acb) as the resulting permutation. To avoid ambiguity it is therefore necessary to assign, once for all, the meaning to be attached to such a symbol as $s_1 s_2$, where s_1 and s_2 are the symbols of two given permutations. We shall always understand by the symbol $s_1 s_2$ *the result of carrying out first the*

permutation s_1 and then the permutation s_2. Thus the two simple examples given above may be expressed in the form

$$(ab)\,(ac) = (abc),$$
$$(ac)\,(ab) = (acb),$$

the sign of equality being used to represent that the permutations are equivalent to each other.

If now

$$s_1 s_2 = s_4 \quad \text{and} \quad s_2 s_3 = s_5,$$

the symbol $s_1 s_2 s_3$ may be regarded as the permutation s_4 followed by s_3 or as s_1 followed by s_5. But if s_1 changes *any* letter a into b, while s_2 changes b into c and s_3 changes c into d, then s_4 changes a into c and s_5 changes b into d. Hence $s_4 s_3$ and $s_1 s_5$ both change a into d; and therefore, a being any letter operated upon by the permutations,

$$s_4 s_3 = s_1 s_5.$$

Hence the meaning of the symbol $s_1 s_2 s_3$ is definite; it depends only on the component permutations s_1, s_2, s_3 and their sequence, and it is independent of the way in which they are associated when their sequence is assigned. And the same clearly holds for the symbols representing the successive performance of any number of permutations. To avoid circumlocution, it is convenient to speak of the permutation $s_1 s_2 \ldots s_n$ as the *product* of the permutations s_1, $s_2, \ldots$, s_n in the sequence given. The product of a number of permutations, thus defined, always obeys the associative law but does not in general obey the commutative law of algebraical multiplication.

7. The permutation which replaces every symbol by itself is called the *identical permutation.* The *inverse* of a given permutation is that permutation which, when performed after the given permutation, gives as result the identical permutation. Let s_{-1} be the permutation inverse to s, so that, if

$$s = \begin{pmatrix} a_1, & a_2, \ldots, & a_n \\ b_1, & b_2, \ldots, & b_n \end{pmatrix},$$

then

$$s_{-1} = \begin{pmatrix} b_1, & b_2, \ldots, & b_n \\ a_1, & a_2, \ldots, & a_n \end{pmatrix}.$$

Let s_0 denote the identical permutation which can be represented by

$$\begin{pmatrix} a_1, a_2, \ldots, a_n \\ a_1, a_2, \ldots, a_n \end{pmatrix}.$$

Then $$ss_{-1} = s_0 \text{ and } s_{-1}s = s_0,$$

so that s is the permutation inverse to s_{-1}.

Now if $$ts = t's,$$

then $$tss_{-1} = t'ss_{-1},$$

or $$ts_0 = t's_0.$$

But ts_0 is the same permutation as t, since s_0 produces no change; and therefore

$$t = t'.$$

In exactly the same way, it may be shewn that the relation

$$st = st'$$

involves $$t = t'.$$

8. The result of performing r times in succession the same permutation s is represented symbolically by s^r. Since, as has been seen, products of permutations obey the associative law of multiplication, it follows that

$$s^\mu s^\nu = s^{\mu+\nu} = s^\nu s^\mu.$$

Now since there are only a finite number of distinct permutations that can be performed on a given finite set of symbols, the series of permutations s, s^2, s^3,... cannot be all distinct. Suppose that s^{m+n} is the first of the series which is the same as one that precedes it, and let that one be s^n. Then

$$s^{m+n} = s^n,$$

and therefore $$s^m s^n (s^n)_{-1} = s^n (s^n)_{-1},$$

or $$s^m = s_0.$$

Hence n must be 1. Moreover there is no index μ smaller than m for which this relation holds. For if

$$s^\mu = s_0,$$

then $$s^{\mu+1} = ss_0 = s,$$

contrary to the supposition that s^{m+1} is the first of the series which is the same as s.

Moreover the $m-1$ permutations $s, s^2, \ldots, s^{m-1}$ must be all distinct. For if

$$s^\mu = s^\nu, \qquad \nu < \mu < m,$$

then $$s^{\mu-\nu} s^\nu (s^\nu)_{-1} = s^\nu (s^\nu)_{-1},$$

or $$s^{\mu-\nu} = s_0,$$

which has just been shewn to be impossible.

The number m is called the *order* of the permutation s. In connection with the order of a permutation, two properties are to be noted. First, if

$$s^n = s_0,$$

it may be shewn at once that n is a multiple of m the order of s; and secondly, if

$$s^\alpha = s^\beta,$$

then $$\alpha - \beta \equiv 0 \pmod{m}.$$

If now the equation

$$s^{\mu+\nu} = s^\mu s^\nu$$

be assumed to hold, when either or both of the integers μ and ν is a negative integer, a definite meaning is obtained for the symbol s^{-r}, implying the negative power of a permutation; and a definite meaning is also obtained for s^0. For

$$s^\mu s^{-\nu} = s^{\mu-\nu} = s^{\mu-\nu} s^\nu (s^\nu)_{-1} = s^\mu (s^\nu)_{-1},$$

so that $$s^{-\nu} = (s^\nu)_{-1}.$$

Similarly it can be shewn that

$$s^0 = s_0.$$

9. If the cycles of a permutation

$$s = (pqr\ldots s)(p'q'\ldots s')(p''q''\ldots s'')\ldots$$

contain $m, m', m'', \ldots$ letters respectively, and if

$$s^\mu = s_0,$$

μ must be a common multiple of $m, m', m'', \ldots$. For s^μ changes p into a letter μ places from it in the cyclical set $p, q, r, \ldots, s$; and therefore, if it changes p into itself, μ must be a multiple of m. In the same way, it must be a multiple of $m', m'', \ldots$. Hence the order of s is the least common multiple of $m, m', m'', \ldots$.

In particular, when a permutation consists of a single cycle, its order is equal to the number of letters which it interchanges. Such a permutation is called a *circular permutation*.

A permutation, all of whose cycles contain the same number of letters, is said to be *regular* in the letters which it interchanges; the order of such a permutation is clearly equal to the number of letters in one of its cycles.

10. Two permutations, which contain the same number of cycles and the same number of letters in corresponding cycles, are called *similar*. If s, s' are similar permutations, so also clearly are s^r, s'^r; and the orders of s and s' are the same.

Let now $$s = (a_p a_q \dots a_s)\,(a_{p'} a_{q'} \dots a_{s'}) \dots$$

and $$t = \begin{pmatrix} a_1, & a_2, \dots, & a_n \\ b_1, & b_2, \dots, & b_n \end{pmatrix}$$

be any two permutations. Then

$$t^{-1}st = \begin{pmatrix} b_1, & b_2, \dots, & b_n \\ a_1, & a_2, \dots, & a_n \end{pmatrix} (a_p a_q \dots a_s)\,(a_{p'} a_{q'} \dots a_{s'}) \dots \begin{pmatrix} a_1, & a_2, \dots, & a_n \\ b_1, & b_2, \dots, & b_n \end{pmatrix}$$
$$= (b_p b_q \dots b_s)\,(b_{p'} b_{q'} \dots b_{s'}) \dots,$$

the latter form of the permutation being obtained by actually carrying out the component permutations of the earlier form. Hence s and $t^{-1}st$ are similar permutations.

Since $$s_2 s_1 = s_1^{-1} s_1 s_2 s_1,$$

it follows that $s_1 s_2$ and $s_2 s_1$ are similar permutations and therefore that they are of the same order. Similarly it may be shewn that $s_1 s_2 s_3 \dots s_{n-1} s_n$, $s_2 s_3 \dots s_{n-1} s_n s_1, \dots$, $s_n s_1 s_2 s_3 \dots s_{n-1}$ are all similar permutations.

It may happen in particular cases that s and $t^{-1}st$ are the same permutation. When this is so, t and s are *permutable*, that is, st and ts are equivalent to one another; for if

$$s = t^{-1}st,$$

then $$ts = st.$$

This will certainly be the case when none of the symbols that are interchanged by t are altered by s; but it may happen when s and t operate on the same symbols. Thus if

$$s = (ab)\,(cd),\quad t = (ac)\,(bd),$$

then $$st = (ad)\,(bc) = ts.$$

Ex. 1. Shew that every regular permutation is some power of a circular permutation.

Ex. 2. If s, s' are permutable regular permutations of the same mn letters of orders m and n, these numbers being relatively prime, shew that ss' is a circular permutation in the mn letters.

Ex. 3*. If
$$s = (123)(456)(789),$$
$$s_1 = (147)(258)(369),$$
$$s_2 = (456)(798),$$
shew that s is permutable with both s_1 and s_2, and that it can be formed by a combination of s_1 and s_2.

Ex. 4. Shew that the only permutations of n given letters which are permutable with a circular permutation of the n letters are the powers of the circular permutation.

Ex. 5. Determine all the permutations of the ten symbols involved in
$$s = (abcde)(\alpha\beta\gamma\delta\epsilon)$$
which are permutable with s.

11. A circular permutation of order two is called a *transposition*. It may be easily verified that
$$(pqr\ldots s) = (pq)(pr)\ldots(ps),$$
so that every circular permutation can be represented as a product of transpositions; and thence, since every permutation is the product of a number of circular permutations, every permutation can be represented as a product of transpositions. It must be remembered, however, that, in general, when a permutation is represented in this way, some of the letters will occur more than once in the symbol, so that the sequence in which the constituent transpositions occur is essential. There is thus a fundamental difference from the case when the symbol of a permutation is the product of circular permutations, no two of which contain a common letter.

Since
$$(p'q') = (pp')(pq')(pp'),$$
every transposition, and therefore every permutation of n letters, can be expressed in terms of the $n-1$ transpositions
$$(a_1a_2),\ (a_1a_3),\ldots,\ (a_1a_n).$$

* It is often convenient to use digits rather than letters for the purpose of illustration.

The number of different ways in which a given permutation may be represented as a product of transpositions is evidently unlimited; but it may be shewn that, however the representation is effected, the number of transpositions is either always even or always odd. To prove this, it is sufficient to consider the effect of a transposition on the square root of the discriminant of the n letters, which may be written

$$D = \prod_{r=1}^{r=n-1} \left\{ \prod_{s=r+1}^{s=n} (a_r - a_s) \right\}.$$

The transposition $(a_r a_s)$ changes the sign of the factor $a_r - a_s$. When q is less than either r or s, the transposition interchanges the factors $a_q - a_r$ and $a_q - a_s$; and when q is greater than either r or s, it interchanges the factors $a_r - a_q$ and $a_s - a_q$. When q lies between r and s, the pair of factors $a_r - a_q$ and $a_q - a_s$ are interchanged and are both changed in sign. Hence the effect of the single transposition on D is to change its sign. Since any permutation can be expressed as the product of a number of transpositions, the effect of any permutation on D must be either to leave it unaltered or to change its sign. If a permutation leaves D unaltered it must, when expressed as a product of transpositions in any way, contain an even number of transpositions; and if it changes the sign of D, every representation of it, as a product of transpositions, must contain an odd number of transpositions. Hence no permutation is capable of being expressed both by an even and by an odd number of transpositions.

A permutation is spoken of as *odd* or *even*, according as the transpositions which enter into its representation are odd or even in number.

Further, an even permutation can always be represented as a product of circular permutations of order three. For any even permutation of n letters can be represented as the product of an even number of the $n-1$ transpositions

$$(a_1 a_2),\ (a_1 a_3),\ldots,\ (a_1 a_n),$$

in appropriate sequence and with the proper number of occurrences; and the product of any consecutive pair of these $(a_1 a_r)\ (a_1 a_s)$ is the circular permutation $(a_1 a_r a_s)$.

Now
$$\begin{aligned}&(a_1a_2a_s)\,(a_1a_2a_r)\,(a_1a_2a_s)^2\\&=(a_1a_2a_s)\,(a_1a_2a_r)\,(a_1a_sa_2)\\&=(a_1a_ra_s),\end{aligned}$$
so that every circular permutation of order three displacing a_1, and therefore every even permutation of n letters, can be expressed in terms of the $n-2$ permutations
$$(a_1a_2a_3),\ (a_1a_2a_4),\ldots,\ (a_1a_2a_n)$$
and their powers.

Ex. 1. Shew that every even permutation of n letters can be expressed in terms of
$$(a_1a_2a_3),\ (a_1a_4a_5),\ldots\ldots,\ (a_1a_{n-1}a_n),$$
when n is odd; and in terms of
$$(a_1a_2a_3),\ (a_1a_4a_5),\ldots\ldots,\ (a_1a_{n-2}a_{n-1}),\ (a_1a_2a_n),$$
when n is even.

Ex. 2. If $n+1$ is odd and m is greater than 1, shew that every even permutation of $mn+1$ letters can be expressed in terms of
$$(a_1a_2\ldots\ldots a_{n+1}),\ (a_1a_{n+2}\ldots\ldots a_{2n+1}),\ldots\ldots,\ (a_1a_{(m-1)n+2}\ldots\ldots a_{mn+1});$$
and if $n+1$ is even, that every permutation of $mn+1$ letters can be expressed in terms of this set of m circular permutations.

The reader, who is not familiar with the notation explained in this chapter, may be advised to study in detail some of the simplest cases that present themselves. The permutations of four symbols are neither too simple nor too complicated for such a purpose. Moreover the fact that to each permutation of four symbols there corresponds a projective transformation of points in a plane, completely defined by the permutation of four arbitrarily chosen points, gives a geometrical interest to the discussion of this case.