Abstract Group Theory

A group is a set of elements, $\mathcal{G}$, along with a law of composition, denoted by $\cdot$, that obeys the following properties:

1. closure: If $a, b \in \mathcal{G} \Rightarrow a \cdot b \in \mathcal{G}$. Namely, the 'product' of any two members of the set is also a member of the set.

2. associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

3. identity: There exists an element E in $\mathcal{G}$ such that $E \cdot a = a \cdot E = a$, for all a in $\mathcal{G}$. E, the identity is unique. It is the group element that 'does nothing'.

4. inverse: For each a in $\mathcal{G}$, there exists $b = a^{-1}$ in $\mathcal{G}$ such that $a \cdot b = b \cdot a = E$. Each element has a unique inverse within the group.

!IMPORTANT! $a \cdot b$ is not necessarily equal to $b \cdot a$!

If the set $\mathcal{G}$ contains a finite number of elements it is called a finite group. In this case, the number of elements is called the order.

We can also have either

- an infinite discrete group, where the number of elements is denumerably infinite

  or

- a continuous group, with the group elements expressed in terms of continuous parameters.

We will usually be concerned with groups where the elements represent symmetry transformations. We will usually refer to the law of composition as multiplication. We will now drop the notation $\cdot$.

Definitions ad nauseum:

If, for all a and b in $\mathcal{G}$, $a \cdot b = b \cdot a$ - that is, all elements commute - the group $\mathcal{G}$ is called Abelian.

Groups with only one (the identity) or two elements are clearly Abelian. In fact, a group with 3 elements is also Abelian and has a unique multiplication table.

Cyclic groups are those for which all elements can be generated by taking powers of one element. If a is in $\mathcal{G}$, then powers of a like $a^2, a^3, \ldots$ are also in $\mathcal{G}$. If $\mathcal{G}$ is finite, then at some integer power $a^n = E$. The smallest such power is called the order of the element a. Cyclic groups are Abelian.

Simple examples

1. The group of order two consisting of the real numbers 1 and -1 with ordinary multiplication as the law of composition - 'under ordinary multiplication'. The multiplication table is

	1	-1
1	1	-1
-1	-1	1

2. The group of order 4 consisting of the numbers 1, -1, i, $-i$, under multiplication.

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Clearly these are both Abelian since ordinary multiplication is commutative. They are also both cyclic, with the first group being generated by powers of -1 and the second by powers of i. The smallest set of elements whose powers and products generate all the elements of a finite group is called the set of generators of the finite group.

Notice that the group is reproduced in each row and each column of these multiplication tables.

Group Rearrangement Theorem

If $a \in \mathcal{G}$ and we let $b \in \mathcal{G}$ run over all elements in $\mathcal{G}$, then ab also runs over all elements.

Proof: For any $c \in \mathcal{G}$, the choice $b = ca^{-1}$ insures that $c = ba$. This is unique since

$$c = ba = b'a \Rightarrow baa^{-1} = b'aa^{-1} \Rightarrow b = b'.$$

Thus all $c \in \mathcal{G}$ can be formed from ba so the theorem is proved.

3. The discrete infinite group of all real integers is a group under addition. The identity element is 0. The inverse of an integer n is $-n$.

4. Consider the symmetry transformation of inversion, which changes the direction of a vector. Along with the identity (do nothing), this constitutes a simple symmetry group of order two. It clearly has the same multiplication table, and hence structure, as the first example.

5. Consider a rotation in 3-d space through an angle zero - our identity - along with a rotation R through π about the z-axis. Again, this forms a cyclic group, conventionally called C_2, that shares the same structure as examples 1 and 4.

This illustrates the concept of a homomorphism: If there is a mapping of the elements g_a of a group $\mathcal{G}$ onto the elements h_a of a group $\mathcal{H}$ such that the law of composition is preserved

$$g_a g_b = g_c \qquad \Rightarrow \qquad h_a h_b = h_c$$

then $\mathcal{H}$ is homomorphic to $\mathcal{G}$. If the mapping is one-to-one, $\mathcal{H}$ is isomorphic to $\mathcal{G}$. This means that two groups which seemingly have very different physical actions can be regarded in an abstract sense as the same. This allows an exploitation of any knowledge of one of the groups to be applied to the other. Now consider a less trivial example of this concept.

Let $\mathcal{G}$ be the group of the permutations of 3 objects, denoted as $\mathcal{S}_3$.

$$E = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

The elements of $\mathcal{S}_3$ can be written as cycles:

$P_1 = (12)$; $P_2 = (23)$; $P_3 = (13)$; $P_4 = (123)$; $P_5 = (132)$.

The set of all permutations of n objects forms a group $\mathcal{S}_n$. A permutation in which the object labelled by i is replaced by that labelled by p_i is denoted as

$$P = \begin{pmatrix} 1 & 2 & ...n \\ p_1 & p_2 & ...p_n \end{pmatrix}.$$

The numbers $p_1, ..., p_n$ are just a rearrangement of

$1, 2, ..., n$. There are $n!$ elements in $\mathcal{S}_n$.

Notice that $\begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$ and $\begin{pmatrix} 3 & 1 & 2 \\ k & i & j \end{pmatrix}$ describe the same permutation.

Thus we can write the inverse of P as $\begin{pmatrix} p_1 & p_2 & ...p_n \\ 1 & 2 & ...n \end{pmatrix}$.

To express successive permutations, write the second permutation such that its top row is the same as the bottom row of the first permutation (first being on the right). Consider P_1 followed by P_5:

$$\begin{aligned} P_5 P_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2 \end{aligned}$$

One can work out the multiplication table of $\mathcal{S}_3$ readily.

Compare $\mathcal{S}_3$ with a group that seems different - the proper covering group of an equilateral triangle, $\mathcal{H} = D_3$.

Labelling the vertices of an equilateral triangle we can identify the set of rotations that leaves the form of the triangle in place but moves the vertices.

R_1 (R_2), a rotation through $2\pi/3$ ($4\pi/3$) about the z-axis coming out of the triangle

$$R_1 \qquad \begin{array}{ccc} & 1 & \\ & \Delta & \\ 2 & & 3 \end{array} \quad \Rightarrow \quad \begin{array}{ccc} & 3 & \\ & \Delta & \\ 1 & & 2 \end{array}$$

$$R_2 \qquad \begin{array}{ccc} & 1 & \\ & \Delta & \\ 2 & & 3 \end{array} \quad \Rightarrow \quad \begin{array}{ccc} & 2 & \\ & \Delta & \\ 3 & & 1 \end{array}$$

R_3, R_4, and R_5 are rotations through π about the axes in the plane of the triangle and bisecting bottom, left and right sides, respectively.

$$R_3 \qquad \begin{array}{ccc} & 1 & \\ & \Delta & \\ 2 & & 3 \end{array} \quad \Rightarrow \quad \begin{array}{ccc} & 1 & \\ & \Delta & \\ 3 & & 2 \end{array}$$

$$R_4 \qquad \begin{array}{ccc} & 1 & \\ & \Delta & \\ 2 & & 3 \end{array} \quad \Rightarrow \quad \begin{array}{ccc} & 2 & \\ & \Delta & \\ 1 & & 3 \end{array}$$

$$R_5 \qquad \begin{array}{ccc} & 1 & \\ & \Delta & \\ 2 & & 3 \end{array} \quad \Rightarrow \quad \begin{array}{ccc} & 3 & \\ & \Delta & \\ 2 & & 1 \end{array}$$

Along with E, the identity, this constitutes the group D_3. The multiplication table is

	E	R_1	R_2	R_3	R_4	R_5
E	E	R_1	R_2	R_3	R_4	R_5
R_1	R_1	R_2	E	R_4	R_5	R_3
R_2	R_2	E	R_1	R_5	R_3	R_4
R_3	R_3	R_5	R_4	E	R_2	R_1
R_4	R_4	R_3	R_5	R_1	E	R_2
R_5	R_5	R_4	R_3	R_2	R_1	E

The isomorphism between $\mathcal{S}_3$ and D_3 is $R_1 \leftrightarrow P_5$, $R_2 \leftrightarrow P_4$, $R_3 \leftrightarrow P_1$, $R_4 \leftrightarrow P_2$, $R_5 \leftrightarrow P_3$.

We will later use permutation symmetry of identical objects to build up a useful graphical language - Young Tableaux - that can also be applied to groups isomorphic to $\mathcal{S}_n$.

A subgroup is a subset of group elements that satisfies the group properties under the same law of multiplication. The identity and the group itself are two subgroups that every group possesses - the improper subgroups. All other subgroups are called proper subgroups.

For D_3, the set (E, R_1, R_2), with the rotations about the z-axis, is an Abelian, cyclic subgroup (C_3). The equivalent set (E, P_4, P_5), with the 3-cycles, is a subgroup of $\mathcal{S}_3$. The three sets (E, R_3), (E, R_4), and (E, R_5) are each abelian, cylic subgroups (C_2) of D_3. Similarly the three sets with the identity and one 2-cyle form subgroups of the permutation group $\mathcal{S}_3$.

Let $S = \{s_1, s_2, \ldots, s_n\}$ be a proper subgroup of $\mathcal{G}$. For any element g_i in $\mathcal{G}$, the set of elements $g_i S = \{g_i s_1, g_i s_2, \ldots, g_i s_n\}$ is called a left coset. Similarly we define a right coset via right multiplication.

If g_i is itself in S, the coset is identical to S, by the definition of a group.

If g_i is not a member of the subgroup S, then the cosets contain no members of S. We can prove this as follows. For g_i not in S, assume $(g_i s_j)$ is in S. Now, s_j and s_j^{-1} must both be in S. If $(g_i s_j) \in S$, then $(g_i s_j) s_j^{-1} \in S$ but this is just g_i in contradiction to the assumption that g_i is not in S.

Note that sometimes cosets are defined such that g_i is not in S so that the coset would never contain part of S. With this definition, a coset is completely different from the subgroup - they contain no elements in common. In particular, since S must contain the identity, the coset cannot. So with this definition, a coset cannot be a group. The cosets $g_1 S$ and $g_2 S$ either coincide or are completely disjoint. Coincidence occurs if and only if $g_1^{-1} g_2 \in S$. The set of all the left or right cosets of S plus S itself contains all the elements of $\mathcal{G}$.

Now we introduce the concept of classes, which can simplify dealing with large groups. First, we say an element $a \in \mathcal{G}$ is conjugate to $b \in \mathcal{G}$ if there exists an element $u \in \mathcal{G}$ such that $a = ubu^{-1}$. This operation is called a similarity transformation of b by u. If b and c are conjugate to a via $a = ubu^{-1}$ and $a = vcv^{-1}$, then b and c are conjugate to each other via $b = u^{-1}au = u^{-1}vcv^{-1}u = (u^{-1}v)c(u^{-1}v)^{-1}$. The set of elements conjugate to a given element forms a class.

The identity element is a class on its own - the only class that is a group.

Each element of an Abelian group is in a class of its own since $a = ubu^{-1} = buu^{-1} = b$.

Each element of a group is a member of only one class. This follows from the property above of b and c conjugate to each other when each is conjugate to a. We can split the elements of a group into sets of elements conjugate to each other - the conjugacy classes of the group.

The classes of the group D_3 are:

$$\begin{aligned} C_1 &= E \\ C_2 &= (R_1, R_2) \\ C_3 &= (R_3, R_4, R_5) \end{aligned}$$

Equivalently, the classes of $\mathcal{S}_3$ are:

$$\begin{aligned} C_1 &= E \\ C_2 &= (P_4, P_5) \\ C_3 &= (P_1, P_2, P_3) \end{aligned}$$

One can use the multiplication table to obtain these classes. Since elements of a class are related via a similarity transformation we have a more intuitive way to proceed. Rotation through an angle θ about an axis $\hat{k}$, denoted as $R_{\hat{k}}(\theta)$ can be related to a rotation through the same angle about any other axis (with a common origin) by

$$R R_{\hat{k}}(\theta) R^{-1} = R_{\hat{k}'}(\theta)$$

where R is the rotation that takes the axis $\hat{k}$ into $\hat{k}'$, $R\hat{k} = \hat{k}'$. Consequently, all elements of a group representing rotations through the same angle belong to the same class, providing their axes of rotation can be carried into each other via one of elements of the group in a similarity transformation. In D_3, R_2 can be considered as a rotation through $2\pi/3$ about the -z-axis, so it satisfies the criterion that the angle is the same as for R_1. The axes about which the rotations $R_{3,4,5}$ take place are carried into each other via $R_{1,2}$. Thus, for a group of geometric transformations such as D_3, the class structure can be obtained with an understanding of the nature of the transformations.

We get the classes of $\mathcal{S}_3$ immediately due to its isomorphism with D_3. However, we also note a particular structure - each class consists of group elements with the same cycle structure. The cycles leaving one element intact belong in a class together, as do those where all three elements are permuted. In general $\mathcal{S}_n$ has as many classes as it has cyclic structures.

Extend this idea of conjugation: consider a subgroup $\mathcal{H}$ of $\mathcal{G}$. Then the elements $h' = ghg^{-1}$, for all $h \in \mathcal{H}$ with $g \in \mathcal{G}$, form another group $\mathcal{H}'$ that is isomorphic to $\mathcal{H}$. $\mathcal{H}'$ is called a conjugate subgroup to $\mathcal{H}$. If, for all $g \in \mathcal{G}$, we have $\mathcal{H}' = \mathcal{H} = g\mathcal{H}g^{-1}$, then $\mathcal{H}$ is called an invariant subgroup. An invariant subgroup goes into itself on conjugation with any other element of $\mathcal{G}$. An invariant subgroup consists of complete classes of the larger group. Note that we can also write this as $g\mathcal{H} = \mathcal{H}g$ - an invariant subgroup is one for which the left and right cosets are the same with respect to all the elements of $\mathcal{G}$. Invariant subgroups are also called normal subgroups, self-conjugate subgroups, or normal divisors.

A group with no nontrivial invariant subgroups is called simple.

Groups without Abelian invariant subgroups (apart from E) are called semi-simple. Semi-simple groups are often made by putting together simple groups.

The center of a group $\mathcal{G}$, denoted by Z is the set of elements that commute with all g. It is an Abelian invariant subgroup.

For a group $\mathcal{G}$ with an invariant subgroup $\mathcal{H}$, we can construct a new group called the factor or quotient group $\mathcal{G}/\mathcal{H}$. The elements of $\mathcal{G}/\mathcal{H}$ are $\mathcal{H}$ and its distinct cosets.

As an example, the group $\mathcal{S}_3$ has the set (E, P_4, P_5) as an invariant subgroup. It consists of the complete classes C_1 and C_2. The permutations P_4 and P_5 are so-called even permutations, consisting of an even number of transpositions (in this case, two). This invariant subgroup is the Alternating group of permutations $\mathcal{A}_3$. The other subgroups of $\mathcal{S}_3$ are not invariant since they do not contain complete classes. Thus we can form the factor group $\mathcal{S}_3/\mathcal{A}_3$ consisting of two elements, namely $\mathcal{A}_3$ itself and its coset which is the set of the remaining elements $B \equiv (P_1, P_2, P_3)$, the odd permutations (single transposition). The factor group satisfies the following multiplication rules: $\mathcal{A}_3 \cdot \mathcal{A}_3 = \mathcal{A}_3$; $\mathcal{A}_3 \cdot B = B = B \cdot \mathcal{A}_3$; and $B \cdot B = \mathcal{A}_3$. These are the well known results that a product of two even permutations is even, an odd permutation followed by (or following) an even permutation is odd, and the product of two odd permutations is even. The factor group $\mathcal{S}_3/\mathcal{A}_3$ is homomorphic to the group $\mathcal{S}_2$ (also $\mathcal{C}_2$): the elements of $\mathcal{A}_3$ map onto the identity E while the elements of B map onto the transposition of two objects $P = (12)$.

A group $\mathcal{G}$ is a direct product of two groups $\mathcal{H}$ and $\mathcal{H}'$ if all elements of $\mathcal{H}$ commute with all elements of $\mathcal{H}'$ and if every member of $\mathcal{G}$ can be written uniquely as a product of elements from $\mathcal{H}$ and $\mathcal{H}'$. That is $g = hh'$. Only the identity is common to $\mathcal{H}$ and $\mathcal{H}'$. We write this as

$$\mathcal{G} = \mathcal{H} \times \mathcal{H}'.$$

The order of the direct product group is the product of the orders of the two groups. If two elements of $\mathcal{G}$, say ab' and cd' (where $a, c \in \mathcal{H}$ and $c', d' \in \mathcal{H}'$), are in the same class, there must be an element ef' of $\mathcal{G}$ such that

$$(ef')(ab')(ef')^{-1} = (cd').$$

Because the elements of the two groups commute,

$$(eae^{-1})(f'b'f'^{-1}) = cd'$$

so a and c are in the same class of $\mathcal{H}$ while b' and d' are in the same class of $\mathcal{H}'$. Consequently there is a class of $\mathcal{G} = \mathcal{H} \times \mathcal{H}'$ for every pair of classes from the two groups.

If one can recognize a group $\mathcal{G}$ as actually being a direct product of two other groups, then it can be understood by dealing more simply with each of the groups separately.