4. Groups of permutations

Consider a set of n distinguishable objects, $\{B_1, B_2, B_3, \ldots, B_n\}$. These may be arranged in $n!$ different ways, called *permutations* of the set. Permutations can also be thought of as transformations of a given ordering of the set into other orderings.

A convenient notation for specifying a given permutation operation is
$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix},$$
where the numbers $\{a_1, a_2, a_3, \ldots, a_n\}$ are the numbers $\{1, 2, 3, \ldots, n\}$ in some order. This operation can be interpreted in two different ways, as follows.

Interpretation 1: The object in position 1 in the initial ordering is moved to position a_1, the object in position 2 to position a_2,..., the object in position n to position a_n. In this interpretation, the numbers in the two rows of the permutation symbol refer to the positions of objects in the ordered set.

Interpretation 2: The object labeled 1 is replaced by the object labeled a_1, the object labeled 2 by the object labeled a_2,..., the object labeled n by the object labeled a_n. In this interpretation, the numbers in the two rows of the permutation symbol refer to the labels of the objects in the set. The labels need not be numerical – for instance, $\begin{pmatrix} A & B & C & D \\ D & C & A & B \end{pmatrix}$ is a well-defined permutation which changes $BDCA$, for example, into $CBAD$.

Either of these interpretations is acceptable, but one interpretation must be used consistently in any application. The particular application may dictate which is the appropriate interpretation to use. Note that, in either interpretation, the order of the columns in the permutation symbol is irrelevant – the columns may be written in any order without affecting the result, provided each column is kept intact. The chronological order in which the objects are rearranged doesn't matter.

As an example, consider the action of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ on the ordered set $wxyz$. Using interpretation 1, the first object, w, is moved to the 4$^{\text{th}}$ position; the second object, x, to the 1$^{\text{st}}$ position; the third object, y, to the 3$^{\text{rd}}$ position; the fourth object, z, to the 2$^{\text{nd}}$ position, producing the final order $xzyw$. In order to use interpretation 2, the objects in the

set must be relabeled — $x_1 = w, x_2 = x, x_3 = y, x_4 = z$ — after which the label 1 is replaced by 4, the label 2 by 1, the label 3 by 3 and the label 4 by 2, producing the final order $x_4x_1x_3x_2 = zwyx$. Both interpretations lead to well-defined permutations of the symbols w, x, y, z, but give different results, so it is essential to specify the interpretation being used.

Now consider the effect of multiplying permutations, where multiplication is defined as consecutive action of two permutations. (Recall the standard convention that the right-hand factor in a product acts first, followed by the left-hand factor.) On the result of the above example, act with the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Using interpretation 1, it acts on $xzyw$ to produce $wyzx$, which is produced from $wxyz$ by the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$. This multiplication can be written $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$. By reordering the columns in the left-hand factor of the product so that the top row reads the same as the bottom row of the right-hand factor, this can be rewritten in the form $\begin{pmatrix} 4 & 1 & 3 & 2 \\ 1 & 4 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$. In this form, it is evident that multiplication can be carried out by "canceling" the bottom row of the right-hand factor against the identical top row of the left-hand factor. The result has the top row of the right-hand factor and the bottom row of the left-hand factor. A moment's consideration will show that this is a universal feature (it simply says, for example, move the 1st object to the 4th position in the first step and the 4th object to the 1st position in the second step, leaving the 1st object in the 1st position overall, and so on), which makes multiplication of permutations trivial.

The same process can be carried out using interpretation 2. Now the second permutation acts on $zwyx$ (which is $x_4x_1x_3x_2$) to produce $x_1x_4x_2x_3$, or $wzxy$, which is also the result of acting on $wxyz$ with the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$. The multiplication is expressed in permutation symbols in exactly the same way as in interpretation 1, and the same rule of multiplication by cancellation can be applied. [The two interpretations again lead to different final results, $wyzx$ and $wzxy$, even though they are applied to the same symbolic multiplication.]

The cancellation rule for evaluating products of permutations shows trivially that the multiplication is associative. There is an identity permutation

$\begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$, and the inverse of any permutation is obtained by exchanging its top and bottom rows. So these transformations constitute a group, where multiplication is understood as consecutive action of the transformations.

1. A permutation of the set $\{B_i\}$, followed by another permutation, clearly produces a permutation of the original set, so the permutations are closed under multiplication.

2. The multiplication of permutations has been shown to be associative. (A permutation can be regarded as a mapping of the set of ordered n-tuples of integers, confirming that the multiplication is associative.)

3. The permutation which leaves the ordered set unchanged is clearly an identity.

4. Given a permutation which changes an initial ordering of the set $\{B_i\}$ into a final ordering, the permutation which changes the final ordering back into the initial ordering is the inverse of the starting permutation.

So the set of all permutations of n objects forms a group, called the *symmetric group* on n objects, denoted $\mathcal{S}_n$. It has order $n!$.

An alternative, more economical and very efficient notation for permutations is provided by *cycles*. A *cycle* is a sequence of up to n labels, $(a_1, a_2, a_3, \ldots, a_m)$ $(m \leq n)$ and represents a permutation symbol

$$\begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_{m-1} & a_m & b_1 & \ldots & b_{n-m} \\ a_2 & a_3 & a_4 & \ldots & a_m & a_1 & b_1 & \ldots & b_{n-m} \end{pmatrix},$$

where $\{b_i\}$ are all the $n - m$ labels not included in the set $\{a_i\}$. It permutes the labels $\{a_i\}$ cyclically and leaves the labels $\{b_i\}$ unchanged. The number of labels it contains is the *degree* of the cycle. A cycle of degree m is referred to as an m-cycle. It is easily seen that two cycles with no label in common commute with one another, while two cycles with any labels in common will generally not commute with one another. The order of the entries in a cycle is significant, but since it is cyclic, the starting point is irrelevant: $(a_1, a_2, \ldots, a_m) = (a_2, \ldots, a_m, a_1)$, etc., so an m-cycle can be written in m different but equivalent ways. For example, $(a_1, a_2, a_3, a_4) = (a_2, a_3, a_4, a_1) = (a_3, a_4, a_1, a_2) = (a_4, a_1, a_2, a_3)$.

The order of a cycle is equal to its degree — acting m times with an m-cycle restores all labels to their starting positions, i.e. is equal to the identity.

Any 1-cycle is equal to the identity, as is any product of 1-cycles. A 2-cycle is called a *transposition*, corresponds to interchanging its two entries, and is its own inverse. Any cycle can be decomposed into a (non-unique) product of transpositions. For instance, $(1, 2, 3, \ldots, n) = (1, n)(1, n-1) \ldots (1, 3)(1, 2)$. [This is not unique because the product $(a, b)(a, b) = 1$ can be inserted anywhere.]

Any permutation can be uniquely resolved into a product of non-overlapping cycles — in the permutation $\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix}$, rearrange the columns so that it starts $\begin{pmatrix} 1 & a_1 & \ldots & a'_{m-1} & \cdots \\ a_1 & a_{a_1} & \ldots & 1 & \cdots \end{pmatrix} = (1, a_1, \ldots, a'_{m-1})$; then rearrange the remaining columns in similar cyclic order, beginning with a label not in the set $\{1, a_1, a_{a_1}, \ldots, a'_{m-1}\}$; and continue until all labels are exhausted. It is customary to omit 1-cycles from this resolution, which is self-evidently unique. The result of the resolution can be characterised by listing the number of r-cycles, ν_r, for each value of r from 1 to n. The list $\{\nu_r\}$ defines the *cycle structure* of the permutation. A permutation which is resolved into cycles all of the same degree is called a *regular* permutation and its order is equal to the degree of its cycles. A regular permutation has either only 1-cycles, in which case it is the identity permutation, or no 1-cycles, in which case it leaves no symbol unpermuted.

The symmetric group on n objects $\mathcal{S}_n$, of order $n!$, has many subgroups, each of which is a group of permutations. A group of permutations is regular if all its elements are regular. If all the elements of a group of permutations, except the identity, leave no symbol unpermuted, then the group is regular.

> [Suppose a permutation contains two cycles of different degrees, $k < l$. Then k applications of the permutation leave k symbols unpermuted and l symbols permuted. But the group is closed under multiplication, so k applications of any element must leave all or none of the symbols unpermuted.]

The conjugate of a permutation by some permutation $T = \begin{pmatrix} \{\lambda\} \\ \{\lambda'\} \end{pmatrix}$ is the product of the conjugates of its constituent cycles. The conjugate of a cycle $C = (a_1, a_2, \ldots, a_m)$ is the cycle $C' = (a'_1, a'_2, \ldots, a'_m)$, where a'_i is the symbol into which a_i is changed by the permutation T.

> [Suppose a particular λ is not one of the $\{a_i\}$. Then $T^{-1} : \lambda' \mapsto \lambda; C : \lambda \mapsto \lambda; T : \lambda \mapsto \lambda' \implies TCT^{-1} : \lambda' \mapsto \lambda'$. If $\lambda = a_i$ for some i, then $T^{-1} : a'_i \mapsto a_i; C : a_i \mapsto a_{i+1}; T : a_{i+1} \mapsto a'_{i+1} \implies TCT^{-1} : a'_i \mapsto a'_{i+1}$.]

So conjugation turns an m-cycle into another m-cycle, which implies that all elements of a given class have the same cycle structure (i.e. the same number of cycles of the same degrees).

For the symmetric group on n objects, $\mathcal{S}_n$, the converse also holds — all permutations having the same cycle structure belong to the same class.

[For two permutations $C_1 C_2 \ldots C_k$ and $C_1' C_2' \ldots C_k'$, where the cycles C_i and C_i' have the same degree for all i, conjugate with the permutation $T = \begin{pmatrix} C_1 & C_2 & \ldots & C_k \\ C_1' & C_2' & \ldots & C_k' \end{pmatrix}$, where each cycle in the permutation symbol is replaced by the string of labels it contains. The permutation T is an element of $\mathcal{S}_n$, so the original two permutations belong to the same class. The result does not hold for a general permutation group, since such a group will generally not contain all the permutations T required for conjugation.]

So a class of $\mathcal{S}_n$ is fully defined by its cycle structure — ν_r cycles of each degree r from 1 to n, such that $\sum_{r=1}^{n} r\nu_r = n$. The number of elements in a class is the number of different ways of dividing n symbols into r-cycles, where each r-cycle occurs ν_r times, with $1 \leq r \leq n$, namely $n!/\prod_{r=1}^{n} r^{\nu_r} \nu_r!$.

[Let the cycles be placed side by side and filled with n symbols in all possible ways. There are $n!$ such arrangements. All arrangements in which the ν_r distinct r-cycles are permuted among themselves are equivalent, so the total number must be divided by the product of $\nu_r!$. All arrangements in which the entries in a particular r-cycle are cyclically permuted are equivalent, so the total number must be divided by the product of r^{ν_r}.]

Consider the set of numbers

$$\mu_i = \sum_{j=i}^{n} \nu_j. \tag{1}$$

These satisfy

$$\mu_1 \geq \mu_2 \geq \mu_3 \geq \ldots \geq \mu_n \geq 0 \tag{2}$$

$$\mu_i - \mu_{i+1} = \nu_i \qquad (\mu_n = \nu_n \implies \mu_{n+1} = 0) \tag{3}$$

$$\sum_{i=1}^{n} \mu_i = n \tag{4}$$

so they constitute a *partition* of n which specifies completely a given class of S_n. The classes of S_n are defined by the partitions of n, one to each

partition, and the number of elements in a class is given by the expression quoted above.

Consider the formal function

$$\Delta = \prod_{i<j}^{n}(x_i - x_j),$$

the product of the differences of all distinct pairs of variables in the set of symbols $\{x_i, i = 1, \ldots, n\}$. If a permutation $P \in S_n$ is applied to the indices of the variables, Δ is either unchanged or changes its sign. Write

$$P\Delta = \zeta(P)\Delta,$$

where $\zeta(P) = \pm 1$ is called the *alternating character* of the permutation P. Every permutation is either *even*, $\zeta(P) = 1$, or *odd*, $\zeta(P) = -1$.

Since $\zeta(P_1 P_2)\Delta = P_1 P_2 \Delta = \zeta(P_2)P_1\Delta = \zeta(P_2)\zeta(P_1)\Delta$, it follows that $\zeta(P_1 P_2) = \zeta(P_1)\zeta(P_2)$. Clearly $\zeta(1) = 1$, so $\zeta(P^{-1}) = \zeta(P)$. Also $\zeta(P_2 P_1 P_2^{-1}) = \zeta(P_1)$, so all members of the same class have the same alternating character. Since $\zeta((1, 2)) = -1$, by inspection, all transpositions are odd. From the decomposition of a cycle into a product of transpositions, $\zeta((a_1, a_2, \ldots, a_m)) = (-)^{m-1}$. For the class defined by the partition $\{\mu_i\}$, with the associated $\{\nu_i\}$, the alternating character is $(-)^{\sum_r \nu_r(r-1)} = (-)^{n-\mu_1}$.

In any group $\mathcal{G}$ of permutations (not necessarily the full symmetric group S_n), either half of the permutations are even or all of them are.

[If the group contains any odd permutation, Q say, then $\sum_{P\in\mathcal{G}} \zeta(P) = \sum_{P\in\mathcal{G}} \zeta(PQ) = \sum_{P\in\mathcal{G}} \zeta(P)\zeta(Q) = -\sum_{P\in\mathcal{G}} \zeta(P) = 0$, where the rearrangement theorem has been used in the first step.]

The set of even permutations of S_n is a subgroup, of order $n!/2$, called the *alternating group* A_n.

The multiplication table of a finite group G has the property that every row is a permutation of the first row, with the additional limitation that no element of the group can occur in the same column in different rows. There are n such permutations for a group of order n. Each element of the group can be associated with the permutation defined by the row of the multiplication table which starts with that element. Let the elements of the group be $\{G_1, G_2, G_3, \ldots, G_n\}$, where usually $G_1 = E$, the identity element of G. The permutation associated with an element $X \in \mathcal{G}$ is $\begin{pmatrix} G_1 & G_2 & G_3 & \ldots & G_n \\ XG_1 & XG_2 & XG_3 & \ldots & XG_n \end{pmatrix}$, where interpretation 2 must necessarily

be used – the permutation replaces each element G_i by the element XG_i of the group, regardless of its position in the list of elements. (Recall that the rearrangement theorem ensures that the bottom row of this symbol is a permutation of the top row.)

Consider the product of two such permutations, using the abbreviated notation $\begin{pmatrix} \{G_i\} \\ \{XG_i\} \end{pmatrix}$ for a permutation. Note that, by the rearrangement theorem, $\begin{pmatrix} \{YG_i\} \\ \{XYG_i\} \end{pmatrix} = \begin{pmatrix} \{G_i\} \\ \{XG_i\} \end{pmatrix}$, for any element $Y \in \mathcal{G}$, since the two permutation symbols differ only in the order of their columns. So $\begin{pmatrix} \{G_i\} \\ \{XG_i\} \end{pmatrix}\begin{pmatrix} \{G_i\} \\ \{YG_i\} \end{pmatrix} = \begin{pmatrix} \{YG_i\} \\ \{XYG_i\} \end{pmatrix}\begin{pmatrix} \{G_i\} \\ \{YG_i\} \end{pmatrix} = \begin{pmatrix} \{G_i\} \\ \{XYG_i\} \end{pmatrix}$, by the cancellation rule for multiplication of permutation symbols. By closure for $\mathcal{G}$, the product $XY \in \mathcal{G}$, so the permutation $\begin{pmatrix} \{G_i\} \\ \{XYG_i\} \end{pmatrix}$ is one of the set of n permutations associated with elements of $\mathcal{G}$. This set is therefore closed under multiplication, which is the usual multiplication of permutations and hence associative. (This same result shows that the association of permutations with elements of the group $\mathcal{G}$ preserves the multiplication.) The existence of an identity E and inverses $\{G_i^{-1}\}$ in $\mathcal{G}$ then ensures the existence of an identity permutation $\begin{pmatrix} \{G_i\} \\ \{EG_i\} \end{pmatrix} = \begin{pmatrix} \{G_i\} \\ \{G_i\} \end{pmatrix}$ and inverse permutations $\begin{pmatrix} \{G_i\} \\ \{X^{-1}G_i\} \end{pmatrix}$, so the set of associated permutations is a group. It is of order n and every one of its permutations is associated with an element of the group $\mathcal{G}$.

The association defined above is therefore a mapping from $\mathcal{G}$ onto the group of associated permutations, which preserves multiplication, i.e. it is a homomorphism. But by the properties of permutation symbols, $\begin{pmatrix} \{G_i\} \\ \{XG_i\} \end{pmatrix} = \begin{pmatrix} \{G_i\} \\ \{YG_i\} \end{pmatrix}$ only if $XG_i = YG_i$ for all $G_i \in \mathcal{G}$, i.e. only if $X = Y$ (by the cancellation property of $\mathcal{G}$). So the mapping under discussion is 1–1 and the homomorphism is an isomorphism.

The permutation $\begin{pmatrix} \{G_i\} \\ \{XG_i\} \end{pmatrix}$ replaces the element $G_i \in \mathcal{G}$ by $XG_i \in \{G_i\}$, the element XG_i by X^2G_i, the element X^2G_i by X^3G_i, and so on, until $X^{r-1}G_i$ is replaced by $X^rG_i = G_i$, where r is the order of X in $\mathcal{G}$.

Thus the permutation contains an r-cycle $(G_i, XG_i, X^2G_i, \ldots, X^{r-1}G_i)$. The cycle could not be of degree less than r, since that would contradict the statement that X is of order r. Suppose, for some j, the element G_j does not belong to this r-cycle. Then $(G_j, XG_j, X^2G_j, \ldots, X^{r-1}G_j)$ is another r-cycle contained in the permutation associated with X, with no overlap with the first cycle. This argument may be repeated until all elements G_i are exhausted. So the permutation may be decomposed into r-cycles and is hence regular. The result holds for every $X \in \mathcal{G}$, with its appropriate order, so the group of permutations isomorphic to $\mathcal{G}$ is regular. This is frequently referred to as the *regular representation* of $\mathcal{G}$. (The fact that the group is regular can be more directly established by noting that the rearrangement theorem ensures that every permutation other than the identity leaves no elements of $\mathcal{G}$ unpermuted.)

These results prove *Cayley's Theorem*: every finite group of order n is isomorphic to a regular subgroup of the symmetric group $\mathcal{S}_n$ of order $n!$.