1. Consider the set $\mathbb{R}^2$ consisting of pairs of real numbers. For $(x, y) \in \mathbb{R}^2$, define scalar multiplication by: $c(x, y) = (cx, cy)$ for any real number c, and define vector addition and multiplication as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)\,, \tag{1}$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)\,. \tag{2}$$

(a) Is $\mathbb{R}^2$ a group?

It is straightforward to check the group axioms and show that $\mathbb{R}^2$ is a group under addition [as defined in eq. (1)]. $\mathbb{R}^2$ is not a group under multiplication. For example, $(0, 0)$ does not possess a multiplicative inverse.

(b) Is $\mathbb{R}^2$ a field?

$\mathbb{R}^2$ is not a field. Recall that all elements of a field, excluding the additive inverse, must possess a multiplicative inverse. In the case of $\mathbb{R}^2$, the additive inverse is $(0, 0)$. However, for any $x \neq 0$ and $y \neq 0$, $(x, 0)$ and $(0, y)$ also do not possess multiplicative inverses.

(c) Is $\mathbb{R}^2$ a linear vector space (over $\mathbb{R}$)?

It is straightforward to check the axioms that define a linear vector space and show that $\mathbb{R}^2$ is a linear vector space over $\mathbb{R}$.

(d) Is $\mathbb{R}^2$ a linear algebra (over $\mathbb{R}$)?

It is straightforward to check the axioms that define a linear algebra and show that $\mathbb{R}^2$ is a linear algebra, where the vector multiplication law is given by eq. (2).

2. Consider the following two groups:

$$T = \big\{\text{proper rotations that map a regular tetrahedron into itself}\big\}\,,$$

$$T_d = \big\{\text{proper rotations and reflections that map a regular tetrahedron into itself}\big\}\,.$$

Show that the following isomorphisms are valid: $T \cong A_4$ and $T_d \cong S_4$.

A regular tetrahedron consists of four equilateral triangles with four vertices (labeled by the integers 1,2,3,4) as shown in Figure 1(a). The symmetry operations, consisting of proper rotations [shown in Figure 1(b) and (c)] and reflections through planes that pass through two of the four tetrahedron vertices, have the effect of permuting the four vertices.

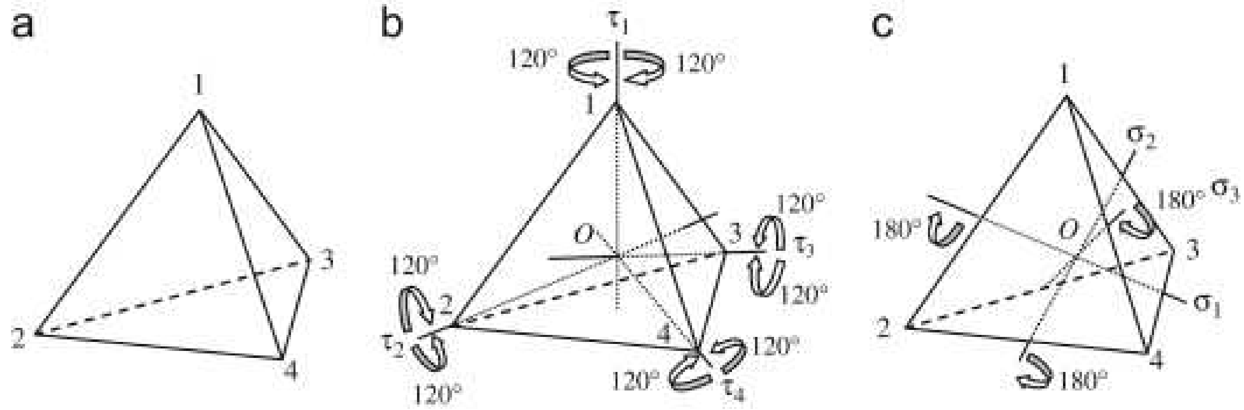

Figure 1: Proper rotations that map a regular tetrahedron into itself.

Consider first the proper rotations. One can rotate by 120° in a clockwise or counterclockwise fashion about an axis through vertex 1, denoted by τ_1 in Figure 1(b). This has the effect of permuting the vertices 2,3,4. All in all, one can perform clockwise or counterclockwise rotations about any one of the four axes [denoted by τ_i, $i = 1, 2, 3, 4$ in Figure 1(b)]. In each case, three of the four vertices are permuted. One can describe each rotation by an element of the permutation group. Using cycle notation, the eight rotation operations described above correspond to the three-cycles of the permutation group S_4. In cycle notation, these are:

$$(123), (132), (124), (142), (134), (143), (234), (243)\,. \tag{3}$$

In addition, one can rotate by 180° about the axes that are denoted by σ_i, $i = 1, 2, 3$ in Figure 1(c). For example, performing a 180° about σ_1 interchanges vertices 1 and 2 and likewise interchanges vertices 3 and 4. Thus, the three possible rotation operations described above correspond to permutations that are the product of two disjoint transpositions. In cycle notation, these are:

$$(12)(34), (13)(24), (14)(23) \tag{4}$$

Finally, the identity element corresponds to performing no rotation (or reflection). This completes the enumeration of all possible proper rotations that map a regular tetrahedron into itself. We conclude that

$$T = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}\,. \tag{5}$$

These twelve elements correspond to the even permutations of the four vertices.[1] Therefore, it follows that

$$T \cong A_4\,,$$

where A_4, the alternating group of four objects, is the subgroup of the permutation group S_4 that consists of the even permutations of four objects.

[1]Even permutations can be expressed as the product of an even number of transpositions. Moreover, as shown in class, an n-cycle can be written as the product of $n-1$ transpositions. Hence, it follows that 3-cycles must be even permutations. Thus, eq. (5) exhausts all the possible even permutations of four objects.

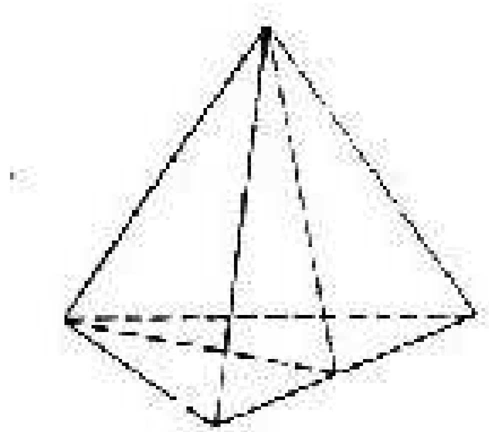

Figure 2: Consider the bisectors of two of the equilateral triangles that are faces of the tetrahedron. The two bisectors meet at a point. The other ends of the two bisectors are connected by one of the tetrahedron edges. This defines one of six possible reflection planes that pass through two of the four vertices of the tetrahedron.

One can also consider six possible reflection planes, one of which is illustrated in Figure 2. Note that each reflection plane passes through two of the four possible tetrahedron vertices. There are $4!/(2!\,2!) = 6$ ways of choosing the two vertices. When a reflection through one of these planes is carried out, the tetrahedron is mapped into itself. The two vertices that are located on the reflection plane are unaffected by the reflection, whereas the other two vertices are interchanged. These correspond to the transpositions of S_4,

$$(12), (13), (14), (23), (24), (34)\,. \tag{6}$$

One can also combine any one of these reflections with a proper rotation. It is sufficient to consider one reflection (e.g., the reflection that interchanges vertices 1 and 2). There are six new permutations that can be produced:

$$(1\ 3\ 4)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4)\,,$$

$$(1\ 4\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 4\ 3)\,,$$

$$(2\ 3\ 4)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)\,,$$

$$(2\ 4\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 3\ 2)\,,$$

$$(1\ 3)(2\ 4)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1\ 4\ 2\ 3)\,,$$

$$(1\ 4)(2\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1\ 3\ 2\ 4)\,.$$

Combining the reflection that interchanges vertices 1 and 2 with the five remaining rotations listed in eqs. (3) and (4) yields the five remaining transpositions,

$$(1\ 2\ 3)(1\ 2) = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} = (1\ 3)\,,$$

$$(1\ 3\ 2)(1\ 2) = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix} = (2\ 3)\,,$$

$$(1\ 2\ 4)(1\ 2) = \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix} = (1\ 4)\,,$$

$$(1\ 4\ 2)(1\ 2) = \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix} = (2\ 4)\,,$$

$$(1\ 2)(3\ 4)(1\ 2) = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix} = (3\ 4)\,.$$

Thus, all the odd permutations of the four tetrahedron vertices can be realized by either a single reflection or a reflection followed by a rotation. One can easily check that two successive symmetry operations of the tetrahedron are in one-to-one correspondence with the multiplication table of S_4. Thus, we conclude that

$$T_d \cong S_4\,.$$

3. Consider the dihedral group D_4.

(a) Write down the group multiplication table.

The elements of D_4 are defined by:

$$D_4 = \{1, r, r^2, r^3, d, rd, r^2d, r^3d\}\,,$$

where the elements satisfy the relations,

$$r^4 = d^2 = 1 \quad \text{and} \quad dr = r^3d\,. \tag{7}$$

We have used the notation $e \equiv 1$ to define the identity element of D_4. Using eq. (7), the group multiplication table is immediately obtained:

	1	r	r^2	r^3	d	rd	r^2d	r^3d
1	1	r	r^2	r^3	d	rd	r^2d	r^3d
r	r	r^2	r^3	1	rd	r^2d	r^3d	d
r^2	r^2	r^3	1	r	r^2d	r^3d	d	rd
r^3	r^3	1	r	r^2	r^3d	d	rd	r^2d
d	d	r^3d	r^2d	rd	1	r^3	r^2	r
rd	rd	d	r^3d	r^2d	r	1	r^3	r^2
r^2d	r^2d	rd	d	r^3d	r^2	r	1	r^3
r^3d	r^3d	r^2d	rd	d	r^3	r^2	r	1

(b) Enumerate the subgroups, the normal subgroups and the classes.

There are eight proper subgroups of D_4:

$$\begin{aligned}\{1,r^2\}\cong\{1,d\}\cong\{1,rd\}\cong\{1,r^2d\}\cong\{1,r^3d\}&\cong\mathbb{Z}_2\,,\\ \{1,r,r^2,r^3\}&\cong\mathbb{Z}_4\,,\\ \{1,r^2,d,r^2d\}\cong\{1,r^2,rd,r^3d\}&\cong D_2\,.\end{aligned}$$

Among these subgroups, four are normal subgroups:[2]

$$\{1,r^2\}\cong\mathbb{Z}_2\,,\quad \{1,r,r^2,r^3\}\cong\mathbb{Z}_4\,,\quad\text{and}\quad \{1,r^2,d,r^2d\}\cong\{1,r^2,rd,r^3d\}\cong D_2\,.$$

Finally, we enumerate the classes:

$$\mathcal{C}_1=\{1\}\,,\quad \mathcal{C}_2=\{r,r^3\}\,,\quad \mathcal{C}_3=\{r^2\}\,,\quad \mathcal{C}_4=\{d,r^2d\}\quad\text{and}\quad \mathcal{C}_5=\{rd,r^3d\}\,. \tag{8}$$

(c) Identify the factor groups. Is the full group the direct product of some of its subgroups?

Using the results of part (b), the possible factor groups are:

$$D_4/\mathbb{Z}_2\cong D_2\,,\qquad D_4/\mathbb{Z}_4\cong\mathbb{Z}_2\,,\qquad D_4/D_2\cong\mathbb{Z}_2\,. \tag{9}$$

The last two factor groups are identified uniquely as $\mathbb{Z}_2$, since this is the only group of two elements. The identification of the first factor group is non-trivial, since there are two possible groups of order four—D_2 and $\mathbb{Z}_4$. Note that D_2 is *not* a cyclic group, whereas $\mathbb{Z}_2$ is a cyclic group. However, it is clear that $D_4/\mathbb{Z}_2$ is not a cyclic group. In particular, writing out the left cosets,

$$D_4/\mathbb{Z}_2=\Big\{\{1,r^2\}\,,\,\{r,r^3\}\,,\,\{d,r^2d\}\,,\,\{rd,r^3d\}\Big\}\,,$$

and identifying $\{1,r^2\}$ as the identity element of $D_4/\mathbb{Z}_2$, it is straightforward to check that the squares of all the other elements of $D_4/\mathbb{Z}_2$ yields the identity element, which is *not* in general satisfied by the elements of $\mathbb{Z}_4$.

In light of eq. (9), the only possible candidates for writing D_4 as a direct product of its subgroups are $\mathbb{Z}_2\otimes D_2$ or $\mathbb{Z}_2\otimes\mathbb{Z}_4$. But the latter two are direct products of abelian groups, which imply that the corresponding direct product groups are abelian, whereas D_4 is a non-abelian group. Hence, D_4 is *not* a direct product of some of its subgroups. On the other hand, D_4 can be expressed as a semi-direct product of its subgroups in two different ways,

$$D_4\cong\mathbb{Z}_4\rtimes\mathbb{Z}_2\cong D_2\rtimes\mathbb{Z}_2\,. \tag{10}$$

[2]One can prove that if a finite group G possesses a subgroup H that contains exactly half the number of elements of G, then H is a normal subgroup of G.

If we take $D_2 = \{1, r^2, rd, r^3d\}$, then we identify $\mathbb{Z}_2 = \{1, d\}$ in both semi-direct products of eq. (10).[3] Note that D_4 cannot be written as $\mathbb{Z}_2 \rtimes D_2$, since the first group of the semi-direct product is the normal subgroup. But, with $\mathbb{Z}_2 = \{1, r^2\}$, we see that one does not obtain all elements of D_4 in the form of $g_1 g_2$, with $g_1 \in \mathbb{Z}_2 = \{1, r^2\}$ and $g_2 \in D_2$.

(d) Write out the class multiplication table.

Using eq. (8) and the group multiplication table, one obtains the following class multiplication table:

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$
$\mathcal{C}_1$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$
$\mathcal{C}_2$	$\mathcal{C}_2$	$2\mathcal{C}_1 + 2\mathcal{C}_3$	$\mathcal{C}_2$	$2\mathcal{C}_5$	$2\mathcal{C}_4$
$\mathcal{C}_3$	$\mathcal{C}_3$	$\mathcal{C}_2$	$\mathcal{C}_1$	$\mathcal{C}_4$	$\mathcal{C}_5$
$\mathcal{C}_4$	$\mathcal{C}_4$	$2\mathcal{C}_5$	$\mathcal{C}_4$	$2\mathcal{C}_1 + 2\mathcal{C}_3$	$2\mathcal{C}_2$
$\mathcal{C}_5$	$\mathcal{C}_5$	$2\mathcal{C}_4$	$\mathcal{C}_5$	$2\mathcal{C}_2$	$2\mathcal{C}_1 + 2\mathcal{C}_3$

(e) Determine explicitly the matrices of the regular representation.

We rewrite the group multiplication table so that the group elements are listed in the first column and the corresponding inverses are listed in the first row.

	1	r^3	r^2	r	d	rd	r^2d	r^3d
1	1	r^3	r^2	r	d	rd	r^2d	r^3d
r	r	1	r^3	r^2	rd	r^2d	r^3d	d
r^2	r^2	r	1	r^3	r^2d	r^3d	d	rd
r^3	r^3	r^2	r	1	r^3d	d	rd	r^2d
d	d	rd	r^2d	r^3d	1	r^3	r^2	r
rd	rd	r^2d	r^3d	d	r	1	r^3	r^2
r^2d	r^2d	r^3d	d	rd	r^2	r	1	r^3
r^3d	r^3d	d	rd	r^2d	r^3	r^2	r	1

The matrix of the regular representation of the element $g \in D_4$ is then obtained from this table by replacing the corresponding every appearance of g with 1, and filling up the rest of the corresponding matrix with zeros. That is,

$$1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad r = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

[3] If $D_2 = \{1, r^2, d, r^2d\}$ then we identify $\mathbb{Z}_2 = \{1, rd\}$ in the second semi-direct product in eq. (10).

$$r^2 = \begin{pmatrix} 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0 \end{pmatrix}, \qquad r^3 = \begin{pmatrix} 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0 \end{pmatrix},$$

$$d = \begin{pmatrix} 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0 \end{pmatrix}, \qquad rd = \begin{pmatrix} 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0 \end{pmatrix},$$

$$r^2d = \begin{pmatrix} 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{pmatrix}, \qquad r^3d = \begin{pmatrix} 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0 \end{pmatrix}.$$

(f) Write out an explicit irreducible two-dimensional representation of D_4. Check that the group multiplication table is preserved. Verify that this representation is irreducible.

In class, we wrote out the following two-dimensional representation for D_n,

$$r = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \qquad d = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For $n = 4$, this yields:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad r^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad r^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$d = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad rd = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad r^2d = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad r^3d = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

One easily checks that the above representation matrices satisfy the group multiplication table.

To show that this is an irreducible representation, we must prove that there is no basis in which the above matrices are reduced to block diagonal form. If such a basis existed, then we could simultaneously diagonalize the matrices that represent r and rd. But these elements do not commute and thus are not simultaneously diagonalizable.

As an alternative proof that the above two-dimensional representation, $D(g)$, is irreducible, one can check explicitly that if $AD(g) = D(g)A$ for all $g \in D_4$, then A is a multiple of the identity. For this problem, it is enough to check that for an arbitrary 2×2 matrix A, if $Ar = rA$ and $Ad = dA$, with r and d given by the 2×2 matrices listed above, then $A = c\mathbb{1}_{2\times 2}$ for some complex number c. Hence, by Schur's second lemma, $D(g)$ is an irreducible representation of D_4.

4. The *center* of a group G, denoted by $Z(G)$, is defined as the set of elements $z \in G$ that commute with all elements of the group. That is,

$$Z(G) = \{z \in G \,|\, zg = gz \,, \forall\, g \in G\} \,.$$

(a) Show that $Z(G)$ is an abelian subgroup of G.

To prove that $Z(G)$ is a subgroup of G, we must prove that:

(i) $z_1,\, z_2 \in Z(G) \quad \Longrightarrow \quad z_1 z_2 \in Z(G)$,

(ii) $e \in Z(G)$, where e is the identity,

(iii) $z \in Z(G) \quad \Longrightarrow \quad z^{-1} \in Z(G)$.

To prove (i), we note that $z_1,\, z_2 \in Z(G)$ means that

$$z_1 g = g z_1 \,, \qquad \text{for all } g \in G, \tag{11}$$

$$z_2 g = g z_2 \,, \qquad \text{for all } g \in G. \tag{12}$$

Multiply eq. (11) on the right by z_2 to obtain

$$z_1 g z_2 = g z_1 z_2 \,. \tag{13}$$

Then, use eq. (12) to write $z_1 g z_2 = z_1 z_2 g$. Then, eq. (13) can be rewritten as

$$z_1 z_2 g = g z_1 z_2 \,,$$

which means that $z_1 z_2$ commutes with any element $g \in G$. Hence, $z_1 z_2 \in Z(G)$.

The proof of (ii) is trivial since e commutes with all elements of G. Finally to prove (iii) we note that $z \in Z(G)$ means that $zg = gz$ for all $g \in G$. Multiplying this equation on the left by g^{-1} and on the right by g^{-1} yields

$$g^{-1} z = z g^{-1} \,, \quad \text{for all } g \in G \,. \tag{14}$$

Taking the inverse of eq. (14) yields

$$z^{-1} g = g z^{-1} \,, \quad \text{for all } g \in G \,.$$

Hence, $z^{-1} \in Z(G)$. Thus, we have succeeded in showing $Z(G)$ is a subgroup of G.

Finally, it should be clear that $Z(G)$ is an abelian subgroup. As previously noted, for any $z_1,\, z_2 \in Z(G)$, eq. (11) is satisfied. In particular, choosing $g = z_2$ in eq. (11), it follows that $z_1 z_2 = z_2 z_1$. This arguments continues to hold for any choice of $z_1, z_2 \in Z(G)$. Thus, we conclude that $Z(G)$ is an *abelian* subgroup of G.

(b) Show that $Z(G)$ is a normal subgroup of G.

To show that $Z(G)$ is a normal subgroup, one must show that for any $z \in Z(G)$ and $g \in G$, we have $gzg^{-1} \in Z(G)$. By definition, if $z \in Z(G)$ then $gz = zg$ for all $g \in G$. Hence, for any $z \in Z(G)$, we have $gzg^{-1} = z$ for all $g \in G$. Since $z \in Z(G)$ by assumption, one can conclude that $gzg^{-1} \in Z(G)$ for all $g \in G$, as required for a normal subgroup.

(c) Find the center of D_4 and construct the group $D_4/Z(D_4)$. Determine whether the isomorphism $D_4 \cong [D_4/Z(D_4)] \otimes Z(D_4)$ is valid.

The multiplication table for D_4 was given in part (a) of problem 2. Inspection of the multiplication table reveals that:

$$Z(D_4) = \{e, r^2\} \cong \mathbb{Z}_2 \,,$$

where the identification of the center follows from the fact that any finite group of two elements must be isomorphic to $\mathbb{Z}_2$.

The left cosets of D_4 with respect to the $\mathbb{Z}_2$ subgroup are:

$$\begin{aligned} \mathbb{Z}_2 &= \{e, r^2\} \,, \\ r\mathbb{Z}_2 &= \{r, r^3\} \,, \\ d\mathbb{Z}_2 &= \{d, r^2 d\} \,, \\ rd\mathbb{Z}_2 &= \{rd, r^3 d\} \,, \end{aligned}$$

which exhausts all the elements of D_4. We identify the quotient group

$$D_4/\mathbb{Z}_2 = \Big\{ \{e, r^2\} \,,\, \{r, r^3\} \,,\, \{d, r^2 d\} \,,\, \{rd, r^3 d\} \Big\} \,.$$

Using the multiplication table for D_4, one can easily construct the multiplication table for $D_4/\mathbb{Z}_2$,

	$\{e, r^2\}$	$\{r, r^3\}$	$\{d, r^2 d\}$	$\{rd, r^3 d\}$
$\{e, r^2\}$	$\{e, r^2\}$	$\{r, r^3\}$	$\{d, r^2 d\}$	$\{rd, r^3 d\}$
$\{r, r^3\}$	$\{r, r^3\}$	$\{e, r^2\}$	$\{rd, r^3 d\}$	$\{d, r^2 d\}$
$\{d, r^2 d\}$	$\{d, r^2 d\}$	$\{rd, r^3 d\}$	$\{e, r^2\}$	$\{r, r^3\}$
$\{rd, r^3 d\}$	$\{rd, r^3 d\}$	$\{d, r^2 d\}$	$\{r, r^3\}$	$\{e, r^2\}$

This is clearly not a cyclic group with one generator. Hence, it is not isomorphic to the cyclic group $\mathbb{Z}_4$, which leave only one remaining possibility, D_2. Indeed, one can check that the multiplication table above is equivalent to that of D_2. Hence,

$$D_4/\mathbb{Z}_2 \cong D_2 \,.$$

Finally, if the isomorphism $D_4 \cong [D_4/Z(D_4)] \otimes Z(D_4)$ were valid, then

$$D_4 \overset{?}{\cong} D_2 \otimes \mathbb{Z}_2 \,.$$

But this identification is incorrect. In particular, D_4 is a nonabelian group, whereas both D_2 and $\mathbb{Z}_2$ are abelian groups. Thus, it follows that $D_2 \otimes \mathbb{Z}_2$ is abelian, which means that this group cannot be isomorphic to the nonabelian group D_4.

5. An automorphism is defined as an isomorphism of a group G onto itself.

(a) Show that for any $g \in G$, the mapping $T_g(x) = gxg^{-1}$ is an automorphism (called an *inner automorphism*), where $x \in G$.

To show that $T_g(x) = gxg^{-1}$ is an automorphism, we must show that it is a homomorphism from the group G to itself that is one-to-one and onto. To prove that T_g is a homomorphism, one must verify that

$$T_g(x)T_g(y) = T_g(xy)\,, \qquad \text{for all } x, y \in G\,. \tag{15}$$

That is, $T_g(x)$ preserves the group multiplication table. The computation is straightforward:

$$T_g(x)T_g(y) = (gxg^{-1})(gyg^{-1}) = gxyg^{-1} = T_g(xy)\,.$$

To see that $T_g(x) = gxg^{-1}$ is one-to-one and onto (i.e. it is an isomorphism), we can invoke the rearrangement lemma. Multiplication on the left and/or on the right by a fixed element of G simply reorders the group multiplication table.[4] Hence, we conclude that T_g is an isomorphism from $G \longrightarrow G$. That is, T_g is an automorphism of the group G.

(b) Show that the set of all inner automorphisms of G, denoted by $\mathcal{I}(G)$, is a group.

Define $\mathcal{I}(G) = \{T_g \,|\, g \in G\}$. Since T_g is an automorphism, we can introduce a group multiplication law that consists of the composition of two maps. In particular,

$$T_{g_1}T_{g_2}(x) = T_{g_1}(g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2)x(g_1 g_2)^{-1} = T_{g_1 g_2}(x)\,,$$

which holds for any $x \in G$. Hence, the composition of two maps is given by:

$$T_{g_1}T_{g_2} = T_{g_1 g_2}\,. \tag{16}$$

It follows that $\mathcal{I}(G)$ satisfies the axioms of a group by virtue of the fact that the group G satisfies the group axioms. In particular, eq. (16) implies that $\mathcal{I}(G)$ is closed with respect to the group multiplication law. Moreover, associativity is guaranteed because $g_1(g_2g_3) = (g_1g_2)g_3$ implies that

$$T_{g_1}(T_{g_2}T_{g_3}) = (T_{g_1}T_{g_2})T_{g_3} = T_{g_1 g_2 g_3}\,.$$

[4] One can also prove the one-to-one and onto properties directly. To prove that the homomorphism is one-to-one, one must show that

$$T_g(x) = T_g(y) \quad \Longrightarrow \quad x = y\,.$$

But, $T_g(x) = T_g(y)$ implies that $gxg^{-1} = gyg^{-1}$. Multiplying this equation on the left by g^{-1} and on the right by g then yields $x = y$. To prove that the homomorphism is onto, one must show that for all $y \in G$, there exists an $x \in G$ such that $T_g(x) = y$. In this case, it is sufficient to choose $x = g^{-1}yg$. Evaluating $T_g(x)$ for this choice,

$$T_g(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y\,,$$

as required. Thus, for any choice of $y \in G$, we have explicitly determined the required x, namely $x = g^{-1}yg$, such that $T_g(x) = y$. That is, the homomorphism maps G *onto* itself.

The identity of $\mathcal{I}(G)$ is T_e (where e is the identity element of the group G) since

$$T_g T_e = T_e T_g = T_{ge} = T_{eg} = T_g \,.$$

The inverse of T_g is $T_{g^{-1}}$, since

$$T_g T_{g^{-1}} = T_{g^{-1}} T_g = T_{gg^{-1}} = T_{g^{-1}g} = T_e \,.$$

Thus, the group axioms are satisfied, which implies that $\mathcal{I}(G)$ is a group.

(c) Show that $\mathcal{I}(G) \simeq G/Z(G)$, where $Z(G)$ is the center of G.

The kernel of the map $f : G \longrightarrow G'$ is defined by

$$K \equiv \ker\, f = \{g \in G \,|\, f(g) = e'\}\,,$$

where G' is the image of f and e' is the identity element of G'. Introduce the two homomorphisms,

$$\begin{array}{ll} \phi : G \longrightarrow G/K & \text{given by } \phi(g) = gK\,, \\ \psi : G/K \longrightarrow G' & \text{given by } \psi(gK) = f(g)\,. \end{array}$$

It follows that $\psi{\cdot}\phi(g) = f(g)$. It is straightforward to show that ψ is an isomorphism, in which case we can identify

$$G' \cong G/K\,. \tag{17}$$

This result can be represented diagrammatically by:

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\phi"'] & & G' \arrow[dl, "\psi"] \\ & G/K & \end{tikzcd}$$

Consider the homomorphism,

$$f : G \longrightarrow \mathcal{I}(G) \quad \text{given by } f(g) = T_g\,.$$

Note that f is onto, i.e. $\mathcal{I}(G)$ is the image of f. The kernel of f is

$$K = \{g \in G\} \,|\, f(g) = T_e\}\,,$$

where T_e is the identity element of $\mathcal{I}(G)$, i.e. $T_e(x) = x$. Thus, K consists of all elements of G satisfying $T_g = T_e$, or equivalently, $gxg^{-1} = x$, which implies that $gx = xg$ for all $x \in G$. We recognize this as the center of G, denoted by $Z(G)$ in problem 4. Using eq. (17), it follows that

$$\mathcal{I}(G) \cong G/Z(G)\,. \tag{18}$$

(d) Show that the set of all automorphisms of G, denoted by $\mathcal{A}(G)$, is a group and that $\mathcal{I}(G)$ is a normal subgroup. (The factor group $\mathcal{A}(G)/\mathcal{I}(G)$ is called the group of *outer automorphisms* of G.)

Let $\mathcal{A}(G)$ be the set of all automorphisms of G. To show that this is a group, we must define the group multiplication law. As in the case of part (b), we define

$$A_1A_2(g) = A_1(A_2(g))\,, \quad \text{for } A_1, A_2 \in \mathcal{A} \text{ and } g \in G\,.$$

That is the multiplication law is simply the composition of maps. It is straightforward to verify that the group axioms are satisfied. Note that since an automorphism is one-to-one and onto, each element of $\mathcal{A}(G)$ possesses a unique inverse. Next, we demonstrate that the set of inner automorphisms, $\{T_g \,|\, g \in G\}$, forms a normal subgroup of $\mathcal{A}(G)$. To do this, one must show that

$$AT_gA^{-1} \in \mathcal{I}(G)\,, \quad \text{for all } A \in \mathcal{A}(G)\,.$$

Consider,

$$\begin{aligned} AT_gA^{-1}(x) &= AT_g(A^{-1}(x)) = A(gA^{-1}(x)g^{-1}) \\ &= A(g)A(A^{-1}(x))A(g^{-1}) = A(g)xA^{-1}(g) \\ &= T_{A(g)}(x)\,, \end{aligned} \tag{19}$$

where we have used the fact that A is a homomorphism, which therefore satisfies

$$A(g_1g_2) = A(g_1)A(g_2) \quad \text{and} \quad A(g^{-1}) = A^{-1}(g)\,, \qquad \text{for any } g, g_1, g_2 \in G\,. \tag{20}$$

It follows that

$$AT_gA^{-1} = T_{A(g)} \in \mathcal{I}(G)\,.$$

(e) Illustrate these results for $G = S_3$ and $G = \mathbb{Z}$.

We now illustrates the above results in three specific examples.

(i) $G = S_3$

First we note that the center of S_3 contains only the identity. This is easily seen by examining the group multiplication table of S_3 and observing that no element other than the identity commutes with all the elements of S_3. Thus, the center $Z(S_3)$ is trivial, and we conclude that $\mathcal{I}(S_3) \cong S_3$.

What are these inner automorphisms? Since the mapping $T_g(x) = gxg^{-1}$ is an inner automorphism, we see that x and $T_g(x)$ are related by conjugation and thus are in the same conjugacy class. In class, I showed that elements of S_n that appear in the same conjugacy class possess the same cycle structure. Applying this result to S_3, it follow that if x is a transposition, then so is $T_g(x)$. Indeed, if I specify how T_g acts on the transpositions, then the corresponding inner automorphism is uniquely specified since the product of any pair of transpositions is given by either (123) or (132). Thus using the group multiplication table of S_3 along with eq. (15), the values of $T_g\big((12)\big)$, $T_g\big((13)\big)$ and $T_g\big((23)\big)$ determine how T_g acts on (123) and (132).[5] Since there are three possible transpositions, this yields $3! = 6$ possible inner automorphisms corresponding to the six possible choices for the three quantities, $T_g\big((12)\big)$, $T_g\big((13)\big)$ and $T_g\big((23)\big)$.

Are there any automorphisms of S_3 that are not inner automorphisms? Any such mapping must map one of the transpositions to either (123) of (132).[6] But, the square of a transposition is the identity, whereas the square of (123) is (132) and vice versa. Thus, such a mapping cannot be an automorphism, as it does not preserve the group multiplication table. Hence, we conclude that $\mathcal{A}(S_3) = \mathcal{I}(S_3) \cong S_3$, in which case the group of outer automorphisms is trivial.

(ii) $G = \mathbb{Z}$

First, we note that $\mathcal{I}(Z)$ is trivial since $\mathbb{Z}$ is abelian. Also, since $\mathbb{Z}$ is a cyclic group, the set of maps $f : \mathbb{Z} \to \mathbb{Z}$ is in one-to-one correspondence with the set of possible values of $f(1)$. If f is a homomorphism, then it must satisfy $f(0) = 0$ and

$$f(k) = f(\underbrace{1 + 1 + \ldots + 1}_{k}) = \underbrace{f(1) + f(1) + \ldots + f(1)}_{k} = kf(1)\,, \tag{21}$$

for any integer k. An automorphism is a homomorphism $f : G \to G$ that is one-to-one and onto. If $f(1) \neq 0$ then $\ker f = \{0\}$, since the identity is the only element of G that is mapped to the identity, in which case it follows that f is a one-to-one map. We now demonstrate that f is an onto map if and only if $f(1) = \pm 1$. First, the homomorphism corresponding to $f(1) = 1$ is the identity map which is one-to-one and onto. Next, eq. (21) implies that the homomorphism corresponding to $f(1) = -1$ is:

$$f : \mathbb{Z} \longrightarrow \mathbb{Z} \quad \text{given by } f(n) = -n \text{ for } n \in \mathbb{Z}\,,$$

which is also one-to-one and onto. For any other integer choice of $f(1) = k \neq \pm 1$, the corresponding map is not onto. In particular, the equation $f(n) = 1$ has no solution for $n \in \mathbb{Z}$. Thus we conclude that the only possible automorphisms $f : \mathbb{Z} \to \mathbb{Z}$ are the maps $f(n) = \pm n$ for $n \in \mathbb{Z}$. Since the set of automorphisms forms a group, as shown in part (d), it follows that $\mathcal{A}(\mathbb{Z})$ is a discrete group of two elements. Only one such group exists, and we conclude that

$$\mathcal{A}(\mathbb{Z}) = \mathbb{Z}_2\,.$$

Since $\mathcal{I}(\mathbb{Z})$ is trivial, it follows that the group of outer automorphisms of the integers is $\mathbb{Z}_2$.

[5] Of course, in light of eq. (15) where $x = e$, it follows that $T_g(e) = e$ for any automorphism T_g.

[6] Only the identity e is mapped onto e by an automorphism, for the same reason cited in the previous footnote.

6. Consider an arbitrary orthogonal matrix R, which satisfies $RR^{\mathsf{T}} = \mathbb{1}$ (where $\mathbb{1}$ is the identity matrix).

(a) Prove that the possible values of $\det R$ are ± 1.

Using the fact that $\det R^{\mathsf{T}} = \det R$, it follows that

$$\det(RR^{\mathsf{T}}) = (\det R)(\det R^{\mathsf{T}}) = [\det R]^2 = 1\,, \tag{22}$$

since $RR^{\mathsf{T}} = \mathbb{1}$ implies that $\det(RR^{\mathsf{T}}) = \det \mathbb{1} = 1$. Taking the square root of eq. (22) yields $\det R = \pm 1$

(b) The group SO(2) consists of all 2×2 orthogonal matrices with unit determinant. Prove that SO(2) is an abelian group.

Suppose that $Q \in \mathrm{SO}(2)$. If we parameterize

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

then we can find relations among the parameters a, b, c and d by imposing the conditions $Q^{\mathsf{T}}Q = \mathbb{1}$ and $\det Q = 1$. That is,

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\,,$$

and $\det Q = ad - bc = 1$. Hence, the relations among the parameters a, b, c and d are determined by the following conditions,

$$a^2 + c^2 = b^2 + d^2 = 1\,, \qquad ab + cd = 0\,, \qquad ad - bc = 1\,. \tag{23}$$

We now consider two cases. First if $c \neq 0$, it follows that $d = -ab/c$. Inserting this result back into eq. (23) yields

$$1 = ad - bc = -\frac{a^2 b}{c} - bc = -\frac{b}{c}\left(a^2 + c^2\right) = -\frac{b}{c}\,,$$

after using eq. (23). That is, $c = -b$. It immediately follows that $d = -ab/c = a$, and we conclude that the most general SO(2) matrix is given by

$$Q = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\,.$$

In light of eq. (23), $c = -b$ yields $a^2 + b^2 = 1$, which implies that $-1 \leq a, b \leq 1$. Thus, it is convenient to parameterize a and b by defining $a = \cos\theta$ and $b = \sin\theta$. Hence, the most general SO(2) matrix is given by

$$Q = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\,, \tag{24}$$

where $0 \leq \theta < 2\pi$.

Next, we examine the case of $c = 0$. In this case, eq. (23) yields $a^2 = 1$, $ab = 0$, and $ad = 1$. It follows that $b = 0$ and $a = d = \pm 1$. Hence the form for Q in this case (where $a = d = \pm 1$ and $b = c = 0$) is consistent with eq. (24).

It is now a simple matter to check that any two elements of SO(2) of the form given in eq. (24) commute. In particular,

$$\begin{pmatrix} \cos\theta_1 & \sin\theta_1 \\ -\sin\theta_1 & \cos\theta_1 \end{pmatrix} \begin{pmatrix} \cos\theta_2 & \sin\theta_2 \\ -\sin\theta_2 & \cos\theta_2 \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 & \sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2 \\ -\sin\theta_1\cos\theta_2 - \cos\theta_1\sin\theta_2 & \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\theta_1+\theta_2) & \sin(\theta_1+\theta_2 \\ -\sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2) \end{pmatrix}.$$

Clearly, if we interchange θ_1 and θ_2, we recover the same result. Hence, all products of SO(2) elements are commutative, and we conclude that SO(2) is an abelian group.

(c) The group O(2) consists of all 2×2 orthogonal matrices, with no restriction on the sign of its determinant. Is O(2) abelian or non-abelian? (If the latter, exhibit two O(2) matrices that do not commute.)

The matrix Q given in eq. (24) is also an element of O(2). An element of O(2) that is not an element of SO(2) is

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

But this matrix does not commute with Q. In particular,

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix},$$

whereas

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Hence, we conclude that O(2) is a non-abelian group.