CHAPTER VIII

GROUPS

TAKE a pack of cards. To make the examination simple, suppose that we take quite a small pack, say eight cards from the ace to the eight of hearts, and we will take them in order with the ace uppermost. Now proceed to shuffle the cards, and to examine what is happening, use a regular method of shuffling them. Take the top ace, place the 2 on top, the 3 below, the 4 on top, the 5 below and so on until the eight cards are used. The order of the cards is then

8, 6, 4, 2, 1, 3, 5, 7.

The order is a little more mixed than it was at the start, but the regularity of the order is still apparent. Shuffle the cards again, then, by the same method. The order becomes

7, 3, 2, 6, 8, 4, 1, 5.

A further shuffle of the same kind gives

5, 4, 6, 3, 7, 2, 8, 1.

This third shuffle was less effective in mixing the cards, for the order seems rather more regular than after the second shuffle. A fourth shuffle brings the cards back to their original position,

1, 2, 3, 4, 5, 6, 7, 8.

Now the total number of ways of shuffling a pack of eight cards is $8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 40{,}320$. So it appears that this shuffling procedure is really rather ineffective, since its repetition will give only four out of forty thousand different shuffles. Is there a more effective shuffle, or will every shuffle come back to the identical shuffle if repeated a few times?

We will denote the above shuffle by S, and examine it more closely. Notice that the ace goes into the position of the 5, the 5 takes the position of the 7, which takes the position of the 8, which in turn takes the position of the ace. These four cards, 1, 5, 7, 8, are said to form a *cycle* in the permutation S. In repeating S to give the permutation 7, 3, 2, 6, 8,

4, 1, 5, which we denote by S^2, these cards follow round one another's positions cyclically, but taking two steps forward for S^2 instead of one. Thus the ace takes the position of the seven, which takes the position of the ace. Similarly, the 5 and the 8 interchange. The cycle on the four cards 1, 5, 7, 8 in S is called a *cycle of order* 4, and is denoted by (1 5 7 8). There is another cycle of order 4 in S, which is (2 4 3 6), and we write

$$S = (1\ 5\ 7\ 8)\ (2\ 4\ 3\ 6).$$

In S^2 each cycle of order 4 is replaced by two cycles of order 2, and

$$S^2 = (1\ 7)\ (5\ 8)\ (2\ 3)\ (4\ 6).$$

If m is the least common multiple of the orders of the cycles in a permutation T, then clearly T^m gives the identical permutation in which no cards are altered. This is denoted by I and $T^m = I$. m is the *order* of the permutation T.

The sum of the orders of the cycles is equal to the number of cards, if we include cycles of order one for the cards whose position is unchanged. For eight cards the greatest value of m is obtained for one cycle of order 5 and one of order 3. Thus for

$$T = (1\ 2\ 3\ 4\ 5)\ (6\ 7\ 8)$$

m is equal to 15 and the permutation has to be repeated 15 times before the original order of the cards is restored.

But even 15 is small compared with 40,320. In order to obtain a good mixing of the cards it is desirable to have a second method of shuffling that can be used in addition. For this we will take the permutation U, which takes the last card and puts it in the position of the first, to give

8, 1, 2, 3, 4, 5, 6, 7.

This gives one cycle of order 8, which is

$$U = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8).$$

If we shuffle first with the permutation S and then follow with the permutation U, the order of the cards will become

7, 8, 6, 4, 2, 1, 3, 5.

This compound permutation is denoted by SU, and in terms of the cycles

$$SU = (1\ 6\ 3\ 7)\ (2\ 5\ 8)\ 4.$$

The 4 is placed alone at the end to indicate that it is a card

left unchanged, or it is sometimes omitted altogether. The rule for multiplying permutations expressed in terms of cycles is as follows:

We have $S = (1\ 5\ 7\ 8)\ (2\ 4\ 3\ 6)$,

$U = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$.

To obtain the product SU notice that in S, 1 is followed by 5, and in U, 5 is followed by 6. Hence in SU, 1 will be followed by 6. In S, 6 appears at the end of the second cycle, and this is interpreted as being followed by the first element of the cycle, 2. In U, 2 is followed by 3. Hence in SU, 6 is followed by 3. Similarly $3 \to 6 \to 7$, $7 \to 8 \to 1$, and $(1\ 6\ 3\ 7)$ completes the cycle.

If, instead of shuffling with S and then with U, we had reversed the order and shuffled first with U and then with S, we should have obtained quite a different permutation,

7, 5, 3, 1, 8, 2, 4, 6.

This compound permutation is denoted by US and in terms of cycles gives

$$US = (1\ 4\ 7)\ (2\ 6\ 8\ 5).$$

Notice that SU and US are entirely different permutations. Multiplication of permutations as defined by the above rule is ***non-commutative.***

These 40,320 permutations are said to form a *group.* Mathematically, a group is defined as follows:

If there is given a set of entities $a, b, c, \ldots$, with a rule for combining any two a, b, of the set to produce a third member of the set denoted by ab, then the set is said to form a *group* if the following conditions are satisfied:

(1) There exists an identity element I of the set such that $I\,a = a\,I = a$ for all elements a of the set.

(2) For each element a of the set there exists an inverse element denoted by a^{-1} such that $a\,a^{-1} = a^{-1}\,a = I$.

(3) Multiplication is associative, i.e.

$$a\,(b\,c) = (a\,b)\,c.$$

It is not assumed that multiplication is commutative.

If the number of elements of the group is finite, the group is called a *finite* group, and the number of elements is called the *order* of the group. The group we have been considering

of the permutations of eight cards is clearly a group of order 40,320.

A group which permutes cards, letters, symbols, or any other set of entities is called a ***permutation group***. The number of cards, letters or symbols is called the ***degree*** of the group. The group of all the possible permutations on r entities is of order $r(r-1)(r-2)\ldots 2.1 = r!$ and is called the ***symmetric group*** of degree r, or the symmetric group of order $r!$.

A group may have a subset of elements which themselves form a group. This is called a subgroup. For the symmetric group of permutations on eight cards that we have been considering, the operations S, S^2, S^3, $S^4 = I$ clearly form a group which is a subgroup of order 4. Similarly the powers of U form a subgroup of order 8. A group such as these, which consist of a single element together with its powers, is called a *cyclic* group.

If the two permutations S and U are combined, with any number of repetitions of each in any order, the resulting permutations will form a group which is either the symmetric group itself or some subgroup. It is called the group *generated* by S and U. It can be shown in this case that S and U generate the whole symmetric group, so that by a judicious mixture of the two methods of shuffling any of the 40,320 different shuffles can be obtained.

If we shuffle the pack according to the inverse of U, then with S, and finally with U to give $U^{-1}SU$ we obtain a permutation which has very similar properties to those of S. It has the same number of cycles of the same orders as for S, but the symbol in each cycle is replaced by the symbol which it replaces in the permutation U. Thus, since in U each of the numbers 1 to 7 replaces the number one greater, and 8 replaces 1, then since

$$S = (1\,5\,7\,8)\ (2\,4\,3\,6),$$

then the rule gives

$$U^{-1}SU = (2\,6\,8\,1)\ (3\,5\,4\,7).$$

The element of the group $U^{-1}SU$ is called the transform of S by the element U. For the symmetric group, but not for most other permutation groups which are subgroups of the symmetric group, any two elements which have the same

number of cycles of the same order, are transforms of one another.

Thus, taking $T = (1\ 2\ 3)\ (4\ 5)\ (6\ 7)$ and $V = (8\ 6\ 2)\ (5\ 3)\ (1\ 4)$, if we choose the substitution W for which the numbers 1, 2, 3, 4, 5, 6, 7 take the places of 8, 6, 2, 5, 3, 1, 4 respectively, then $W^{-1}TW = V$ and V is the transform of T by W, while W is the transform of V by W^{-1}. This procedure might not be valid for a subgroup, because, though the required permutation W must belong to the symmetric group, it might not be a member of the given subgroup.

If V is the transform of T by any element of the group, then V and T are said to be *conjugate* elements. The set of all elements conjugate to a given element is a *class of conjugate elements*, or shortly *a class* of the group.

The classes of the symmetric groups depend on the possible arrangements of cycles, and these in turn depend upon *partitions*. If the number 8 is expressed in any way as a sum of integers, then this set of integers, irrespective of their order, is said to form a *partition* of 8. Corresponding to each partition of 8 there is a class of the symmetric group of degree 8.

Thus, since $8 = 5 + 2 + 1$, the set of numbers 5, 2, 1 forms a partition of 8 which is written shortly as (5 2 1). Each element of the group which has one cycle of order 5, one cycle of order 2, with one symbol unchanged belongs to the one class corresponding to the partition (5 2 1). The identity element of the group, leaving every symbol unchanged, has 8 cycles of order 1, and corresponds to the partition $8 = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$. This partition is written as (1^8).

There are 22 partitions of 8, namely (8), (71), (62), (61^2), (53), (521), (51^3), (4^2), (431), (42^2), (421^2), (41^4), (3^22), (3^21^2), (32^21), (321^3), (31^5), (2^4), (2^31^2), (2^21^4), (21^6), (1^8). There are thus 22 classes of the symmetric group. The *order* of the class, which is the number of elements which belong to the class, can be calculated as follows.

Consider the class (32^21). Two elements of the class may be taken as $S = (123)\ (45)\ (67)\ 8$, and $T = (876)\ (54)\ (32)\ 1$. A permutation which transforms the first into the second is the one for which 1, 2, 3, 4, 5, 6, 7, 8 replaces 8, 7, 6, 5, 4, 3, 2, 1. But the cycle (876) could be written as (768) or (687).

Also the cycle (54) could be written as (45) and (32) as (23). This gives $3 \times 2 \times 2 = 12$ different ways of writing the permutation (876) (54) (32) 1, and for each of the twelve there is a permutation which transforms S into T. Further, we can interchange the two cycles (54) and (32), and this gives another twelve, so that altogether 24 elements of the group transform S into T. Similarly 24 elements transform S into any other member of the class, and since there are altogether 8! elements by which we can transform S, it is clear that the total number of elements in the class is $8! \div 24$.

If a is the number of cycles of order 1, b the number of cycles of order 2, c the number of order 3, etc., then the order of the class $(1^a\, 2^b\, 3^c \ldots)$ is by the same reasoning $8!/(1^a\, a!\, 2^b\, b!\, 3^c\, c! \ldots)$. The same method of reasoning shows that for any group whatsoever, the order of each class always divides exactly the order of the group.

If a group H of order h has a subgroup G of order g, then it can be shown that g always divides h exactly.

Let S_2 be an element of H which is not in G. Then if the elements of G are all multiplied by S_2 on the left, we get another set of g elements denoted by $S_2 G = G_2$, all of which are distinct from those of G. If this does not exhaust the elements of H and S_3 is a distinct element, then $S_3 G = G_3$ is a third set of g elements, all of which are distinct from those of G and G_2. Proceeding in the same way until all elements of H are exhausted, we obtain say ν sets each of g elements, $G, G_2, G_3, \ldots, G_\nu$, which are called *cosets* of G, and $g\,\nu = h$, so g divides h exactly.

If the cosets

$$G, S_1 G, S_2 G, \ldots, S_\nu G$$

are multiplied on the left by any element T of the group, then each coset is changed into another (or the same) coset. If TS_i is a member of $S_j G$, then TG_i becomes G_j. In this way, multiplying by T on the left effects a permutation of the cosets. Corresponding to another element U, multiplying on the left effects another permutation of the cosets, and the product of these permutations corresponds to the product UT of the elements of the group.

Each subgroup G of H, therefore, leads to a representation

of H as a permutation group of degree $\nu = h/g$. The importance of this result follows from the fact that almost every group possesses a subgroup; most of them have numerous subgroups. The only groups without subgroups are cyclic groups of prime order. Even in this case we can consider that the identity element by itself forms a subgroup of order one. It certainly does define in the same way a permutation representation whose degree is equal to the order of the group, and which is called the ***regular permutation representation of the group***.

Hence a knowledge of the permutation groups implies a knowledge of all possible finite groups, since they all have representations as permutation groups.