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:

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

$$(x_1, y_1) \bullet (x_2, y_2) = (x_1x_2, y_1y_2)\,. \tag{2}$$

(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)]. Note that since addition is commutative, $\mathbb{R}^2$ an abelian group under addition. $\mathbb{R}^2$ is not a group under multiplication. For example, $(0, 0)$ does not possess a multiplicative inverse.

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

$\mathbb{R}^2$ is a ring with respect to addition and multiplication as specified by eqs. (1) and (2). From part (a), R^2 is an abelian group under addition. It also satisfies the conditions of closure and associativity with respect to multiplication. Moreover, the multiplicative identity is $\mathbb{1} = (1, 1)$. Finally, it is straightforward to check that multiplication is distributive over addition.

(c) 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.

(d) 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 $\mathbb{R}$.

(e) Is $\mathbb{R}^2$ an algebra (over $\mathbb{R}$)?

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

Suppose that the multiplication law given by eq. (2) is replaced by

$$(x_1, y_1) \bullet (x_2, y_2) = \, (x_1x_2 - y_1y_2 \, , \, x_1y_2 + x_2y_1) \, . \tag{3}$$

Do any of the results obtained in parts (a)–(e) above change? Identify a well know mathematical object that is isomorphic to $\mathbb{R}^2$ if eq. (2) is replaced by eq. (3).

The only results that change are the answers to parts (b), (c) and (e) above. If we employ eq. (3) instead of eq. (2) for the multiplication rule, then the multiplicative identity is now identified as $\mathbb{1} = (1, 0)$, since $(x, y) \bullet (1, 0) = (x, y)$. Thus, $\mathbb{R}^2$ is still a ring with the new multiplication law. Moreover, all the axioms for a field are now satisfied. In particular, one can now show that the multiplicative inverse of (x, y) is given by,

$$(x,y)^{-1} = \left(\frac{x}{x^2+y^2} \, , \, -\frac{y}{x^2+y^2} \right) \, , \qquad \text{for any } (x,y) \neq (0,0).$$

Indeed, it is a simple exercise to check that $(x, y)^{-1} \bullet (x, y) = (1, 0)$ using the multiplicative law given by eq. (3).

In light of the addition and multiplication laws specified by eqs. (1) and (3), we can identify $\mathbb{R}^2 \cong \mathbb{C}$, which is the field of complex numbers. That is, the map $f : \mathbb{R}^2 \longrightarrow \mathbb{C}$ defined by $f(x, y) = x+iy$ is an isomorphism. In particular, one can easily check that eqs. (1) and (3) are preserved by this map, since complex addition and multiplication is given by,

$$(x_1 + iy_1) + (x_2 + iy_2) = x_1 + x_2 + i(y_1 + y_2) \, ,$$

$$(x_1 + iy_1) \bullet (x_2 + iy_2) = x_1x_2 - y_1y_2 + i(x_1y_2 + x_2y_1) \, .$$

Finally $\mathbb{R}^2 \cong \mathbb{C}$ is both a vector space over $\mathbb{R}$ and an algebra over $\mathbb{R}$. In particular, the complex numbers $\mathbb{C}$ can be regarded as the vector space $\mathbb{R}^2$ over the field $\mathbb{R}$, where the vectors are $v = x\hat{\boldsymbol{e}}_0 + y\hat{\boldsymbol{e}}_1$, with x, $y \in \mathbb{R}$. We can identify $\hat{\boldsymbol{e}}_0$ as the identity element. The vector product is then determined by defining $\hat{\boldsymbol{e}}_1 \times \hat{\boldsymbol{e}}_1 = -\hat{\boldsymbol{e}}_0$. The inverse is $v^{-1} = \big(x\hat{\boldsymbol{e}}_0 - y\hat{\boldsymbol{e}}_1\big)/\|v\|^2$ (for $v \neq 0$), where the squared norm of the vector $\|v\|^2 \equiv x^2 + y^2$.

2. The permutation group S_n has $n!$ elements. Consider the alternating group A_n consisting of the even permutations of n objects.

(a) Prove that there are an equal number of even and odd permutations of n objects if $n \geq 2$. This result then shows that the order of A_n is $\frac{1}{2}n!$ for $n \geq 2$.

Consider a fixed permutation corresponding to the 2-cycle (12). Denoting O_n as the set of odd permutations of n objects, consider the map $f : A_n \to O_n$, such that $f(\tau) = (12) \cdot \tau$, where $\tau \in A_n$. Since the permutation τ is an even permutation, it follows that $(12) \cdot \tau$ is an odd permutation. Moreover, every odd permutation is the product of an odd number of transpositions. Since $(12)(12) = \mathbb{1}$, one can multiply any odd permutation by (12)(12) on the left without changing it. Hence, every odd permutation is the product of (12) and an even number of transpositions. That is, the function f is surjective (onto).

Next, suppose that τ, $\sigma \in A_n$, and $f(\tau) = f(\sigma)$. It then follows that $(12)\tau = (12)\sigma$. Multiplying this equation on the left by (12) yields $\tau = \sigma$. That is, the map f is injective (one-to-one).

A map that is both surjective and injective is bijective. It follows that A_n and O_n have the same number of elements, since f maps each element of A_n uniquely into an element of O_n and all elements of O_n are the result of some $f(\tau)$. Since the permutation group S_n has $n!$ elements, it follows that A_n has $\frac{1}{2}n!$ elements.

(b) What goes wrong with your proof of part (a) in the case of $n = 1$?

If $n = 1$, then the group S_1 has one element, the identity $\mathbb{1}$, which is an even permutation. No odd permutation exists so the proof provided in part (a) no longer applies.

(c) Prove that the sign of a cyclic permutation in S_n is $(-1)^{n-1}$.

A cyclic permutation in S_n is an n-cycle that is either of the form

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

or of the form

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & 1 & \cdots & n-2 & n-1 \end{pmatrix} = (1\ n\ n-1 \cdots 3\ 2) = (1\ n)(n\ n-1)\cdots(3\ 2)\,, \tag{5}$$

after making use of Theorem 1.7 of Haber and Terning. These results imply that a cyclic permutation of S_n can be expressed as the product of $n-1$ transpositions. Since each transposition is an odd permutation, it follows that the sign of any cyclic permutation in S_n is $(-1)^{n-1}$.

3. Consider the possibility that a set G of $n \times n$ matrices forms a group with respect to matrix multiplication.

(a) Prove that if G is a group and if one of the elements of G is a non-singular matrix then all of the elements of G must be non-singular matrices. Conclude that all the elements of G are either non-singular matrices or singular matrices.

Let $G = \{A_0, A_1, A_2, \ldots\}$ be a group of $n \times n$ matrices, where $A_0 \equiv \mathbb{1}$ is the group identity element.[1] First, suppose that the identity element A_0 is a non-singular matrix, in which case $\det A_0 \neq 0$. Then consider

$$A_i B_i = A_0\,, \qquad \text{for } i \neq 0 \text{ (no sum over } i)\,, \tag{6}$$

[1]The group G may be a discrete or continuous group of matrices.

where B_i is the group inverse of A_i. Taking the determinant of both sides of eq. (6), it follows that $\det A_i \neq 0$ and $\det B_i \neq 0$, since the determinant of an $n \times n$ matrix is finite. That is, A_i is a non-singular matrix for all i. Hence, if the identity element is a non-singular matrix, then all the elements of G are non-singular matrices.

Next, suppose that the identity element A_0 is a singular matrix, in which case $\det A_0 = 0$. Since A_0 is the group identity element, it follows that

$$A_i A_0 = A_i\,, \qquad \text{for any } i \neq 0\,. \tag{7}$$

Taking the determinant of both sides of eq. (7), it follows that $\det A_i = 0$ for all i. Hence, if the identity element is a singular matrix, then all the elements of G are singular matrices.

<u>*REMARKS:*</u>

1. In the case where all elements of G are non-singular matrices, then we can multiply both sides of eq. (7) by the matrix inverse A_i^{-1} to conclude that $A_0 = \mathbb{1}_{n\times n}$, where $\mathbb{1}_{n\times n}$ is the $n \times n$ identity matrix. In the case where all the elements of G are singular matrices, then A_0 *cannot* be the identity matrix (since $\mathbb{1}_{n\times n}$ is non-singular).

2. One can shorten the above proof by proving directly that if *any* element of G is singular then all elements of G are singular. Suppose $x \in G$ is a singular matrix, in which case $\det x = 0$. Consider any other element $y \in G$ where $y \neq x$. Then by writing $y = x(x^{-1}y)$ and taking the determinant of both sides of this equation, it follows that

$$\det y = \det x \ \det(x^{-1}y) = 0\,.$$

Hence, if any element of G is a singular matrix then all elements of G are singular matrices. An immediate consequence of this result is that if any element of G is a non-singular matrix then all elements of G must be non-singular matrices.

(b) Consider the set of 2×2 singular matrices G of the form

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix}, \tag{8}$$

where $x \in \mathbb{R}$ and $x \neq 0$. Prove that G is a group with respect to matrix multiplication. Determine the matrix corresponding to the identity element of G. Determine the inverse of the element specified in eq. (8).

Observe that

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} z & z \\ z & z \end{pmatrix}, \qquad \text{where } z = 2xy\,.$$

This demonstrates that the elements of G satisfy closure on matrix multiplication. Next, we note that

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix},$$

which implies that

$$\mathbb{1} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} , \tag{9}$$

is the identity element. Finally,

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix} \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} ,$$

which implies that the group inverse of the element specified in eq. (8) is

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} . \tag{10}$$

(c) The group defined in part (b) is isomorphic to a well known group. Identify this group.

Consider the function from $G \to \mathbb{R}^*$ that maps the elements

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix} \quad \longmapsto \quad 2x \,, \qquad \text{for all } x \in \mathbb{R}^* \,, \tag{11}$$

where $\mathbb{R}^* \equiv \mathbb{R}^0 - \{0\}$ is the group of non-zero real numbers with respect to multiplication. This map is an isomorphism. It is easy to check that the group multiplication law is preserved, since

$$\begin{pmatrix} \frac{1}{2}x & \frac{1}{2}x \\ \frac{1}{2}x & \frac{1}{2}x \end{pmatrix} \begin{pmatrix} \frac{1}{2}y & \frac{1}{2}y \\ \frac{1}{2}y & \frac{1}{2}y \end{pmatrix} = \begin{pmatrix} \frac{1}{2}xy & \frac{1}{2}xy \\ \frac{1}{2}xy & \frac{1}{2}xy \end{pmatrix} \quad \longmapsto \quad (x)(y) = xy \,,$$

is in one-to-one correspondence with multiplication in $\mathbb{R}^*$. Moreover, the identity [eq. (9)] maps to 1, which is the identity of $\mathbb{R}^*$. Finally, the inverse given in eq. (10) is mapped by eq. (11) to $1/(2x)$, which is the inverse of $2x$ in $\mathbb{R}^*$. We conclude that $G \cong \mathbb{R}^*$.

We can see the isomorphism more explicitly by considering the equivalent representation,

$$S^{-1} \begin{pmatrix} x & x \\ x & x \end{pmatrix} S \,, \qquad \text{where } S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} ,$$

A straightforward computation yields

$$\frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x & x \\ x & x \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2x & 0 \\ 0 & 0 \end{pmatrix} .$$

Thus, the matrix representation given in eq. (8) is completely reducible and is the direct sum of two one dimensional representations. We can simply discard the zeros, which leaves a one-dimensional representation that is isomorphic to $\mathbb{R}^*$ with the map given by eq. (11).

4. 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

$$\det(RR^{\mathsf{T}}) = (\det R)(\det R^{\mathsf{T}}) = [\det R]^2 = 1\,, \tag{12}$$

since $RR^{\mathsf{T}} = \mathbb{1}$ implies that $\det(RR^{\mathsf{T}}) = \det \mathbb{1} = 1$. Taking the square root of eq. (12) 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,

$$a^2 + c^2 = b^2 + d^2 = 1\,, \qquad ab + cd = 0\,, \qquad ad - bc = 1\,. \tag{13}$$

We now consider two cases. First if $c \neq 0$, it follows that $d = -ab/c$. Inserting this result back into eq. (13) 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. (13). 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. (13), $c = -b$ 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

$$Q = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\,, \tag{14}$$

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

Next, we examine the case of $c = 0$. In this case, eq. (13) 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. (14).

It is now a simple matter to show that SO(2) is a group and any two elements of SO(2) of the form given in eq. (14) commute. In particular,

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

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

$$= \begin{pmatrix} \cos(\theta_1+\theta_2) & \sin(\theta_1+\theta_2 \\ -\sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2) \end{pmatrix} . \tag{15}$$

The form of the group multiplication law given above exhibits closure. The identity corresponds to taking $\theta = 0$ in eq. (14), and the inverse of Q is obtained by taking $\theta \to -\theta$. The multiplication law for real matrices is associative. Finally, if we interchange θ_1 and θ_2 in eq. (15), 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. (14) 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.

<u>*REMARK*</u>:

Note that SO(2) is a normal subgroup of O(2). To prove this result, consider the homomorphism, $f : \mathrm{O}(2) \longrightarrow \{+1\,, -1\}$, which is defined by $f(A) = \det A$, for $A \in \mathrm{O}(2)$. The kernel of f is SO(2), since the latter corresponds to the set of all elements of O(2) with determinant equal to one. Hence, $\mathrm{O}(2)/\mathrm{kef}\ f \cong \{+1\,,\,-1\}$. Since we can identify $\mathbb{Z}_2 = \{+1\,,\,-1\}$ where the group operation is ordinary multiplication, we can conclude that $\mathrm{O}(2)/\mathrm{SO}(2) \cong \mathbb{Z}_2$.

However, it does *not* follow that $\mathrm{O}(2) \cong \mathrm{SO}(2) \times \mathbb{Z}_2$. Indeed, $\mathrm{O}(2)$ is a nonabelian group whereas $\mathrm{SO}(2) \times \mathbb{Z}_2$ is an abelian group. Nevertheless, it is true that $\mathrm{O}(2)$ is a semidirect product,

$$\mathrm{O}(2) \cong \mathrm{SO}(2) \rtimes \mathbb{Z}_2\,.$$

To show this, we simply need to exhibit a $\mathbb{Z}_2$ subgroup of $\mathrm{O}(2)$ such that $\mathrm{SO}(2) \cap \mathbb{Z}_2 = \{e\}$, where e is the identity element of $\mathrm{O}(2)$. A possible choice for the $\mathbb{Z}_2$ subgroup of $\mathrm{O}(2)$ that satisfies this requirement is,

$$\mathbb{Z}_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

One can easily verify that this $\mathbb{Z}_2$ subgroup is not a normal subgroup of $\mathrm{O}(2)$. In particular, $g\mathbb{Z}_2 g^{-1} \neq \mathbb{Z}_2$ for all $g \in \mathrm{O}(2)$, as one can easily check.

5. Consider the dihedral group D_4.

(a) Write down the group multiplication table.

The elements of D_4 are defined by:

$$D_4 = \{1, r, r^2, r^3, f, rf, r^2 f, r^3 f\}\,,$$

where the elements satisfy the relations,

$$r^4 = f^2 = 1 \quad \text{and} \quad fr = r^3 f\,. \tag{16}$$

We have used the notation $e \equiv 1$ to define the identity element of D_4.

Using eq. (16), the group multiplication table is immediately obtained:

	1	r	r^2	r^3	f	rf	r^2f	r^3f
1	1	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	1	rf	r^2f	r^3f	f
r^2	r^2	r^3	1	r	r^2f	r^3f	f	rf
r^3	r^3	1	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	1	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	1	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	1	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	1

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

There are eight proper subgroups of D_4:

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

Among these subgroups, four are normal subgroups:

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

Finally, we enumerate the classes:

$$\mathcal{C}_1=\{1\}\,,\quad \mathcal{C}_2=\{r,r^3\}\,,\quad \mathcal{C}_3=\{r^2\}\,,\quad \mathcal{C}_4=\{f,r^2f\}\quad\text{and}\quad \mathcal{C}_5=\{rf,r^3f\}\,. \tag{17}$$

REMARK:

Theorem 3.4 of Haber and Terning states 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.

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

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

$$D_4/\mathbb{Z}_2\cong D_2\,,\qquad D_4/\mathbb{Z}_4\cong\mathbb{Z}_2\,,\qquad D_4/D_2\cong\mathbb{Z}_2\,. \tag{18}$$

The last two quotient groups are identified uniquely as $\mathbb{Z}_2$, since this is the only group of two elements. The identification of the first quotient group is non-trivial, since there are two possible groups of order four—D_2 (also known as K_4) and $\mathbb{Z}_4$. Note that $D_2\cong\mathbb{Z}_2\times\mathbb{Z}_2$ is *not* a cyclic group, whereas $\mathbb{Z}_4$ 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,

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

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 $D_4/\mathbb{Z}_2$ yield the identity element, which is *not* in general satisfied by the elements of $\mathbb{Z}_4$.

In light of eq. (18), the only possible candidates for writing D_4 as a direct product of its subgroups are $\mathbb{Z}_2\times D_2$ or $\mathbb{Z}_2\times\mathbb{Z}_4$. 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. However, D_4 can be expressed as a semidirect product of its subgroups in two different ways,

$$D_4\cong\mathbb{Z}_4\rtimes\mathbb{Z}_2\cong D_2\rtimes\mathbb{Z}_2\,. \tag{19}$$

If we take $D_2 = \{1, r^2, rf, r^3f\}$, then we identify $\mathbb{Z}_2 = \{1, f\}$ in both semidirect products of eq. (19).[2] Note that D_4 cannot be written as $\mathbb{Z}_2 \rtimes D_2$, since the first group of the semidirect 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_1g_2, with $g_1 \in \mathbb{Z}_2 = \{1, r^2\}$ and $g_2 \in D_2$.

(d) Write out the conjugacy class multiplication table.

The conjugacy classes of D_4 were given in eq. (17). Using the multiplication table of D_4 given in part (a), one immediately 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 obtained in part (a) 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	f	rf	r^2f	r^3f
1	1	r^3	r^2	r	f	rf	r^2f	r^3f
r	r	1	r^3	r^2	rf	r^2f	r^3f	f
r^2	r^2	r	1	r^3	r^2f	r^3f	f	rf
r^3	r^3	r^2	r	1	r^3f	f	rf	r^2f
f	f	rf	r^2f	r^3f	1	r^3	r^2	r
rf	rf	r^2f	r^3f	f	r	1	r^3	r^2
r^2f	r^2f	r^3f	f	rf	r^2	r	1	r^3
r^3f	r^3f	f	rf	r^2f	r^3	r^2	r	1

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

[2]If $D_2 = \{1, r^2, f, r^2f\}$ then we identify $\mathbb{Z}_2 = \{1, rf\}$ in the second semidirect product in eq. (19).

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

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

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

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

6. 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,

$$Z(G) = \{z \in G \mid zg = gz\,, \text{for all } g \in G\}. \tag{20}$$

(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:

$$\begin{aligned}
&\text{(i)} \quad z_1,\, z_2 \in Z(G) \quad \Longrightarrow \quad z_1 z_2 \in Z(G), \\
&\text{(ii)} \quad e \in Z(G), \quad \text{where } e \text{ is the identity}, \\
&\text{(iii)} \quad z \in Z(G) \quad \Longrightarrow \quad z^{-1} \in Z(G).
\end{aligned}$$

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

$$z_1 g = g z_1\,, \qquad \text{for all } g \in G, \tag{21}$$

$$z_2 g = g z_2\,, \qquad \text{for all } g \in G. \tag{22}$$

Multiply eq. (21) on the right by z_2 to obtain

$$z_1 g z_2 = g z_1 z_2\,. \tag{23}$$

Then, use eq. (22) to write $z_1 g z_2 = z_1 z_2 g$. Then, eq. (23) 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

$$g^{-1} z = z g^{-1}\,, \quad \text{for all } g \in G\,. \tag{24}$$

Taking the inverse of eq. (24) 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. (21) is satisfied. In particular, choosing $g = z_2$ in eq. (21), 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 $gzg^{-1} = zgg^{-1} = z \in Z(G)$ 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 $D_4 \cong [D_4/Z(D_4)] \times Z(D_4)$ is valid.

The multiplication table for D_4 was given in part (a) of problem 5. 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:

$$\begin{aligned} \mathbb{Z}_2 &= \{e, r^2\} \,, \qquad & r\mathbb{Z}_2 &= \{r, r^3\} \,, \\ f\mathbb{Z}_2 &= \{f, r^2 f\} \qquad & rf\mathbb{Z}_2 &= \{rf, r^3 f\} \,, \end{aligned}$$

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

$$D_4/\mathbb{Z}_2 = \biggl\{ \{e, r^2\} \,,\, \{r, r^3\} \,,\, \{f, r^2 f\} \,,\, \{rf, r^3 f\} \biggr\} \,.$$

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

	$\{e, r^2\}$	$\{r, r^3\}$	$\{f, r^2 f\}$	$\{rf, r^3 f\}$
$\{e, r^2\}$	$\{e, r^2\}$	$\{r, r^3\}$	$\{f, r^2 f\}$	$\{rf, r^3 f\}$
$\{r, r^3\}$	$\{r, r^3\}$	$\{e, r^2\}$	$\{rf, r^3 f\}$	$\{f, r^2 f\}$
$\{f, r^2 f\}$	$\{f, r^2 f\}$	$\{rf, r^3 f\}$	$\{e, r^2\}$	$\{r, r^3\}$
$\{rf, r^3 f\}$	$\{rf, r^3 f\}$	$\{f, r^2 f\}$	$\{r, r^3\}$	$\{e, r^2\}$

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 $D_4 \cong [D_4/Z(D_4)] \times Z(D_4)$ were valid, then

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

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 $D_2 \times \mathbb{Z}_2$ is abelian, which means that this group cannot be isomorphic to the nonabelian group D_4.

7. 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

$$T_g(x)T_g(y) = T_g(xy)\,, \qquad \text{for all } x, y \in G\,. \tag{25}$$

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.[3] 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 $\mathrm{Inn}(G)$, is a group.

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

$$T_{g_1}T_{g_2}(x) = T_{g_1}(g_2xg_2^{-1}) = g_1g_2xg_2^{-1}g_1^{-1} = (g_1g_2)x(g_1g_2)^{-1} = T_{g_1g_2}(x)\,,$$

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

$$T_{g_1}T_{g_2} = T_{g_1g_2}\,. \tag{26}$$

It follows that $\mathrm{Inn}(G)$ satisfies the axioms of a group by virtue of the fact that the group G satisfies the group axioms. In particular, eq. (26) implies that $\mathrm{Inn}(G)$ 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

$$T_{g_1}(T_{g_2}T_{g_3}) = (T_{g_1}T_{g_2})T_{g_3} = T_{g_1g_2g_3}\,.$$

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

$$T_gT_e = T_eT_g = T_{ge} = T_{eg} = T_g\,.$$

[3]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 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 $\mathrm{Inn}(G)$ is a group.

(c) Show that $\mathrm{Inn}(G) \simeq G/Z(G)$, 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

$$G' \cong G/K\,. \tag{27}$$

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, $f : G \longrightarrow \mathrm{Inn}(G)$, given by $f(g) = T_g$. Note that f is onto, i.e. $\mathrm{Inn}(G)$ 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 $\mathrm{Inn}(G)$, 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. (27), it follows that

$$\mathrm{Inn}(G) \cong G/Z(G)\,. \tag{28}$$

(d) Show that the set of all automorphisms of G, denoted by $\mathrm{Aut}(G)$, is a group and that $\mathrm{Inn}(G)$ is a normal subgroup. (The quotient group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group*.[4]

[4]This nomenclature is unfortunate, since the group of outer automorphisms is *not* the same as the set of outer automorphisms, which is defined as the subset of automorphisms that are not inner. For example, since the identity automorphism is inner, it follows that the *set* of outer automorphisms is *not* a group.

Let $\mathrm{Aut}(G)$ 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

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

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 $\mathrm{Aut}(G)$ possesses a unique inverse. Next, we demonstrate that the set of inner automorphisms, $\{T_g \,|\, g \in G\}$, is a normal subgroup of $\mathrm{Aut}(G)$. To do this, one must show that $AT_gA^{-1} \in \mathrm{Inn}(G)$, for all $A \in \mathrm{Aut}(G)$. Consider,

$$\begin{aligned} AT_gA^{-1}(x) &= AT_g(A^{-1}(x)) = A(gA^{-1}(x)g^{-1}) \\ &= A(g)A(A^{-1}(x))A(g^{-1}) = A(g)xA^{-1}(g) \\ &= T_{A(g)}(x)\,, \end{aligned} \tag{29}$$

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

$$A(g_1g_2) = A(g_1)A(g_2) \quad \text{and} \quad A(g^{-1}) = A^{-1}(g)\,, \qquad \text{for any } g, g_1, g_2 \in G\,. \tag{30}$$

It follows that

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

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

We now illustrates the above results in two 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 $\mathrm{Inn}(S_3) \cong S_3$.

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. (25), 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 $T_g\big((23)\big)$.

[5]Of course, in light of eq. (25) where $x = e$, it follows that $T_g(e) = e$ for any automorphism T_g.

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 $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$, in which case the group of outer automorphisms is trivial.

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

First, we note that $\mathrm{Inn}(Z)$ 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

$$f(k) = f(\underbrace{1 + 1 + \ldots + 1}_{k}) = \underbrace{f(1) + f(1) + \ldots + f(1)}_{k} = kf(1)\,, \tag{31}$$

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. (31) 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 $\mathrm{Aut}(\mathbb{Z})$ is a discrete group of two elements. Only one such group exists, and we conclude that

$$\mathrm{Aut}(\mathbb{Z}) = \mathbb{Z}_2\,.$$

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

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