MAF3

HAMERMESH

"Group Theory"

CHAPTER 1

ELEMENTS OF GROUP THEORY

1-1 Correspondences and transformations. All of us are familiar with the concept of a *correspondence*, or *mapping:* We have a *set* of *objects* which we call *points;* these may be *finite* in number, in which case we can enumerate and label them as, say "the points a, b, c," (for a set of three objects) or the points $p_1, \ldots, p_n$ (or the points $1, 2, \ldots, n$) for a set of n objects. They may be *infinite* in number, say "the points designated by the integers 1, 2, etc."; or they may constitute a continuum (all the points in the XY-plane). By a *mapping* of the set of points on itself, we mean that we are given a recipe whereby we associate with each point p of the set an *image* point p' in the set. We say that p' is the *image* of p under the *mapping* M. We indicate this symbolically by

$$p \xrightarrow{M} p', \qquad \text{or} \qquad p' = Mp. \tag{1-1}$$

We can describe Eq. (1-1) by the statement: The operator M acting on the object p changes it to the object p'. For a finite set of points the description of a mapping can be done by enumeration; e.g., for a set of three points, a, b, c, we can describe a mapping by saying: The mapping M takes the point a into its image b, the point b into a, and the point c into c, or symbolically,

$$M \equiv \begin{Bmatrix} a \to b \\ b \to a \\ c \to c \end{Bmatrix}. \tag{1-2}$$

Another possible mapping M' might be

$$M' \equiv \begin{Bmatrix} a \to a \\ b \to a \\ c \to a \end{Bmatrix}. \tag{1-3}$$

For an infinite set of points, enumeration is not possible. Instead we give a *functional law* (or recipe) for the mapping M. For example, we may consider the set of points on the X-axis, and a mapping M whose law is $x \to x' = x + 2$; i.e., each point is to be shifted two units to the right to arrive at its image.

Two mappings M, M' of a set of points are *identical* if $Mp = M'p$ for all points p. Conversely, $M = M'$ means that $Mp = M'p$ for all points p.

One special and important mapping is the *identity* I which maps each point on itself; $Ip = p$. We can perform mappings in succession: If M takes p into $p'(p' = Mp)$, and M' takes p' into $p''(p'' = M'p')$, then

$$p'' = M'p' = M'(Mp), \tag{1–4}$$

which we write as

$$p'' = M'Mp. \tag{1–4a}$$

In other words, there is a single mapping (which we denote by $M'M$) which produces the same effect as the successive application of M and M'. If by a sequence of mappings M_1, M_2, etc., we set up the correspondences

$$p \to p' \to p'' \ldots,$$
$$p' = M_1p, \quad p'' = M_2p', \quad p''' = M_3p'', \ldots,$$

then

$$p''' = M_3(M_2p') = M_3(M_2(M_1p)) = M_3M_2(M_1p) = M_3M_2M_1p,$$

i.e., *mappings* satisfy the *associative law.*

In our example of three points [Eqs. (1–2) and (1–3)] the mapping $M'M$ means

$$\begin{Bmatrix} a \to b \to a \\ b \to a \to a \\ c \to c \to a \end{Bmatrix} = \begin{Bmatrix} a \to a \\ b \to a \\ c \to a \end{Bmatrix}. \tag{1–5}$$

If we had performed the mappings in reverse order, we would have obtained MM',

$$\begin{Bmatrix} a \to b \\ b \to b \\ c \to b \end{Bmatrix}, \tag{1–5a}$$

so that $MM' \neq M'M$. Thus the *composition* or *product* of *mappings* gives a result which, in general, depends on the order in which the mappings are performed; mappings are *noncommutative operations.*

We shall be interested only in one-to-one mappings, or *transformations;* i.e., mappings in which no two points of the set have the same image, and every point p' of the set is the image of one (*only* one) point p. The mapping M in Eq. (1–2) was one-to-one, while M' in Eq. (1–3) was not.

Given a one-to-one mapping, we can find the *inverse* mapping which undoes its work. Thus, if the transformation M takes p into p', $p' = Mp$, its inverse M^{-1} takes p' into p, $p = M^{-1}p'$. Then $p' = Mp = MM^{-1}p'$, whence

$$MM^{-1} = I, \tag{1–6}$$

and $p = M^{-1}p' = M^{-1}Mp$, so that $M^{-1}M = I$. For example, the inverse of

$$M = \begin{Bmatrix} a \to b \\ b \to a \\ c \to c \end{Bmatrix}$$

is

$$M^{-1} = \begin{Bmatrix} a \to b \\ b \to a \\ c \to c \end{Bmatrix};$$

hence, in this case, M is its own inverse.

The inverse of a composite of transformations is easily found. For the mappings M, M' which appear in Eq. (1–4),

$$p = M^{-1}p', \qquad p' = M'^{-1}p'', \qquad p = M^{-1}M'^{-1}p'',$$

so that

$$(M'M)^{-1} = M^{-1}M'^{-1}. \tag{1–7}$$

In words, the *inverse* of the *composite* is obtained by carrying out the *inverse transformations* in *reverse* order.

The following cases are examples of transformations.

EXAMPLES.

(1) *Permutation.* A set of n boxes (points) are labeled 1 to n. Each box contains an object. The objects are rearranged in the boxes so that once more there is one object in each of the n boxes. For example, if the object which was in box 1 before is now in box 3, we shall say that 3 is the image of 1 under the transformation. Consider a specific example of 4 boxes. The objects in the boxes are rearranged so that the occupant of 1 goes to 4, of 2 goes to 3, of 4 goes to 2, and of 3 goes to 1. This mapping is

$$\begin{Bmatrix} 1 \to 4 \\ 2 \to 3 \\ 4 \to 2 \\ 3 \to 1 \end{Bmatrix}.$$

We may say that our transformation is a *transition* from one *arrangement* of the numbers $1, \ldots, 4$ to another arrangement. Such transformations are called *permutations.* One common notation for permutations is to write below each object its image under the transformation. In this notation, our example would be written as

$$\begin{pmatrix} 1234 \\ 4312 \end{pmatrix}.$$

We have written the numbers in the top line in natural order, but this is not necessary; the same permutation could have been written as

$$\begin{pmatrix}1324\\4132\end{pmatrix} \quad \text{or} \quad \begin{pmatrix}4213\\2341\end{pmatrix}.$$

So long as the object-image associations are the same, these various ways of recording represent the same permutation.

Our example is a permutation of four symbols, so we say that it is a permutation of *degree* 4. We could have carried out other rearrangements of the four symbols, e.g., the point 1 could have 1, 2, 3, or 4 as its image. This would leave only three choices for the image of 2, which would then leave only two choices for the image of 3, and finally one choice for the image of 4. Thus there are $4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24$ permutations of degree 4. Similarly, the number of permutations on n symbols, i.e., the number of permutations of degree n, is $n!$

(2) *Translations.* The points of a line are labeled by the coordinate x. The transformation is the shifting of each point two units to the right:

$$x \to x' = x + 2.$$

(3) *Projective transformations of a line.* The projective transformations of the points on the X-axis are defined by

$$x \to x'; \qquad x' = \frac{ax + b}{cx + d}, \qquad \text{where } ad - bc \neq 0.$$

Problem. The cross ratio of four points on a line is defined as

$$\frac{(x_1 - x_2)/(x_3 - x_2)}{(x_1 - x_4)/(x_3 - x_4)},$$

where x_1, x_2, x_3, x_4 are the coordinates of the four points. Show that the cross ratio is *invariant* under projective transformation, i.e., the cross ratio calculated for the image points has the same form as that for the object points.

EXAMPLES (*cont.*).

(4) The permutations of degree n can also be viewed as special *linear transformations* in *n-dimensional space.* The point whose νth coordinate is x_ν is mapped into the point whose p_νth coordinate (relative to the same

axes) is x_ν, where p_ν is the image of ν under the permutation. The permutation is

$$\begin{pmatrix}1 & 2 & \dots & n\\ p_1 & p_2 & \dots & p_n\end{pmatrix},$$

while the corresponding coordinate transformation is

$$\begin{aligned} x'_{p_1} &= x_1,\\ x'_{p_2} &= x_2,\\ &\vdots\\ x'_{p_n} &= x_n. \end{aligned}$$

For the special case given in Example 1, the corresponding coordinate transformation would be

$$\begin{aligned} x_1 &= x'_4,\\ x_2 &= x'_3,\\ x_3 &= x'_1,\\ x_4 &= x'_2. \end{aligned}$$

(5) *Linear transformations in n-dimensional space.* The transformations of Example 4 are special cases of linear transformations in n-dimensional space. With respect to a fixed coordinate system, the linear transformation maps the point with coordinates $(x_1, \dots, x_n)$ into the point with coordinates $(x'_1, \dots, x'_n)$, where the x''s are given by

$$x'_i = \sum_{j=1}^{n} a_{ij}x_j \qquad (i = 1, \dots, n). \tag{1–8}$$

The n^2 coefficients a_{ij} in these linear equations form a square array, the *matrix* $\mathbf{a}$ of the transformation. The transformation (1–8) will have an inverse if the *determinant* of the matrix $\mathbf{a}$ differs from zero, i.e., if $\mathbf{a}$ is a *nonsingular* matrix. If we follow the transformation (1–8) by a second transformation,

$$x''_i = \sum_{j=1}^{n} b_{ij}x'_j \qquad (i = 1, \dots, n),$$

the resultant transformation (product) will be

$$\begin{aligned} x''_i = \sum_{j=1}^{n} b_{ij}x'_j &= \sum_{j=1}^{n} b_{ij} \sum_{k=1}^{n} a_{jk}x_k\\ &= \sum_{k=1}^{n} \left(\sum_{j=1}^{n} b_{ij}a_{jk} \right) x_k. \end{aligned} \tag{1–9}$$

From (1–9) we see that the single transformation which would take us directly from the x's to the x'''s is

$$x_i''' = \sum_{k=1}^{n} c_{ik}x_k,$$

where

$$c_{ik} = \sum_{j=1}^{n} b_{ij}a_{jk} \qquad (i, k = 1, \ldots, n). \tag{1–10}$$

Equation (1–10) gives the rule for combination of elements of the matrices $\mathbf{b}$ and $\mathbf{a}$ to form the *product matrix* $\mathbf{c}$:

$$\mathbf{c} = \mathbf{ba}. \tag{1–11}$$

The last equation is a symbolic statement of the n^2 equations (1–10). Equation (1–8) can also be expressed as a symbolic equation. We may look upon the coordinates $x_1, \ldots, x_n$ as elements of a matrix having n rows and *one* column:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \tag{1–12}$$

and similarly, for $\mathbf{x}'$. Then Eq. (1–8) can be expressed symbolically as

$$\mathbf{x}' = \mathbf{ax}, \tag{1–13}$$

and the inverse transformation as

$$\mathbf{x} = \mathbf{a}^{-1}\mathbf{x}', \tag{1–13a}$$

where $\mathbf{a}^{-1}$ is the matrix of the coefficients of the inverse transformation.

1–2 Groups. Definitions and examples. By a group of transformations, G, we mean an aggregate of transformations of a given point set which

(1) contains the identity transformation;

(2) for every transformation M, also contains its inverse M^{-1};

(3) if it includes M and M', also includes their composite MM'.

The euclidean (rigid-body) motions of ordinary space form a group; the set of all $n!$ permutations of n points form a group; the motions of an equilateral triangle which bring it into coincidence with itself form a group, etc.

From the notion of transformation groups, we arrive at the concept of an abstract group by dissociating points and transformations from any special pictorial significance.

An *abstract group* G is a set of *elements* a, b, c, etc., for which a law of composition or "multiplication" is given so that the "*product*" ab of any two elements is well defined, and which satisfies the following conditions:*

(1) If a and b are elements of the set, then so is ab.

(2) Multiplication is *associative;* that is, $a(bc) = (ab)c$.

(3) The set contains an element e called the *identity* such that $ae = ea = a$ for every element a of the set.

(4) If a is in the set, then so is an element b such that $ab = ba = e$. The element b is called the *inverse* of a, and is denoted by $b = a^{-1}$.

Though we frequently refer to the law of combination as "multiplication," this does not imply ordinary multiplication. The set of rational fractions (omitting zero) form a group under ordinary multiplication. The set of integers, positive, negative, and zero, form a group if the law of combination is ordinary addition. Even in these examples we are not referring to the abstract group, but rather to a concrete example (a "realization") of the abstract group. The *structure* of an abstract group is determined by stating the result of the "multiplication" of every ordered pair of elements, either by enumeration or by stating a functional law, without any particularization of the nature of the elements.

Two elements a, b of a group are said to *commute* with each other if

$$ab = ba, \tag{1–14}$$

i.e., if their product is independent of order. From the group postulates we see that the *identity* element e *commutes* with *all* the elements of the group. If all the elements of a group commute with one another, the group is said to be *commutative* or *abelian*. The use of the symbol $+$ for combination is customary for abelian groups. In such groups, the "product" of the elements a and b is written as $a + b$ (or $b + a$), the symbol 0 is used for the identity, and the inverse of a is written $(-a)$.

The number of elements in a group is called the *order* of the group.

---

* These postulates are actually redundant; (3) and (4) can be replaced by the weaker requirements:

(3′) The set contains an element e called a *left identity*, such that $ea = a$ for every element a of the set.

(4′) If a is in the set, then so is an element b, such that $ba = e$, where e is the left identity described in (3′). The element b is called a *left inverse* of a with respect to the left identity e.

The interested reader should prove that the left identity e in (3′) is also a right identity, that is, $ae = a$, and is unique, and that the element b in (4′) is also a right inverse ($ab = e$) and is uniquely determined by a. Thus (3) and (4) are consequences of the weaker requirements (3′) and (4′).

If we select an element a of the group G, we can form products of a with itself, e.g.,

$$aa,$$

which we denote by a^2. Similarly, by a^n we mean the element which results from a product of n elements each equal to a. Our symbol a^{-1} for the inverse of a was introduced with this notation in mind. Thus

$$a^{-1} \cdot a = e = a^0.$$

We can also define negative powers of a:

$$a^{-m} = (a^{-1})^m = (a^m)^{-1}, \tag{1-15}$$

the last step being a consequence of (1–7). If all the powers of the element a are distinct, then a is said to be of *infinite order*. If this is not the case, then, as we take successive powers of a, we shall find two integers r and s $(r > s)$ such that

$$a^r = a^s.$$

Multiplying by a^{-s}, we have

$$a^{r-s} = e, \qquad r - s > 0.$$

Suppose that n is the smallest positive integer such that a^n is the identity, i.e.,

$$a^n = e, \qquad n > 0; \tag{1-16}$$

and if $a^k = e$, $k > 0$, then $k \geq n$. We say that the element a is of *order* n.

If the element a is of order n, then all the elements

$$a^0 = e, a, a^2, \ldots, a^{n-1} \tag{1-17}$$

are distinct (for if $a^r = a^s$, $a^{r-s} = e$ with $r - s < n$). Thus, every other power of a will be equal to one of the elements listed in (1–17). Any integer k can be written as

$$k = sn + t, \qquad 0 \leq t < n;$$

hence

$$a^k = a^{sn+t} = a^{sn}a^t = (a^n)^s a^t = a^t.$$

From this argument, we also see that if $a^k = e$, k is a multiple of n.

The group of order 1 contains one element, the identity e: $ee = e$.

The group of order 2 contains two distinct elements. One of these must be the identity e. Call the second element a. Then $aa(= a^2)$ cannot be a since $a^2 = a$ implies $a = e$, so we must have $a^2 = e$; that is, a is its own inverse, $a = a^{-1}$. The following examples are groups of order 2:

EXAMPLES.

(1) The elements are the integers 0, 1. The law of combination is addition modulo 2, i.e., we add the elements and find the remainder after division by 2:

$$0 + 0 = 0, \qquad 0 + 1 = 1 + 0 = 1, \qquad 1 + 1 = 0.$$

(2) The objects are the points of three-dimensional space. The element e is the identity transformation, while a is the transformation which replaces each point by its mirror image in a given plane (say the YZ-plane), so that a means changing the sign of the x-coordinate of every point.

(3) The same as (2), but now a is the inversion in the origin of coordinates (i.e., a replaces x, y, z by $-x$, $-y$, $-z$).

(4) The same, but with a the rotation through 180° about, say the Z-axis.

(5) The same, but now a is the reciprocal transformation in the unit sphere: The point with spherical coordinates r, θ, ϕ is imaged in the point $1/r$, θ, ϕ.

(6) The elements are the integers 1, -1, and the law of combination is ordinary multiplication.

(7) The elements are the permutations on two symbols,

$$e = \begin{Bmatrix} 1 \to 1 \\ 2 \to 2 \end{Bmatrix}, \qquad a = \begin{Bmatrix} 1 \to 2 \\ 2 \to 1 \end{Bmatrix}.$$

Here we have seven different realizations of the abstract group of order 2. All these groups have precisely the same structure, and are said to be *isomorphic*.

In general, we shall say that two groups G, G' are *isomorphic* $(G \approx G')$ if their elements can be put into one-to-one correspondence which is preserved under combination. For example, consider the groups (1), (6), and (7) cited above. We make the correspondence:

Group (1):	0	1	$1 + 1 = 0$,
Group (6):	1	-1	$(-1)(-1) = 1$,
Group (7):	$\begin{pmatrix} 1 \to 1 \\ 2 \to 2 \end{pmatrix}$	$\begin{pmatrix} 1 \to 2 \\ 2 \to 1 \end{pmatrix}$	$\begin{pmatrix} 1 \to 2 \\ 2 \to 1 \end{pmatrix}\begin{pmatrix} 1 \to 2 \\ 2 \to 1 \end{pmatrix} = \begin{pmatrix} 1 \to 1 \\ 2 \to 2 \end{pmatrix}$.

If we indicate the correspondent of a (in G) by a' (in G'), so that the prime on an element signifies its correspondent, then G and G' are isomorphic if

$$a'b' = (ab)'.$$

Note that $a'b'$ means the product of a', b' according to the law of combination of G', while ab means the product of a and b according to the law of combination of the group G. For example, the laws of combination in the three groups above were addition, multiplication, and successive transformation, respectively.

If two groups are isomorphic, they have the same structure; the symbols or words may differ, but the abstract groups are the same.

Next consider the abstract group of order 3. Call the distinct elements a, b, e. The product ab cannot equal a (or b) since this would imply $b = e$ (or $a = e$). So ab must equal e. Similarly, we see that $a^2 = b$. Thus the group of order 3 consists of a, a^2, $a^3 = e$. This is an example of a *cyclic* group, one which consists of the powers of a single element.

Some realizations of this group are:

(1) The rotations in the plane of the equilateral triangle ABC which bring it into coincidence with itself.

(2) The rotations of three-dimensional space through angles of 0°, 120°, and 240° about the Z-axis.

(3) The cube roots of unity with ordinary multiplication as the law of combination.

For groups of higher order, this process of enumeration would become quite painful. The law of combination can be presented conveniently in the form of a *group table:* We label the rows and columns of a square array according to the elements of the group. In the box in the nth row and mth column, we record the product of the element labeling the nth row by the element labeling the mth column:

	· · · b
·	
·	
·	
a	ab

For example, the table for the group of order 2 is

	e	a
e	$e^2 = e$	$ea = a$
a	$ae = a$	$a^2 = e$

or briefly,

	e	a
e	e	a
a	a	e

For the group of order 3, we have

	e	a	$b(= a^2)$
e	e	a	b
a	a	b	e
b	b	e	a

We shall usually omit the first row and first column since all they do is to repeat the labeling. Note that the group tables for these examples are symmetric about the main diagonal. This will be the case if, and only if, the group is abelian. Also, we see that in each column (and in each row) all the elements of the group are displayed once and only once. The reason for this is that if we multiply all elements of the group from the left (or right) by a particular element a, then all the products obtained must be distinct: If $ab = ac$, then $b = c$.

There are two distinct structures for abstract groups of order 4:

(A)

e	a	b	c
a	b	c	e
b	c	e	a
c	e	a	b

$a^2 = b, \quad ab = c = a^3,$
$a^4 = b^2 = e,$

i.e., the cyclic group a, a^2, a^3, $a^4 = e$.

(B)

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

$a^2 = b^2 = c^2 = e,$
$ab = c, \quad ac = b, \quad bc = a.$

This group is called the *four-group*, and is often denoted by the symbol V.

From the symmetry of the tables we see that both groups are abelian.

Problems. (1) Show that (A) and (B) are the only possible structures for the group of order 4.

(2) Show directly that the group of order 4 must be abelian.

(3) Give a realization of each of the groups of order 4.

Let us consider some further examples of groups.

EXAMPLES.

(1) The elements are the integers

$$\ldots -3, -2, -1, 0, 1, 2, \ldots,$$

and the law of combination is ordinary addition. The sum of any two integers is again an integer, 0 is the identity, and the inverse of n is $-n$. This group is of *infinite order*. The identity, 0, has order one; the order of all other elements is infinite.

(2) The elements are all rational numbers with addition as the law of combination.

(3) The elements are all complex numbers with addition as the law of combination.

Note that the non-negative integers do *not* form a group under addition. The "products" are in the set, the set contains the identity (0), but the inverses are not in the set.

(4) The group of even integers under addition: This group is of infinite order. Note that group (1) is isomorphic to group (4). To each element n of group (1) we may associate the element $2n$ in group (4). This example shows that a group can be isomorphic with another group which is only a part of the first. (Of course, this *cannot* occur for groups of *finite* order.)

(5) The powers of 2 under ordinary multiplication, that is,

$$\ldots 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, \ldots .$$

If we make n in group (1) correspond to 2^n in group (5), we see that the two groups are isomorphic.

(6) The rational numbers, excluding zero, under multiplication.

(7), (8) Similarly, the real numbers (complex numbers), excluding zero, under multiplication.

(9) The nth roots of unity under multiplication. These are the numbers $e^{2\pi mi/n}$, $m = 0, 1, \ldots, n-1$. This is a cyclic group, all the elements being powers of $e^{2\pi i/n}$. It is clear that there is only one structure of the cyclic group of order n; i.e., all cyclic groups of order n are isomorphic to one another, for if the elements of the two cyclic groups are powers of a and b, respectively, we make the correspondence $a^r \leftrightarrow b^r$. This example also shows that there are groups of *any finite order* n. Moreover, if we have any cyclic group of infinite order, i.e., a group with elements

$$\ldots a^{-3}, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots ,$$

it is isomorphic to group (1), and hence there is only one structure for the cyclic group of *denumerable* order.

(10) The permutations of degree n,

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix},$$

form a group called the *symmetric group* of degree n, which we denote by the symbol S_n. The number of elements in S_n is easily found: 1 can be replaced by any of the symbols 1 to n; after this is done, 2 can be replaced by any of the remaining $n-1$ symbols, etc. Thus the order of the symmetric group S_n is $n!$

Consider the permutation of degree 8,

$$\begin{pmatrix} 12345678 \\ 23154768 \end{pmatrix}.$$

Starting with the symbol 1, we see that the permutation takes 1 into 2. We then look for 2 in the top line and see that the permutation takes 2 into 3, and 3 into 1, closing a *cycle*, which we write as (123). We now start with some other symbol in the top line, say 8. The permutation takes 8 into 8, giving a cycle (8). Continuing, we find the cycles (45) and (67). We may write our permutation alternatively as

$$(123)(45)(67)(8).$$

Note that the cycles have no letters in common. The cycle (123) may be looked upon as an abbreviation for the following permutation of degree 8:

$$\begin{pmatrix} 12345678 \\ 23145678 \end{pmatrix}.$$

We may shorten the notation and omit the unpermuted symbol 8, writing our original permutation as

$$(123)(45)(67), \tag{1-18}$$

but we must keep in mind the degree of the permutation. Since the cycles have no elements in common, they commute with one another, e.g.,

$$(123)(45) = (45)(123),$$

so the order in which we write the cycles is irrelevant. Moreover, in writing an individual cycle, we can start at any point in the chain:

$$(123) = (231) = (312).$$

A cycle containing *two* symbols (2-cycle) is called a *transposition*. Any cycle can be written as a product of transpositions (having elements in common). Thus

$$(123) = (13)(12),$$

and, in general,

$$(12 \ldots n) = (1n) \cdots (13)(12).$$

The cycle on 3 letters is written as a product of 2 transpositions, the cycle on n letters as a product of $n-1$ transpositions.

Proceeding in this fashion, one can resolve any permutation into a product of transpositions. In our example,

$$(123)(45)(67) = (13)(12)(45)(67). \tag{1-19}$$

In (1–18), the number of permuted symbols is 7, and the number of *independent* cycles is 3. The difference of these numbers, $7 - 3 = 4$, is called the *decrement* of the permutation. The reader should supply the proof that if the decrement of a permutation is even (odd), its resolution into a product of transpositions will have an even (odd) number of factors. Permutations with even (odd) decrement are said to be even (odd) permutations.

We now show that if we multiply a given permutation by a transposition, we change the decrement by ± 1, i.e., we go from an even permutation to an odd one, or vice versa. Consider the transposition (ab) by which we multiply the given permutation. We resolve the permutation into independent cycles. Suppose a and b occur in the same cycle:

$$(a \ldots xb \ldots y).$$

Then

$$(ab)(a \ldots xb \ldots y) = (a \ldots x)(b \ldots y),$$

so that the decrement is decreased by 1. Conversely, if a and b are in different independent cycles, we see (by reversing the steps) that multiplying by (ab) increases the decrement by 1. The product of two even (or odd) permutations is an even permutation. The product of an odd and an even permutation is odd. The inverse of an even (odd) permutation is even (odd). The odd permutations of degree n do not form a group (since their products are even permutations). The even permutations of degree n do form a group, the *alternating group* $\mathfrak{A}_n$, which has $n!/2$ elements.

(11) Start with the set of all positive integers. Consider permutations in which any *finite* number of the symbols are permuted. The set of permutations constructed in this way is called the *denumerable symmetric group*.

(12) The group of nonsingular n-by-n matrices, with matrix multiplication as the law of combination.

(13) The unimodular group: the same as (12), except that the elements have determinant $= \pm 1$.

(14) The special unimodular group: the same as (13), except that the determinants are $+1$.

1-3 Subgroups. Cayley's theorem. If we select from the elements of the group G a subset $\mathfrak{H}$, we use the notation $\mathfrak{H} \subset G$ to symbolize that $\mathfrak{H}$ is contained in G. If the subset $\mathfrak{H}$ forms a group (under the *same* law of combination that was used in G), $\mathfrak{H}$ is said to be a *subgroup* of the group G. Every group has two trivial subgroups: the group consisting of the identity element alone, and the whole group G itself. These are said to be *improper* subgroups. The problem of finding all other (*proper*) subgroups of a given group G is one of the main problems of group theory.

We must emphasize the requirement that $\mathfrak{H}$ form a group under the same law of combination as G. The rational numbers form a group G under addition. The positive rational numbers form a group G' under multiplication; but G' is not a subgroup of G, even though the elements of G' are a subset of the elements of G.

To test a subset $\mathfrak{H}$ of elements of the group G to see whether $\mathfrak{H}$ is a subgroup, we require that

(1) the product of any pair of elements of $\mathfrak{H}$ be in $\mathfrak{H}$;

(2) $\mathfrak{H}$ contain the inverse of each of its elements.

The other requirements for a group are taken care of because $\mathfrak{H}$ is contained in the group G. Thus, the associative law held for G and thus holds for $\mathfrak{H}$. The group G contained an identity element, and from (2) and (1) it follows that $\mathfrak{H}$ contains it.

For a finite group (or any group, all of whose elements are of finite order), only requirement (1) is needed. In this case, for each element a in $\mathfrak{H}$, there exists a power of a (also in $\mathfrak{H}$), say a^{n-1}, such that $aa^{n-1} = a^n = e$, so that requirement (2) is a consequence of (1).

In general, both requirements are needed for infinite groups. For example, the positive integers under addition satisfy the first and not the second requirement, and hence do not form a subgroup of all integers under addition.

The alternating group $\mathfrak{A}_n$ is a subgroup of the symmetric group S_n on the same symbols ($\mathfrak{A}_n \subset S_n$). For $n = 3$, S_3 consists of the elements e; (123), (132); (12), (13), (23), and $\mathfrak{A}_3$ contains e; (123), (132).

If $\mathfrak{H}$ is a subgroup of G, and K is a subgroup of $\mathfrak{H}$, then K is a subgroup of G. This *transitive* relation leads to the idea of sequences of subgroups, each containing all those preceding it in the sequence. For example, we may take for G all integers under addition, for $\mathfrak{H}$ all even integers under addition, for K all multiples of $2^2 = 4$ under addition, next all multiples of 2^3, etc.:

G: $\ldots -2, -1, 0, 1, 2, \ldots,$

$\mathfrak{H}$: $\ldots -4, -2, 0, 2, 4, \ldots,$

K: $\ldots -8, -4, 0, 4, 8, \ldots,$

and so on.

Each group contains all the successive subgroups listed below it, that is,

$$G \supset \mathcal{H} \supset K \supset \ldots;$$

and in this case, moreover, all these groups are isomorphic:

$$G \approx \mathcal{H} \approx K \approx \cdots.$$

Thus a group can be isomorphic with one of its proper subgroups, but this is not possible for groups of finite order.

In the case of S_3 given above,

$$S_3 \supset \mathfrak{A}_3 \supset e,$$

where e is the group consisting of the identity only. For all groups of finite order, sequences such as those presented in this special example start with G and end with the group containing only e. Other sequences in S_3 would be:

$$S_3 \supset \mathcal{H}_1 \supset e,$$

$$S_3 \supset \mathcal{H}_2 \supset e,$$

$$S_3 \supset \mathcal{H}_3 \supset e,$$

where $\mathcal{H}_1$ contains two elements, e and (23), $\mathcal{H}_2$ contains e and (13), and $\mathcal{H}_3$ contains e and (12).

A group G' may be isomorphic with one or more subgroups of another group G; for example, S_2, the permutation group on two symbols, is isomorphic with the subgroups $\mathcal{H}_1$, $\mathcal{H}_2$, and $\mathcal{H}_3$ of S_3. Clearly this implies that

$$\mathcal{H}_1 \approx \mathcal{H}_2 \approx \mathcal{H}_3.$$

In general, S_{n-1} is isomorphic with the n subgroups of S_n which are obtained by leaving first the symbol 1, then 2, . . . , then n unchanged. We may also note that the elements of G which are common to two subgroups F_1, F_2 of G form a set D (the *intersection* of F_1 and F_2) which is again a subgroup of G, for if a and b are in D, then a, b are in F_1 and in F_2; therefore, ab and a^{-1} are in F_1 and F_2, and hence are in D, so that D satisfies our requirements for a subgroup. Since every subgroup of G contains the identity e, the intersection of any number of subgroups (i.e., the elements common to all) forms a subgroup which contains at least the identity.

The symmetric groups S_n are especially important because they actually exhaust the possible structures of finite groups. This is shown by *Cayley's theorem:*

THEOREM. Every group G of order n is isomorphic with a subgroup of the symmetric group S_n.

Before proving the theorem, we wish to note its consequences. Cayley's theorem implies that the number of possible nonisomorphic groups of order n is *finite*, for these groups are isomorphic with subgroups of S_n. Since S_n is a finite group, it has only a finite number of subgroups, so that our statement is proved. This is an important result because it at least limits the task of finding independent structures of the group of order n. Now for Cayley's theorem: Let the elements of the group G be $a_1, a_2, \ldots, a_n$. Take any element b; its products with each of the elements in group G are $ba_1, ba_2, \ldots, ba_n$, all of which are different since $ba_i = ba_j$ means $a_i = a_j$. Thus the products ba_i give the elements of G in some new order. We associate with the element b the permutation π_b,

$$b \to \pi_b = \begin{pmatrix} a_1 \ldots a_n \\ ba_1 \ldots ba_n \end{pmatrix},$$

of the n objects $a_1, \ldots, a_n$. Another element c of G is associated with the permutation π_c:

$$c \to \pi_c = \begin{pmatrix} a_1 \ldots a_n \\ ca_1 \ldots ca_n \end{pmatrix}.$$

By this same rule, the element cb is associated with the permutation

$$cb \to \pi_{cb} = \begin{pmatrix} a_1 \ldots a_n \\ cba_1 \ldots cba_n \end{pmatrix}.$$

To prove the isomorphism we must show that π_{cb} is the product of the permutations π_c and π_b.

As we have seen before, only the object-image relation is essential in describing a permutation, while the order in which we write the symbols to be permuted is irrelevant. Thus, π_c can also be written as

$$\pi_c = \begin{pmatrix} ba_1 \ldots ba_n \\ c(ba_1) \ldots c(ba_n) \end{pmatrix}.$$

Taking the product of the images of c and b,

$$\pi_c \pi_b = \begin{pmatrix} ba_1 \ldots ba_n \\ cba_1 \ldots cba_n \end{pmatrix} \begin{pmatrix} a_1 \ldots a_n \\ ba_1 \ldots ba_n \end{pmatrix},$$

we obtain

$$\begin{pmatrix} a_1 \ldots a_n \\ cba_1 \ldots cba_n \end{pmatrix} = \pi_{cb}.$$

The permutation π_e associated with the identity e of G is the identity permutation

$$\pi_e \pi_b = \pi_{eb=b}.$$

Also,

$$\pi_{a^{-1}}\pi_a = \pi_{a^{-1}a} = \pi_e,$$

so that the permutations associated with the elements of G are a subgroup of S_n, and the theorem is proved.

The permutations which we have associated with each group element are just those we would obtain by looking at the group table. For example, in the four-group V, the structure table is

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

To find the permutation corresponding to, say the element a, we write in the top line the symbols

$$eabc,$$

and enter below them the symbols as they appear in the row where we multiply by a on the left, that is,

$$aecb;$$

so

$$a \to \pi_a = \begin{pmatrix} eabc \\ aecb \end{pmatrix}.$$

If we label the elements e, a, b, c as 1, 2, 3, 4, the permutations corresponding to e, a, b, c are:

$$\pi_e = \begin{pmatrix} 1234 \\ 1234 \end{pmatrix},$$

$$\pi_a = \begin{pmatrix} 1234 \\ 2143 \end{pmatrix} = (12)(34),$$

$$\pi_b = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix} = (13)(24),$$

$$\pi_c = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix} = (14)(23).$$

The permutation groups formed in this way have some special features: (1) They are subgroups of order n of the symmetric group S_n. (2) We see that, except for the identity (which permutes *none* of the symbols), the permutations leave *no* symbol unchanged, for π_b takes a_i into ba_i which can equal a_i only if b is the identity. Permutations in S_n having these two properties are called *regular permutations*. Subgroups which contain only regular permutations have other properties which are consequences of the first two. If two of the permutations, π_1, π_2, took the same symbol, say 3, into the same symbol, say 4, then the permutation $\pi_1\pi_2^{-1}$, which is also in the group, would have to leave 3 and 4 unchanged. On the other hand, so long as $\pi_1 \neq \pi_2$, $\pi_1\pi_2^{-1}$ cannot be the identity, and hence it does permute some of the symbols. But this contradicts our previous result that all the permutations (except the identity) leave no symbol unchanged. Since there are n permutations on the n letters, we conclude that the symbol 1 is taken into a different symbol $(1, \ldots, n)$ by each of the permutations in the group. (The same applies to each of the other symbols.) For example, in V, π_e takes 1 into 1, π_a takes 1 into 2, π_b takes 1 into 3, and π_c takes 1 into 4.

Another interesting property of the regular permutation subgroups is the following: Consider any one of the permutations, π_b, and resolve it into independent cycles. We claim that *all* the cycles must have the *same length*. If the resolution of π_b contained two cycles of differing lengths l_1, l_2 $(l_1 < l_2)$, then $\pi_b^{l_1}$, which is also in the group, would leave all the symbols in the first cycle unchanged, while it would *not* leave all the symbols in the second cycle unchanged; this contradicts our definition of the regular permutation subgroup. For example, in a regular subgroup, a permutation like

$$(12)(345)$$

cannot occur, since its square is

$$(1)(2)(354).$$

The four-group illustrates our statement. Each of its permutations is a product of two independent 2-cycles.

The cyclic group of order 4 gives us the regular subgroup of S_4:

$$e; \quad (1234); \quad (13)(24); \quad (1432).$$

The first element has four 1-cycles, the second and fourth have one 4-cycle, and the third has two 2-cycles.

Cayley's theorem can be used to determine possible group structures. For example, suppose that n is a prime number. Then the group of order n is isomorphic to a regular subgroup of S_n. Since the permutations are regular, their resolution into independent cycles must have all cycles equal in length; therefore, the cycle length must be a divisor of n. Since n is prime, the cycle lengths can only be n or 1 (for the identity). So the regular

subgroup is just the cyclic group containing the permutation $(12 \ldots n)$ and its powers. Thus we show that if the order n of a group is *prime*, then the group is *cyclic*. We shall give an alternative proof later in this chapter. Our result solves the problem of finding the possible structures of groups of *prime order*.

Now let us use Cayley's theorem to find the possible group structures of order 4. According to the theorem, our problem is equivalent to finding the regular subgroups of S_4. The permutations of the subgroup must have either one 4-cycle or two 2-cycles (the identity, of course, has four 1-cycles). First suppose that one of the permutations is a 4-cycle, say (1234). Taking successive powers, we obtain (1234), (13)(24), (1432), e, that is, a total of four elements. This is the cyclic group of order 4. Next, suppose that there are no 4-cycles, but only permutations with two 2-cycles. The square of such a permutation is e, and there are just three such permutations,

$$(12)(34); \qquad (13)(24); \qquad (14)(23),$$

which, together with e, give us the four-group.

Problems. (1) Give the elements of the regular subgroup of S_6 which is isomorphic with the cyclic group of order 6.

(2) Use Cayley's theorem to find the possible structures of groups of order 6.

1–4 Cosets. Lagrange's theorem. The abstract groups of order 1, 2, 3 have no proper subgroups. The cyclic group of order 4 has a subgroup of order 2, consisting of a^2 and e, since $(a^2)(a^2) = a^4 = e$. The four-group has three proper subgroups of order 2: a, e; b, e; c, e, all of which have the same structure. We note that the order of the subgroups, 2, is a divisor of the order of the group, 4. We shall now show that this result (due to Lagrange) is generally valid:

The *order* of a *subgroup* of a *finite group* is a *divisor* of the *order* of the group.

Let the group G of order g contain the subgroup $\mathfrak{H}$ of order h. If $\mathfrak{H}$ exhausts the group G, then $\mathfrak{H} = G$, and the result is trivial. (Note that the equals sign here means that the two sets contain the same elements.) If not, then let a be an element of G which is not contained in $\mathfrak{H}$. Denoting the elements of $\mathfrak{H}$ by $e, H_2, H_3, \ldots, H_h$, we form the products $ae = a$, $aH_2, aH_3, \ldots, aH_h$. We shall denote this aggregate of products symbolically as $a\mathfrak{H}$. The products aH_ν are all different, for if $aH_\nu = aH_\mu$, then $H_\nu = H_\mu$. Also, none of them are contained in $\mathfrak{H}$, for if $aH_\nu = H_\mu$, then $a = H_\mu H_\nu^{-1}$, and a would be contained in $\mathfrak{H}$ contrary to our assumption.

Now we have two sets of h distinct elements each, $\mathfrak{H}$ and $a\mathfrak{H}$, which are contained in G. If the group G has not been exhausted, we proceed as before, choosing some element b of G which is not contained in either $\mathfrak{H}$ or $a\mathfrak{H}$. The set $b\mathfrak{H}$ will again yield h new elements of the group G, for if $bH_\nu = aH_\mu$, then $b = aH_\mu H_\nu^{-1}$, and b would be contained in $a\mathfrak{H}$ contrary to our assumption. Continuing this process, we can exhibit the group G as the sum of a finite number of distinct sets of h elements each:

$$G = \mathfrak{H} + a\mathfrak{H} + b\mathfrak{H} + \cdots + k\mathfrak{H}.^* \tag{1–20}$$

Thus the order g of the group G is a multiple of the order h of its subgroup $\mathfrak{H}$, that is,

$$g = mh, \tag{1–21}$$

where m is called the *index* of the subgroup $\mathfrak{H}$ under the group G. The sets (complexes) of elements of the form $a\mathfrak{H}$ in (1–20) are called *left cosets* (*residue classes, nebenklassen, nebengruppen*) of $\mathfrak{H}$ in G. They are certainly not subgroups since they do not contain the identity element. We could, of course, also have carried out our proof by multiplying $\mathfrak{H}$ on the right. This would lead to the resolution of G into *right cosets* with respect to the subgroup $\mathfrak{H}$:

$$G = \mathfrak{H} + \mathfrak{H}a' + \mathfrak{H}b' + \cdots + \mathfrak{H}k'. \tag{1–20a}$$

From Eq. (1–21) we see that a group whose order is a prime number can have no proper subgroups.

Starting with any element a (of order h) of the group G, we can generate a cyclic group by taking successive powers of a. The cyclic group $\{a\}$: $a^0 = e, a, a^2, \ldots, a^{h-1}$, which is generated by a is called the *period* of a. It is the smallest subgroup of G which contains the element a. From Eq. (1–21), h is a divisor of g, so the *orders* of all *elements* of a *finite group* must be *divisors* of the *order* of the group. We conclude that a group of prime order is necessarily cyclic, and can be generated from any of its elements other than the identity element. This gives us the answer to the problem of finding the structure of the group of order 5: It is generated from an element a such that $a^5 = e$; and similarly for the groups of order 7, 11, 13, etc.

---

* The plus sign in Eq. (1–20) denotes the summation of sets: The set G contains all the elements in $\mathfrak{H}$ and all the elements in $a\mathfrak{H}$, etc. In this case, the sets $\mathfrak{H}, a\mathfrak{H}, \ldots$ have no elements in common. In general, the *sum* of two *sets* A and B is the set of all objects which are contained in at least one of the sets A, B.

The following are examples of the resolution of a group into cosets:

EXAMPLES.

(1) Let G be the group of integers under addition, and $\mathfrak{C}$ the group of multiples of 4 under addition. Then

$$G = \mathfrak{C} + (1 + \mathfrak{C}) + (2 + \mathfrak{C}) + (3 + \mathfrak{C}),$$

so that $\mathfrak{C}$ has the index 4 in G. Here the coset $(1 + \mathfrak{C})$ is the set of integers of the form $4n + 1$ (n integral). Two elements a and b of G are in the same coset if $a - b$ is divisible by 4.

(2) Let $G = S_3$ and $\mathfrak{C}$ be the subgroup containing e and (12). Then

$$S_3 = \mathfrak{C} + (13)\mathfrak{C} + (23)\mathfrak{C} = \mathfrak{C} + \mathfrak{C}(13) + \mathfrak{C}(23).$$

Problem. The cyclic permutations on four symbols form a subgroup $\mathfrak{C}$ of S_4. Resolve S_4 into left cosets with respect to $\mathfrak{C}$. Compare this resolution with one into right cosets.

Lagrange's theorem can be used for finding the possible structures of groups of a given order. As an example, we find all structures of order 6. Since the order of the group is 6, the order of each of its elements is a divisor of 6, i.e., 1, 2, 3, or 6. If the group contains an element a of order 6, then the group is the cyclic group $a, a^2, \ldots, a^6 = e$. To find other possible structures, we suppose that the group contains no element of order 6, but has an element a of order 3. Thus the group contains the subgroup a, a^2, $a^3 = e$. If the group also contains another element, b, then it contains the six distinct elements e, a, a^2, b, ba, ba^2. The element b has order 2 or 3. If the order of b is 3, that is, $b^3 = e$, the element b^2 must be one of the six elements listed. We cannot have $b^2 = e$ (since we assumed that b is of order 3), and $b^2 = b$, ba, or ba^2 implies $b = e$, a, or a^2, respectively, which contradicts our assumption that b is distinct from these elements. Furthermore, $b^2 = a$ implies $ba = e$, and $b^2 = a^2$ implies $ba^2 = e$, both of which contradict our assumptions. Thus, the order of b cannot be 3, and we must have $b^2 = e$. The product ab cannot be e, a, a^2, or b. If $ab = ba$, then

$$(ab)^2 = (ab)(ab) = (ab)ba = ab^2a = a^2,$$

$$(ab)^3 = a^2(ab) = b; \qquad (ab)^4 = a, \qquad (ab)^5 = ba^2, \qquad (ab)^6 = e,$$

and therefore the group would contain an element, ab, of order 6, contrary to assumption. (This can be done more briefly: a is of order 2, b of order 3, and $ab = ba$, that is, a and b commute. Taking powers, we see that the order of ab is the least common multiple of the orders of a and b.) We are now left with

$$b^2 = e, \qquad ab = ba^2;$$

$ab = ba^2$ implies $(ab)^2 = (ab)ba^2 = e$.

This last assumption leads to no contradictions. The group of order 6 thus found can be characterized briefly. It is constructed by taking all possible products of a and b, where

$$a^3 = b^2 = (ab)^2 = e.$$

The group table is easily constructed:

e	a	a^2	b	ba	ba^2
a	a^2	e	ba^2	b	ba
a^2	e	a	ba	ba^2	b
b	ba	ba^2	e	a	a^2
ba	ba^2	b	a^2	e	a
ba^2	b	ba	a	a^2	e

This group is isomorphic with S_3.

Problem. Find the possible structures of groups of order 8.

1–5 Conjugate classes. An element b of the group G is said to be *conjugate* to the element a if we can find an element u in G such that

$$uau^{-1} = b. \tag{1–22}$$

Sometimes, we say that b is the *transform* of a by u. By choosing $u = e$, we see that a is conjugate to itself. Also, if b is conjugate to a and c is conjugate to b, then c is conjugate to a, for if $c = vbv^{-1}$, $b = uau^{-1}$, then $c = vuau^{-1}v^{-1} = (vu)a(vu)^{-1}$. Furthermore, from (1–22), $a = u^{-1}b(u^{-1})^{-1}$; so if b is conjugate to a, a is conjugate to b. Thus we have a relation between elements which fulfills all the requirements for an *equivalence relation* (symbol $\equiv$):

(1) $a \equiv a$.

(2) If $a \equiv b$, then $b \equiv a$.

(3) If $a \equiv b$, and $b \equiv c$, then $a \equiv c$.

An equivalence relation can be used to separate a set into *classes*—in our case, to separate the group into classes of elements which are conjugate to one another. In an abelian group each element forms a class by itself, since for any a, b, $bab^{-1} = a$. In every group, the identity element e forms

a class by itself. We note that all elements in the same class have the same order; if $a^h = e$ and $b = uau^{-1}$, then $b^h = (uau^{-1})^h = uau^{-1}uau^{-1} \cdots = ua^hu^{-1} = ueu^{-1} = e$.

Conjugate transformations. For groups of transformations, the notion of conjugate elements has a simple physical meaning. Suppose that a is the reflection in the plane P, and c is a rotation about some axis. Since a leaves every point x of P unchanged, $ax = x$. Then

$$(cac^{-1})(cx) = cax = cx.$$

So the transformation cac^{-1} leaves the set of points cx unchanged. In other words, cac^{-1} is the reflection in the plane obtained from P by the rotation c. Similarly, if a represents a rotation about one axis, then cac^{-1} represents a rotation through the same angle about the axis obtained from the first by transforming with c.

For example, suppose a group contains an element a which is the rotation through angle ϕ about the line l. Let c be some other transformation of the group, say a translation. Then c takes l into another line l'. The transformation cac^{-1} has the following properties: c^{-1} takes the line l' into the line l; then a is a rotation through angle ϕ about l and leaves the points of l fixed; and finally, c takes l back into l'. The net result leaves the points of l' fixed; hence cac^{-1} is a rotation (through angle ϕ) about the line l'.

Conjugate permutations. Now let us apply the notion of conjugate elements to permutations. Suppose that a is the permutation

$$\begin{pmatrix} 1 & \dots & n \\ a_1 & \dots & a_n \end{pmatrix}$$

and b the permutation

$$\begin{pmatrix} 1 & \dots & n \\ b_1 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & \dots & a_n \\ a_{b_1} & \dots & a_{b_n} \end{pmatrix}.$$

Then

$$bab^{-1} = \begin{pmatrix} a_1 & \dots & a_n \\ a_{b_1} & \dots & a_{b_n} \end{pmatrix} \begin{pmatrix} 1 & \dots & n \\ a_1 & \dots & a_n \end{pmatrix} \begin{pmatrix} b_1 & \dots & b_n \\ 1 & \dots & n \end{pmatrix}$$

$$= \begin{pmatrix} b_1 & \dots & b_n \\ a_{b_1} & \dots & a_{b_n} \end{pmatrix}.$$

Comparing with a, we see that to obtain bab^{-1} we apply the permutation b to the top row of a and to the bottom row of a individually. For example, let

$$a = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix}, \qquad b = \begin{pmatrix} 1234 \\ 2134 \end{pmatrix};$$

we apply the permutation b to the top row of a, so that 1234 becomes 2134, and to the bottom row of a, so that 4321 becomes 4312; thus bab^{-1} is

$$\begin{pmatrix} 2134 \\ 4312 \end{pmatrix} = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}.$$

The procedure works equally well if the permutations are given in cycle form; e.g., $a = (12)(345)$ and $b = (24135)$. Then $bab^{-1} = (34)(512)$. We see that conjugate permutations have the same cycle structure so that the permutations in a given class are either all even or all odd. For example, in S_3, e forms a class by itself, the elements (12), (13), (23) form a class, and the elements (123), (213) form a class; so S_3 contains three conjugate classes. In S_4, the distinct classes are:

1. e;
2. (12), (13), (14), (23), (24), (34);
3. (12)(34), (13)(24), (14)(23);
4. (123), (132), (124), (142), (134), (143), (234), (243);
5. (1234), (1243), (1324), (1342), (1423), (1432).

Problem. Separate the elements of S_5 into conjugate classes.

From the procedure used in the example of S_4, the general method should be clear. The permutations of S_n operate on a total of n symbols. Suppose that we resolve the permutations into independent cycles and let the number of 1-cycles be ν_1, of 2-cycles be $\nu_2, \dots$, of n-cycles be ν_n. Since the total number of symbols is n, we must have

$$\nu_1 + 2\nu_2 + \cdots + n\nu_n = n. \tag{1–23}$$

A permutation which when resolved into independent cycles has ν_1 1-cycles, ν_2 2-cycles, $\dots$, ν_n n-cycles is said to have the cycle structure $(1^{\nu_1}, 2^{\nu_2}, \dots, n^{\nu_n})$, or briefly, (ν). As we saw above, all the permutations of S_n which have the same cycle structure (ν) form a conjugate class in S_n. Each solution of (1–23) for positive integers $\nu_1, \dots, \nu_n$ gives a class in S_n, and hence the number of classes is just the number of such solutions. If we let

$$\begin{aligned} \nu_1 + \nu_2 + \cdots + \nu_n &= \lambda_1, \\ \nu_2 + \nu_3 + \cdots + \nu_n &= \lambda_2, \\ &\vdots \\ \nu_n &= \lambda_n, \end{aligned} \tag{1–24}$$

then

$$\lambda_1 + \lambda_2 + \cdots + \lambda_n = n \qquad \text{and} \qquad \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0. \tag{1–25}$$

The splitting-up of n into a sum of n integers as in (1–25) is called a *partition* of n. From (1–23), (1–24), and (1–25) each solution of (1–23) (in non-negative integers) corresponds to a partition of n into $(\lambda_1, \ldots, \lambda_n)$. Conversely, given a partition as in (1–25), there is a corresponding cycle structure, namely:

$$\begin{aligned} \nu_1 &= \lambda_1 - \lambda_2, \\ \nu_2 &= \lambda_2 - \lambda_3, \\ &\vdots \\ \nu_n &= \lambda_n. \end{aligned} \tag{1–26}$$

Usually we do not bother to record those λ's in (1–25) which are 0; e.g., the partition of 5,

$$(22100),$$

i.e., $5 = 2 + 2 + 1 + 0 + 0 = \lambda_1 + \lambda_2 + \cdots + \lambda_5$ is written as (221) or, even more briefly, as $(2^2 1)$. From (1–26), the corresponding cycle structure is

$$\begin{aligned} \nu_1 &= \lambda_1 - \lambda_2 = 2 - 2 = 0, \\ \nu_2 &= \lambda_2 - \lambda_3 = 2 - 1 = 1, \\ \nu_3 &= \lambda_3 = 1, \end{aligned}$$

i.e., one 2-cycle and one 3-cycle.

Similarly in S_6, the partition (31^3) has

$$\nu_1 = 2, \quad \nu_2 = 0, \quad \nu_3 = 0, \quad \nu_4 = 1;$$

so the cycle structure corresponding to (31^3) is two 1-cycles and one 4-cycle.

A transposition in S_n contains one 2-cycle and $(n - 2)$ 1-cycles; hence the partition corresponding to this cycle structure is $(n - 1, 1)$.

We see that the problem of finding the number of conjugate classes in S_n is reduced to the problem of partitioning n. We list the partitions for the first few symmetric groups and the total number, r, of classes:

S_1: (1); $r = 1$,
S_2: (2), (1^2); $r = 2$,
S_3: (3), (21), (1^3); $r = 3$,
S_4: (4), (31), (2^2), (21^2), (1^4); $r = 5$.

Note the order in which we record the partitions. The partition having maximum λ_1 is recorded first, and if two partitions have the same $\lambda_1, \ldots, \lambda_i$, then the one with larger λ_{i+1} is listed first.

Problem. Continue the table to $n = 5, 6, 7$. For $n = 5$, give the cycle structure corresponding to each partition.

An important datum is the number of permutations of S_n in a given conjugate class. This number $n_{(\nu)}$ is easily found as follows: The class with cycle structure (ν) contains the permutations with ν_1 1-cycles, ν_2 2-cycles, $\ldots$, ν_n n-cycles. We imagine the structure to be written out with no symbols inserted:

$$\underbrace{(.)\cdots(.)}_{\nu_1 \text{ 1-cycles,}} \quad \underbrace{(..)(..)\cdots(..)}_{\nu_2 \text{ 2-cycles,}} \quad \underbrace{(...)\cdots(...)\cdots}_{\nu_3 \text{ 3-cycles,}} \quad \text{etc.}$$

There is a total of n places in the various cells into which the n symbols 1 to n are to be placed. This can be done in $n!$ ways. However, duplications will result; e.g., if 1 and 2 appear in 1-cycles, (1)(2) is the same as (2)(1). All the ν_1 1-cycles can be permuted (in $\nu_1!$ ways), all the ν_2 2-cycles can be permuted among themselves in $\nu_2!$ ways, etc., so that a given permutation will be repeated $\nu_1!\nu_2!\cdots\nu_n!$ times. In addition, a 2-cycle like (12) can also appear as (21); a 3-cycle like (123) can also appear as (231) or (312), etc.; thus each permutation is repeated $1^{\nu_1}2^{\nu_2}\ldots n^{\nu_n}$ times. Hence the number of *distinct* permutations of S_n having the cycle structure (ν) is

$$n_{(\nu)} = \frac{n!}{\nu_1! \cdot 2^{\nu_2} \cdot \nu_2! \cdot 3^{\nu_3} \cdot \nu_3! \cdots n^{\nu_n} \cdot \nu_n!} \tag{1–27}$$

Problem. Find the number of permutations in each class of S_5.

It is important to remember that what we have done above applies *only* to the full symmetric group S_n. For example, in S_4 the permutations

$$(12)(34), \quad (13)(24), \quad (14)(23)$$

are all in the same class because S_4 contains a permutation $b = (23)$ such that

$$b(12)(34)b^{-1} = (13)(24).$$

If we consider the four-group V, the permutations listed above are not in the same class in V, since V does not contain the transpositions. In fact, since V is abelian, each of its elements forms a class by itself.

Problem. By taking successive products of the permutations

$$(1234)(5678) \quad \text{and} \quad (1537)(2846),$$

show that one generates a group of order 8. Separate the elements of the group into conjugate classes. Show that this group (the *quaternion group*) is isomorphic to the group with elements

$$1, -1, i, -i, j, -j, k, -k;$$
$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j.$$

1–6 Invariant subgroups. Factor group. Homomorphism. Starting from a subgroup $\mathfrak{H}$ of the group G, we can form the set of elements $a\mathfrak{H}a^{-1}$, where a is any element of G. (By $a\mathfrak{H}a^{-1}$ we mean the set of elements aha^{-1}, where h runs through all the elements of $\mathfrak{H}$.) This set of elements (or *complex*) is again a subgroup of G, (reader, please verify), and is said to be a *conjugate subgroup* of $\mathfrak{H}$ in G. By choosing various elements a from G, we may obtain different conjugate subgroups. It may happen that for *all* a,

$$a\mathfrak{H}a^{-1} = \mathfrak{H}, \tag{1–28}$$

i.e., all the conjugate subgroups of $\mathfrak{H}$ in G are identical with $\mathfrak{H}$. In this case we say that $\mathfrak{H}$ is an *invariant subgroup* (*self-conjugate subgroup, normal divisor*) in G. Written out, (1–28) states that, given an element h_1 in $\mathfrak{H}$, we can, for any a, find an element h_2 in $\mathfrak{H}$ such that $ah_1a^{-1} = h_2$ or $ah_1 = h_2a$. The last equation can be written as

$$a\mathfrak{H} = \mathfrak{H}a, \tag{1–29}$$

and leads to a second definition of an invariant subgroup: The subgroup $\mathfrak{H}$ is invariant in G if the left and right cosets formed with any element a of G are the same. We may say from (1–29) that the subgroup $\mathfrak{H}$, taken as an entity, commutes with all elements of G. From the statements following (1–28) we also see that (1–28) implies the result: If h_1 is in $\mathfrak{H}$, then all elements ah_1a^{-1} are in $\mathfrak{H}$. In other words, a subgroup $\mathfrak{H}$ of G is invariant if, and only if, it contains elements of G in *complete classes;* i.e., for any class of G, $\mathfrak{H}$ contains either *all* or *none* of the elements in the class. The identity element and the whole group G are trivial invariant subgroups of G. A group which has no invariant (proper) subgroups is said to be *simple*. A group is said to be *semisimple* if none of its invariant subgroups are abelian. All the subgroups of an abelian group are clearly invariant.

Invariant subgroups have some very special properties. If $\mathfrak{H}$ is invariant in G, then

$$(a\mathfrak{H})(b\mathfrak{H}) = a(\mathfrak{H}b)\mathfrak{H} = a(b\mathfrak{H})\mathfrak{H} = ab(\mathfrak{H}\mathfrak{H}) = (ab)\mathfrak{H}, \tag{1–30}$$

since $\mathfrak{H}\mathfrak{H}$ simply gives the set of elements in $\mathfrak{H}$. Thus the product of two cosets of an invariant subgroup is again a coset. Also, we note that

$$\mathfrak{H}(a\mathfrak{H}) = (\mathfrak{H}a)\mathfrak{H} = (a\mathfrak{H})\mathfrak{H} = a(\mathfrak{H}\mathfrak{H}) = a\mathfrak{H}, \tag{1–31}$$

so that multiplying any coset of $\mathfrak{H}$ by $\mathfrak{H}$ yields the coset; the invariant subgroup $\mathfrak{H}$ behaves like an identity element in this multiplication of cosets. Again, if we have a coset $a\mathfrak{H}$, we can find the coset which is its inverse (under our new "coset multiplication"), namely, the coset $a^{-1}\mathfrak{H}$ which contains a^{-1}:

$$(a^{-1}\mathfrak{H})(a\mathfrak{H}) = a^{-1}\mathfrak{H}a\mathfrak{H} = a^{-1}a\mathfrak{H}\mathfrak{H} = \mathfrak{H}. \tag{1–32}$$

When we consider the cosets of $\mathfrak{H}$ as elements, and define product as the result of coset multiplication, the cosets of the invariant subgroup form a group which is called the *factor group* (or *quotient group*), symbolized by $G/\mathfrak{H}$, whose order is the index of $\mathfrak{H}$ in G.

Let us find the conjugate subgroups of the subgroup $\mathfrak{H}$ $[e, (12)(34)]$ in the group S_4. The subgroup $\mathfrak{H}$ is not invariant since it does not contain all elements of the third class listed for S_4 in Section 1–5. When we form $a\mathfrak{H}a^{-1}$ with elements a from S_4, we must get cycle structures which are the same as those of the elements of $\mathfrak{H}$. Thus the conjugate subgroups are:

$$\begin{aligned} \mathfrak{H}: &\quad e, (12)(34), \\ \mathfrak{H}': &\quad e, (13)(24), \\ \mathfrak{H}'': &\quad e, (14)(23). \end{aligned}$$

Each is obtained 8 times:

$$\begin{aligned} \mathfrak{H} \text{ for } a &= e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423); \\ \mathfrak{H}' \text{ for } a &= (14), (23), (132), (124), (143), (234), (1243), (1342); \\ \mathfrak{H}'' \text{ for } a &= (13), (24), (123), (142), (134), (243), (1234), (1432). \end{aligned}$$

On the other hand, the subgroup

$$V\colon e, (12)(34), (13)(24), (14)(23)$$

is invariant in S_4 since it contains elements of S_4 in complete classes.

Problems. (1) Without enumerating, find the conjugate subgroups of S_3 in S_4; of S_2 in S_4; of the cyclic group $[e, (123), (132)]$ in S_4.

(2) Prove that a subgroup of index 2 is necessarily invariant.

(3) Show that all subgroups of the quaternion group are invariant.

In the cyclic group G of order 4 $(a, a^2, a^3, a^4 = e)$, the subgroup $\mathfrak{C}$ (e, a^2) is invariant (G is abelian!). The factor group $G/\mathfrak{C}$ contains two elements,

$$E = (e, a^2), \qquad A = (a, a^3),$$

with $A^2 = E$.

Earlier we introduced the concept of isomorphism for groups which had the same structure. A one-to-one correspondence was set up between elements a of a group G and elements a' in a group G', such that $(ab)' = a'b'$. By a *homomorphic* mapping of G on G' we mean a similar correspondence which preserves products, but now *several* elements of G may have the *same image* in G'.

For example, let G be the cyclic group of order 4, and let G' consist of an identity element alone. We map all the elements of G into the identity of G'. Similarly, if G' is the group of order 2, with elements b and $b^2 = e$, we obtain a homomorphism of G on G' if we map (a^2, e) into $b^2 = e$, and (a, a^3) into b.

In a homomorphic mapping of G on G', the image of the identity element e of G is the identity e' of G', for if $ab = a$ (so that b is the identity of G), then $a'b' = a'$, so that b' is the identity in G'. If the set of elements a_1, $a_2, \ldots, a_h$ of G are mapped on e', then choosing some other element b of G, we find h distinct elements $ba_1, ba_2, \ldots, ba_h$ of G which are mapped on the same element b' of G', for $(ba)' = b'a' = b'e' = b'$. Thus equal numbers of elements of G are mapped on each element of G'. If a is mapped on e', so is a^{-1}, as one can verify by taking images in the equation $aa^{-1} = e$. Hence the elements of G which are mapped on e' form a group, in fact an *invariant subgroup* of G, for if a is mapped on e', then so are all the elements in its class, since $(uau^{-1})' = u'a'(u^{-1})' = u'e'(u')^{-1} = e'$. Calling this invariant subgroup $\mathfrak{C}$, we find that any coset $a\mathfrak{C}$ is mapped on a single element of G', since $(a\mathfrak{C})' = a'\mathfrak{C}' = a'e' = a'$. Thus we see that G' is isomorphic to the factor group $G/\mathfrak{C}$.

1–7 Direct products. A group G is said to be the *direct product* of its subgroups $\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_n$ if:

(1) The elements of different subgroups commute.

(2) Every element of g is expressible in one and only one way as

$$g = h_1 \ldots h_n,$$

where h_1 is in $\mathfrak{C}_1, \ldots,$ and h_n is in $\mathfrak{C}_n$.

It is assumed that none of the subgroups consists of the identity element only. Symbolically, we write

$$G = \mathfrak{C}_1 \times \mathfrak{C}_2 \times \cdots \times \mathfrak{C}_n. \tag{1–33}$$

The subgroups $\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_n$ are said to be *direct factors* of G.

From requirements (1) and (2) it follows that the subgroups $\mathfrak{C}_i$ have only the identity in common. It also follows that all the $\mathfrak{C}_i$ are invariant subgroups in G. According to (2), any element g of G can be written as

$$g = h_1 h_2 \ldots h_n,$$

where, according to (1), the h_i all commute with one another. Suppose h_i' belongs to $\mathfrak{C}_i$. Then any conjugate of h_i' is of the form

$$gh_i'g = (h_1 h_2 \ldots h_n)\, h_i'\, (h_1 h_2 \ldots h_n)^{-1} = h_i h_i' h_i^{-1}, \tag{1–34}$$

and also belongs to $\mathfrak{C}_i$. [The factors in (1–34) which belong to other subgroups than $\mathfrak{C}_i$ commute through and cancel.] Thus $\mathfrak{C}_i$ contains elements of G in complete classes, and is therefore invariant in G.

As an example of the resolution of a group into direct factors, consider the cyclic group G of order 6 $(a^6 = e)$. It can be written as the direct product of the subgroups

$$A\colon\ e, a^2, a^4,$$

$$B\colon\ e, a^3.$$

We have

$$G = A \times B.$$

Every element of G is expressible in only one way as a product of an element of A by an element of B. (Reader, check!)

In our work we shall also deal with a direct product $G \times G'$ of two groups G, G'. To obtain it, form all pairs

$$(a, a'),$$

where a is in G and a' in G'. The product of pairs is defined by

$$(a, a')(b, b') = (ab, a'b'). \tag{1–35}$$

If e, e' are the identity elements of G, G', then the pairs (a, e') form a subgroup Γ which is isomorphic to G, the pairs (e, a') form a subgroup Γ' which is isomorphic to G', and the group of element pairs defined above is the direct product of Γ and Γ' according to our previous definition. Usually we shall say simply that it is the direct product of G and G'. It is clear that the order of the direct product of two groups is the product of their orders.