Abstract Algebra, 3rd Edition

David S. Dummit and Richard M. Foote
newell.jensen@gmail.com

Chapter 1 - Introduction to Groups

Exercises:

1.1 BASIC AXIOMS AND EXAMPLES

Let G be a group.

1. Determine which of the following binary operations are associative:

(a) the operation $*$ on $\mathbb{Z}$ defined by $a * b = a - b$

$a * (b * c) = a - (b - c) = (a - b) - c = (a * b) * c \implies$ associative

(b) the operation $*$ on $\mathbb{R}$ defined by $a * b = a + b + ab$

$a * (b * c) = a + (b + c + bc) + a(b + c + bc) = (a + b + ab) + c + (a + b + ab)c = (a * b) * c \implies$ associative

(c) the operation $*$ on $\mathbb{Q}$ defined by $a * b = \frac{a+b}{5}$

$a * (b * c) \implies \frac{5a+b+c}{25}$ while $(a * b) * c \implies \frac{a+b+5c}{25} \implies$ not associative

(d) the operation $*$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) * (c, d) = (ad + bc, bd)$

$(a, b) * ((c, d) * (e, f)) = (a, b) * (cf + de, df) = (adf + bcf + bde, bdf) = (f(ad + bc) + bd(e), bd(f)) = (ad + bc, bd) * (e, f) = ((a, b) * (c, d)) * (e, f) \implies$ associative

(e) the operation $*$ on $\mathbb{Q} - \{0\}$ defined by $a * b = \frac{a}{b}$

$a * (b * c) = \frac{a}{(\frac{b}{c})} = \frac{(\frac{a}{b})}{c} = (a * b) * c \implies$ associative

2. Decide which of the binary operations in the preceding exercise are commutative.

(a) $a = -5, b = 3 \implies a - b = -5 - 3 = -8$ while $b - a = 3 - (-5) = 8 \implies$ not commutative

(b) $a + b + ab = b + a + ba \implies$ commutative

(c) $\frac{a+b}{5} = \frac{b+a}{5} \implies$ commutative

(d) $(ad + bc, bd) = (cb + da, db) \implies$ commutative

(e) $\frac{a}{b} \neq \frac{b}{a} \implies$ not commutative

3. Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well-defined).

Proof. Suppose we have $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$. In order to show that these are associative under addition, we need to show that arbitrary representatives from these residue classes are associative under addition.

Therefore, suppose we have $a \in \overline{a}, b \in \overline{b}, c \in \overline{c}$ so that $\overline{a} * (\overline{b} * \overline{c}) \implies a + (b + c) \implies (a + b) + c \implies (\overline{a} * \overline{b}) * \overline{c}$ $\square$

4. Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well-defined).

Proof. Suppose we have $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$. In order to show that these are associative under multiplication, we need to show that arbitrary representatives from these residue classes are associative under multiplication.

Therefore, suppose we have $a \in \overline{a}, b \in \overline{b}, c \in \overline{c}$ so that $\overline{a} * (\overline{b} * \overline{c}) \implies a(bc) \implies (ab)c \implies (\overline{a} * \overline{b}) * \overline{c}$ □

5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

Proof. The residue class $\overline{0} \in \mathbb{Z}/n\mathbb{Z}$ does not have a multiplicative inverse $\overline{a}$ such that $\overline{0} * \overline{a} = \overline{1}$. Therefore, for all $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is not a group under under multiplication. □

6. Determine which of the following sets are groups under addition:

(a) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd.

0 is the additive identity, the rational numbers are associative from $\mathbb{Z}$ and additive inverses also exist. It is also closed under addition since:

$\frac{t}{2n+1} + \frac{s}{2k+1}$ for integers t, n, s, k gives us $\frac{t(2k+1)+s(2n+1)}{(2n+1)(2k+1)} \implies \frac{2(tk+sn)+t+s}{2(2nk+n+k+1)+1}$ shows us that the denominator is still an odd number.

Therefore, this is a group.

(b) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even.

0 is the additive identity, the rational numbers are associative from $\mathbb{Z}$ and additive inverses also exist. It is also closed under addition since:

$\frac{t}{2n} + \frac{s}{2k}$ for integers t, n, s, k gives us $\frac{t(2k+1)+s(2n)}{(2n)(2k)} \implies \frac{tk+sn}{2nk}$ shows us that the denominator is still an even number.

Therefore, this is a group.

(c) the set of rational numbers of absolute value < 1.

$\frac{3}{4} + \frac{3}{4} = \frac{3}{2} > 1$

Therefore, this is not a group.

(d) the set of rational numbers of absolute value ≥ 1.

0 the additive identity is not in the set.

Therefore, this is not a group.

(e) the set of rational numbers with denominators equal to 1 or 2.

0 is the additive identity ($\frac{0}{1}$), the rational numbers are associative from $\mathbb{Z}$ and additive inverses also exist. The numbers with denominator 1 are just $\mathbb{Z}$ while the numbers with denominator 2 are just $\mathbb{Z}$ divided by 2.

Therefore, this is a group.

(f) the set of rational numbers with denominators equal to 1, 2 or 3.

$\frac{5}{2} + \frac{1}{3} = \frac{17}{6}$

Therefore, this is not a group.

7. Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x*y$ be the fractional part of $x+y$ (i.e., $x*y = x+y-[x+y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $*$ is a well-defined binary operation on G and that G is an abelian group under $*$ (called the *real numbers mod 1*).

Proof. well-defined - If $x, y \in G$, then $[x+y]$ is equal to 0 or 1. If $[x+y] = 0$ then $x+y \in G$. If $[x+y] = 1$ then $1 < x+y < 2$ and $x+y-1 \in G$. Therefore $*$ maps $G \times G \to G$ and is well-defined.

associative - If $x, y, z \in G$, then

$$\begin{aligned} x*(y*z) &= x + (y*z) - [x + (y*z)] \\ &= x + (y+z-[y+z]) - [x + (y+z-[y+z])] \\ &= x+y+z-[y+z]-[x+y+z]+[y+z] \\ &= x+y+z-[x+y+z] \\ &= x+y+z-[x+y]+[x+y]-[x+y+z] \\ &= (x+y-[x+y])+z-[(x+y-[x+y])+z] \\ &= (x*y)+z-[(x*y)+z] \\ &= (x*y)*z \end{aligned}$$

identity - 0 is the identity element as $0*x = 0+x-[x+0] = x$ and $x*0 = x+0-[x+0] = x$.

inverses - if $x \in G$ then $(1-x) \in G$ and $(1-x)*x = 1-x+x-[1-x+x] = 1-[1] = 1-1 = 0$ and $x*(1-x) = x+1-x-[x+1-x] = 1-[1] = 1-1 = 0$.

commutative - $x*y = x+y-[x+y] = y+x-[y+x] = y*x$.

$(G, *)$ is an abelian group. □

8. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

Let $z_1, z_2 \in G$:

(a) Prove that G is a group under multiplication (called the group of *roots of unity in* $\mathbb{C}$).

Proof. binary relation - $z_1 * z_2 = z_1^n \cdot z_2^k = 1^n \cdot 1^k = 1$ for $n, k \in \mathbb{Z}^+$. Thus, $z_1 * z_2 \in G$.

identity - 1 is the identity element as $1 * z_1 = 1 \cdot z_1^n = 1 \cdot 1^n = 1$ and $z_1 * 1 = z_1^n \cdot 1 = 1^n \cdot 1 = 1$ and $1 \in G$.

inverses - As the elements of G are already equal to the identity they are their own inverses.

commutative - $z_1 * z_2 = 1 \cdot 1 = z_2 * z_1$.

The *roots of unity in* $\mathbb{C}$ is an abelian group. □

(b) Prove that G is not a group under addition.

Proof. $z_1 + z_2 = 1 + 1 = 2 \notin G$. □

9. Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

Let $x_1, x_2 \in G$ such that $x_1 = a_1 + b_1\sqrt{2}$ and $x_2 = a_2 + b_2\sqrt{2}$.

(a) Prove that G is a group under addition.

Proof. binary relation - $x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in G$.

identity - 0 is the additive identity for this group as $0 + x_1 = a_1 + b_1\sqrt{2}$.

inverses - $-x_1 + x_1 = -a_1 - b_1\sqrt{2} + a_1 + b_1\sqrt{2} = 0$

This is a group. □

(b) Prove that the nonzero elements of G are a group under multiplication. ["Rationalize the denominators" to find multiplicative inverses].

Proof. binary relation - $x_1x_2 = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + a_1b_2\sqrt{2} + a_2b_1\sqrt{2} + b_1b_22 = (a_1a_2 + b_1b_22) + (a_1b_2 + a_2b_1)\sqrt{2} \in G$.

identity - 1 is the multiplicative identity as $x_11 = (a_1 + b_1\sqrt{2}) \cdot 1 = x_1$.

inverses - As mentioned in the exercise lets rationalize the denominators.

$$\begin{aligned}(a + b\sqrt{(2)})(a - b\sqrt{2}) &= a^2 - 2b^2 \\ &= \frac{1}{a + b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2}\end{aligned}$$

Therefore the inverses are $(\frac{a}{a^2-2b^2}) + (\frac{-b}{a^2-2b^2})\sqrt{2}$.

This is a group. □

10. Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

This table is called a *Cayley table* after the British mathematician Arthur Cayley. We will leave it to the reader to complete this proof.

11. Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

$$\begin{aligned}|\overline{0}| &= 1 \\ |\overline{1}| &= 12 \\ |\overline{2}| &= 6 \\ |\overline{3}| &= 4 \\ |\overline{4}| &= 3 \\ |\overline{5}| &= 12 \\ |\overline{6}| &= 2 \\ |\overline{7}| &= 12 \\ |\overline{8}| &= 3\end{aligned}$$

$$|\overline{9}| = 4$$
$$|\overline{10}| = 6$$
$$|\overline{11}| = 12$$

12. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times : \overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}$

$$|\overline{1}| = 1$$
$$|\overline{-1}| = 2$$
$$|\overline{5}| = 12$$
$$|\overline{7}| = 12$$
$$|\overline{-7}| = 12$$
$$|\overline{13}| = 1$$

13. Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z} : \overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

$$|\overline{1}| = 36$$
$$|\overline{2}| = 18$$
$$|\overline{6}| = 6$$
$$|\overline{9}| = 4$$
$$|\overline{10}| = 18$$
$$|\overline{12}| = 3$$
$$|\overline{-1}| = 36$$
$$|\overline{-10}| = 18$$
$$|\overline{-18}| = 2$$

14. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times : \overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

$$|\overline{1}| = 1$$
$$|\overline{-1}| = 2$$
$$|\overline{5}| = 6$$
$$|\overline{13}| = 3$$
$$|\overline{-13}| = 6$$
$$|\overline{17}| = 2$$

15. Prove that $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$ for all $a_1, a_2, \dots, a_n \in G$.

Proof. base case - from Proposition 1(4) we know that $(a * b)^{-1} = (b^{-1}) * (a^{-1})$

induction hypothesis - assume that $(a_1 a_2 \dots a_{n-1})^{-1} = a_{n-1}^{-1} \dots a_1^{-1}$ holds up to $n-1$.

induction step - Let $a = (a_1 a_2 \dots a_{n-1})$ and $b = (a_n)$, then

$$\begin{aligned} (a * b)^{-1} &= (b^{-1}) * (a^{-1}) && \text{[base case]} \\ &= ((a_1 a_2 \dots a_{n-1})(a_n))^{-1} \end{aligned}$$

$$= (a_n^{-1})((a_1 a_2 \dots a_{n-1})^{-1})$$
$$= (a_n^{-1})((a_{n-1}^{-1} \dots a_1^{-1}) \qquad \text{[induction hypothesis]}$$

Therefore, $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$ for all $a_1, a_2, \dots, a_n \in G$. □

16. Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

Proof. If $x^2 = 1$ then either $x = -1$ or $x = 1$. If $x = -1$ then $x^2 = (-1)(-1) = 1$ and $|-1| = 2$. If $x = 1$ then $1^1 = 1$ and $|1| = 1$. Therefore $|x|$ is either 1 or 2.

Conversely if $|x|$ is either 1 or 2 then let $|x| = 1$. An element of a group has order 1 if and only if it is the identity thus $x = 1$ [Example 1 after Proposition 2]. If $|x| = 2$ then since in multiplicative groups $\mathbb{R} - \{0\}$ or $\mathbb{Q} - \{0\}$ the element -1 has order 2 and all other non-identity elements have infinite order [Example 3 after Proposition 2].

Therefore, $x^2 = 1$. □

17. Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

Proof. If $|x| = n$ then

$$\begin{aligned} 1 &= x^n \\ 1 &= x^1 x^{n-1} \\ x^{-1}1 &= x^{-1}x^1 x^{n-1} \\ x^{-1} &= 1x^{n-1} \\ x^{-1} &= x^{n-1} \end{aligned}$$

Therefore, if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$. □

18. Let x and y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

Proof. If $xy = yx$ then

$$\begin{aligned} y^{-1}xy &= y^{-1}yx \\ y^{-1}xy &= 1x \\ y^{-1}xy &= x \\ x^{-1}y^{-1}xy &= x^{-1}x \\ x^{-1}y^{-1}xy &= 1 \end{aligned}$$

Now to prove the converse direction, if $x^{-1}y^{-1}xy = 1$ then

$$\begin{aligned} x^1 x^{-1}y^{-1}xy &= x \\ 1y^{-1}xy &= x \\ y^{-1}xy &= x \\ yy^{-1}xy &= yx \\ 1xy &= yx \\ xy &= yx \end{aligned}$$

Therefore, $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$. □

19. Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.

(a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.

Proof. If x^{a+b} then there are $a+b$ terms of x multiplied together. That is

$$\begin{aligned} x^{a+b} &= x_1 \cdot x_2 \cdot x_3 \cdots x_a \cdot x_{a+1} \cdot x_{a+2} \cdots x_{a+b} \\ &= (x_1 \cdot x_2 \cdot x_3 \cdots x_a)(x_1 \cdot x_2 \cdots x_b) \\ &= x^a x^b \end{aligned}$$

If $(x^a)^b$ then there are a terms of x multiplied together that are then themselves multiplied together b times. That is $(x^a)^b = x^{a_1} \cdot x^{a_2} \cdots x^{a_b}$. Since we know that $x^{a+b} = x^a x^b$ we see that $x^a x^a = x^{a+a} = x^{2a}$ so that we have $(x^a)^b = x^{a_1} \cdot x^{a_2} \cdots x^{a_b} = x^{a_1+a_2+a_3+\cdots+a_b} = x^{ab}$. □

(b) Prove that $(x^a)^{-1} = x^{-a}$.

Proof. From proof of part (a) above we know that $(x^a)^b = x^{ab}$, let $b = -1$ □

(c) Establish part (a) for arbitrary integers a and b (positive, negative or zero).

positive: we already established part (a) using arbitrary positive integers.

zero: $x^{0+b} = x^0 x^b \implies x^b = 1x^b = x^b$, $x^{a+0} = x^a x^0 \implies x^a = x^a 1 = x^a$, $(x^0)^b = x^{0b} \implies (1)^b = x^0 \implies 1 = 1$, $(x^a)^0 = xa0 \implies 1 = x^0 \implies 1 = 1$.

negative:

$$\begin{aligned} x^{-a+b} &= x_1^{-1} \cdot x_2^{-1} \cdot x_3^{-1} \cdots x_a^{-1} \cdot x_1 \cdot x_2 \cdots x_b \\ &= (x_1^{-1} \cdot x_2^{-1} \cdot x_3^{-1} \cdots x_a^{-1})(x_1 \cdot x_2 \cdots x_b) \\ &= (x^{-a})(x^b) \\ &= x^{-a} x^b \end{aligned}$$

With same argument we can see that $x^{a-b} = x^a x^{-b}$ and that $x^{-a-b} = x^{-a} x^{-b}$.

From part (a) we know $(x^a)^b = x^{ab}$ so that we have $(x^{-a})^b = x^{-ab}$, $(x^a)^{-b} = x^{a(-b)} = x^{-ab}$, and $(x^{-a})^{-b} = x^{(-a)(-b)} = x^{ab}$.

20. For x and element in G show that x and x^{-1} have the same order.

Proof. If $|x| = a$ and $|x^{-1}| = b$ then $x^a = 1$ and $(x^{-1})^b = 1$ so that $x^a = (x^{-1})^b$. Therefore, since $(x^-1)^b = x^{-b}$ (cf. Exercise 19) we have that $x^a = x^{-b} \implies a = -b$ but the order must be a positive number so a must be equal to b. □

21. Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

Proof. If $|x| = n$ and $n = 2k-1$ for some $k \in \mathbb{Z}+$ then $|x| = 2k-1 \implies$

$$\begin{aligned} x^{2k-1} &= 1 \\ x^{2k} x^{-1} &= 1 \end{aligned}$$

$$
\begin{aligned}
x^{2k}x^{-1}x &= 1x \\
x^{2k}1 &= x \\
(x^2)^k &= x && \text{[Exercise 19]}
\end{aligned}
$$

Therefore, if n is odd, then $x = (x^2)^k$ for some k. □

22. If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Proof. Let $x, g \in G$ and $|x| = a$ and $|g| = b$.

$$
\begin{aligned}
x &= (x^{-1})^{-1} \\
&= (x^{-1}1)^{-1} \\
&= (x^{-1}g^{-1}g)^{-1} \\
&= ((x^{-1}g^{-1})(g))^{-1} \\
&= g^{-1}xg
\end{aligned}
$$

Since $x = g^{-1}xg$, then $|x| = |g^{-1}xg|$.

In general we have that $|ab| = |ba|$ since by Exercise 20 we know that $|x| = |x^{-1}|$ therefore $|ab| = |(ab)^{-1}| \implies |ab| = |b^{-1}a^{-1}| \implies |ab| = |ba|$. □

23. Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t, prove that $|x^s| = t$.

Proof. $|x| = n$ then

$$
\begin{aligned}
x^n &= 1 \\
x^{st} &= 1 \\
(x^s)^t &= 1 \\
|x^s| &= t
\end{aligned}
$$

Therefore, if $n = st$ for some positive integers s and t, then $|x^s| = t$. □

24. If a and b are *commuting* elements of G, prove that $(ab)^n = a^n b^n$ for $n \in \mathbb{Z}$. [Do this by induction for positive n first.]

Proof. $(n = 0)$ is trivially true as anything raised to power of 0 is 1 therefore $(ab)^0 = a^0 b^0 = 1$

$(n > 0)$

base case - since $ab = ba$ we can see that $(ab)^1 = b^1 a^1 \implies (ab)^1 = a^1 b^1$.

induction hypothesis - Assume that $(ab)^{n-1} = a^{n-1}b^{n-1}$.

induction step - Let $x = ab$, then

$$
\begin{aligned}
x^n &= x^1 x^{n-1} && [x^{a+b} = x^a x^b \text{ Exercise 19}] \\
(ab)^n &= (ab)^1 (ab)^{n-1} \\
(ab)^n &= aba^{n-1}b^{n-1} && \text{[base case and induction hypothesis]} \\
(ab)^n &= aba^{n-1}b^{n-1} && [a \text{ and } b \text{ are commutative elements}]
\end{aligned}
$$

$$(ab)^n = aa^{n-1}bb^{n-1}$$
$$(ab)^n = a^n b^n$$

$(n < 0)$

base case - since $ab = ba$ we can see that

$$(ab)^{-1} = b^{-1}a^{-1}$$
$$(ab)^{-1} = a^{-1}b^{-1}$$

induction hypothesis - Assume that $(ab)^{-(n-1)} = a^{-(n-1)}b^{-(n-1)}$.

induction step - Let $x = ab$, then

Since a and b are commutative elements we can interchange them so that

$$\begin{aligned}
x^{-n} &= x^{-1}x^{-(n-1)} = (ab)^{-n} && [x^{-a-b} = x^{-a}x^{-b} \text{ Exercise 19}] \\
&= (ab)^{-1}(ab)^{-(n-1)} \\
&= a^{-1}b^{-1}a^{-(n-1)}b^{-(n-1)} && [\text{base case and induction hypothesis}] \\
&= a^{-1}b^{-1}a^{-(n-1)}b^{-(n-1)} && [a \text{ and } b \text{ are commutative elements}] \\
&= a^{-1}a^{-(n-1)}b^{-1}b^{-(n-1)} \\
&= a^{-n}b^{-n}
\end{aligned}$$

Therefore, if a and b are *commuting* elements of G, then $(ab)^n = a^n b^n$ for $n \in \mathbb{Z}$. □

25. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Proof. If $x^2 = 1$ then $x^2 = xx^{-1}$ since $1 = xx^{-1}$. Therefore, for all $x \in G$ we have shown that each element is equal to its inverse. Thus, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. □

26. Assume H is a nonempty subset of $(G, *)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H, hk$ and $h^{-1} \in H$. Prove that H is a group under the operation $*$ restricted to H (such a subset H is called a *subgroup* of G).

Proof. associative - Let $h, k, s \in G$. $h(ks) \implies hks \implies (hk)s$.

inverses - given by hypothesis.

identity - $hh^{-1} = 1$, where 1 is the identity element.

Therefore, H is a subgroup of G. □

27. Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup (cf. the preceding exercise) of G (called the *cyclic subgroup* of G generated by x).

Proof. associative - Let $n, k, s \in \mathbb{Z}$.

$$\begin{aligned}
x^n(x^k x^s) &= x^n(x)^{k+s} \\
&= x^{n+k+s}
\end{aligned}$$

$$= (x)^{n+k}x^s$$
$$= (x^n x^k)x^s$$

inverses - For a given n we have x^n and the inverse of this is just $-n$ so that we have x^{-n}.

identity - $x^0 = 1$ and additionally for any n we have $x^n x^{-n} = 1$, where 1 is the identity element.

Therefore, this a subgroup of G. □

28. Let $(A, *)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:

(a) Prove that the associative law holds: for all $(a_i, b_i) \in A \times B, i = 1, 2, 3$

$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3)$

Proof.

$$\begin{aligned}(a_1, b_1)[(a_2, b_2)(a_3, b_3)] &= (a_1, b_1)(a_2 * a_3, b_2 \diamond b_3)\\ &= (a_1 * (a_2 * a_3), b_1 \diamond (b_2 \diamond b_3))\\ &= ((a_1 * a_2) * a_3), (b_1 \diamond b_2) \diamond b_3))\\ &= (a_2 * a_3, b_2 \diamond b_3)(a_3, b_3)\\ &= [(a_1, b_1)(a_2, b_2)](a_3, b_3)\end{aligned}$$

□

(b) Prove that $(1, 1)$ is the identity of $A \times B$

Proof. $(a, b)(1, 1) \implies (a * 1, b \diamond 1) \implies (a, b)$. □

(c) Prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

Proof. $(a, b)(a^{-1}, b^{-1}) \implies (a * a^{-1}, b \diamond b^{-1}) \implies (e, f)$ where e, f are the identity elements for the groups A, B respectively. □

29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

Proof. If $A \times B$ is an abelian group then

$$\begin{aligned}(a_1, b_1)(a_2, b_2) &= (a_2, b_2)(a_1, b_1)\\ &= (a_1 a_2, b_1 b_2) = (a_2 a_1, b_2 b_1)\end{aligned}$$

So that $a_1 a_2 = a_2 a_1$ and $b_1 b_2 = b_2 b_1$. Therefore, A and B are both abelian.

Conversely, if A and B are both abelian then $a_1 a_2 = a_2 a_1, b_1 b_2 = b_2 b_1$ and

$$\begin{aligned}(a_1 a_2, b_1 b_2) &= (a_2 a_1, b_2 b_1)\\ &= (a_1, b_1)(a_2, b_2)\\ &= (a_2, b_2)(a_1, b_1)\end{aligned}$$

Therefore, $A \times B$ is an abelian group. □

30. Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

$$\begin{aligned} \textit{Proof.}\ (a,1)(1,b) &\implies (a*1, 1*b) \implies (a,b) \\ (1,b)(a,1) &\implies (1*a, b*1) \implies (a,b) \end{aligned}$$

Therefore $(a, 1)(1, b) = (1, b)(a, 1)$.

The identity for $A \times B$ was shown to be $(1, 1)$ [Exercise 28]. Therefore, since $|a| = m \implies a^m = 1$ and $|b| = n \implies b^n = 1$, we see that $|(a, b)| = x \implies (a^x, b^x) = (1, 1)$. But in order for a^x, b^x to be equal to 1 x needs to be a multiple of both m and n. The lowest common multiple of m and n will give us this, which is just the lowest common multiple of $|a|$ and $|b|$. □

31. Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every non-identity element of $G - t(G)$ has order 2.]

Proof. $e \notin t(G)$ as it is its own inverse. Additionally, if $g = g^{-1}$ then $|g| = |g^{-1}| = 2$. Therefore $t(G)$ is the set with elements that have order greater than 2. Thus, if $g \in t(G)$ then $g^{-1} \in t(G)$ so there must be an even number of elements in t(G). Since G and $t(G)$ both have an even number of elements so too must $G - t(G)$ and since one of the elements in $G - t(g)$ is the identity element and it is the only element of order 1 the other element must be an element of order 2. □

32. Is x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Proof. Suppose $x^a = x^b$ for some integers a and b with $0 \leq a \leq b \leq n - 1$. Since $1 = x^a x^{-a}$ then $1 = x^a x^{-a} = x^b x^{-a} = x^{b-a}$. Thus, $b - a = 0$ so that $b = a$ and therefore $1, x, x^2, \ldots, x^{n-1}$ are all distinct. All of these elements are in G so $|x| \leq |G|$. □

33. Let x be an element of finite order n in G.

(a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n - 1$.

Proof. Suppose $x^i = x^{-i} \implies x^{2i} = 1$. But we were given that $|x| = 2i + 1 \implies x^{2i+1} = 1$, which is a contradiction. Therefore $x^i \neq x^{-i}$. □

(b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-1}$ if and only if $i = k$.

Proof. Since $n = 2k$ we know that $|x| = 2k \implies x^{2k} = 1$.

If $x^i = x^{-1}$ then

$$\begin{aligned} x^k &= x^{-k} && [(x^k)^2 = 1] \\ (x)^k &= (x^{-1})^k \\ ((x)^k)^{-k} &= ((x^{-1})^k)^{-k} \\ x &= x^{-1} \end{aligned}$$

Therefore, since $x = x^{-1}$

$$\begin{aligned}
xx = x^{-1}x &= 1 \\
x^{-1}x^{-1} &= 1 && [x = x^{-1}] \\
(x^{-1})^2 &= 1 \\
(x^{-1})^2 &= (x^k)^2 && [x^{2k} = 1] \\
((x^{-1})^2)^{-2} &= ((x^k)^2)^{-2} \\
x^{-1} &= x^k \\
x^i &= x^k && [x^i = x^{-1}]
\end{aligned}$$

Therefore, $i = k$.

Conversely, if $i = k$ then $(x^i)^2 = 1 \implies x^i = x^{-1}$ as x^i must be its own inverse from the same argument above.

Therefore, if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-1}$ if and only if $i = k$. □

34. If x is an element of infinite order in G, prove that the elements $x^n, n \in \mathbb{Z}$ are all distinct.

Proof. Suppose $x^a = x^b$ for some integers $a \leq b$. Since $1 = x^a x^{-a}$ then $1 = x^a x^{-a} = x^b x^{-a} = x^{b-a}$. Thus, $b - a = 0$ so that $b = a$ and therefore x^n is distinct. This works for $-a \leq -b$ as well with the same argument. □

35. If x is an element of finite order n in G, use the Division Algorithm to show that *any* integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all distinct elements of the cyclic subgroup (cf. Exercise 27 above) of G generated by x).

Proof. By the Division Algorithm we know that $s = nq+r$ for some integer s and where $0 \leq r < n$. Therefore

$$\begin{aligned}
x^s &= x^{nq+r} \\
&= x^{nq}x^r \\
&= 1x^r \\
&= x^r
\end{aligned}$$

Therefore, $s = r$. Since $r \in \{0, 1, 2, \ldots, n-1\}$ we see that x^r will equal one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$. □

36. Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Exercise 32, every element has order ≤ 3). use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

Proof. We know that $ab \neq a$ and $ab \neq b$. Therefore $ab = 1$ or $ab = c$. Assume that $ab = 1$. Then this means that a and b are inverses so that $a^2 \neq 1 \implies a^3 = 1$ since we know it can't be of order 1 (identity) and it can't have order higher than 3. Thus, $ab = 1 \implies b = a^2$ and $a^4 = b^2 \implies a = b^2$. But then we no longer have a choice for ac as $ac \neq 1$ ($ab = 1$), $ac \neq b$ ($b = a^2$), $ac \neq c$, $ac \neq a$. This is a contradiction so ab must be equal to c.

We could have used the above argument to find ba as well. Furthermore the entirety can be repeated to find $ac = ca = b$ and $cb = bc = a$. Since none of the elements were found to have order 3, this means all of the non-identity elements of this group have order 2 so that:

$$\begin{aligned} a^2 = (bc)^2 = (cb)^2 = 1 \\ b^2 = (ac)^2 = (ca)^2 = 1 \\ c^2 = (ba)^2 = (ab)^2 = 1 \end{aligned}$$

Therefore, this group is abelian [Exercise 25]. □

1.2 DIHEDRAL GROUPS

In these exercises, D_{2n} has the usual presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

1. Compute the order of each of the elements in the following groups:

(a) $D_6 = \{1, r, r^2, s, sr, sr^2\}$

$$\begin{aligned} |1| &= 1 \\ |r| &= 3 \\ |r^2| &= 3 \\ |s| &= 2 \\ |sr| &= 2 \\ |sr^2| &= 2 \end{aligned}$$

(b) $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$$\begin{aligned} |1| &= 1 \\ |r| &= 4 \\ |r^2| &= 2 \\ |r^3| &= 4 \\ |s| &= 2 \\ |sr| &= 2 \\ |sr^2| &= 2 \\ |sr^3| &= 2 \end{aligned}$$

(c) $D_{10} = \{1, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$

$$\begin{aligned} |1| &= 1 \\ |r| &= 5 \\ |r^2| &= 5 \\ |r^3| &= 5 \\ |s| &= 2 \\ |sr| &= 2 \\ |sr^2| &= 2 \\ |sr^3| &= 2 \end{aligned}$$

$$|sr^4| = 2$$

2. Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

Proof. If $x \in D_{2n}$ such that x is not a power of r then using the generators and relations above this means that it can only be s as all other elements will have a power of r in them (the identity is $r^n = 1$). Therefore, using the relation $rs = sr^{-1} \implies rx = xr^{-1}$. □

3. Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

Proof. We know that the only element of D_{2n} that is not a power of r is s [Exercise 2] and by the relation $s^2 = 1$ we know that $|s| = 2$.

We can also easily see that the order of sr is 2 as well

$$\begin{aligned}(sr)(sr) &= s(rs)r \\ &= ssr^{-1}r && [rs = sr^{-1}] \\ &= s^2 = 1 && [s^2 = 1]\end{aligned}$$

Additionally, all elements of D_{2n} are generated from s and sr since $s(sr) = s^2r = r$. Therefore, the unique elements $s^k r^i$, where $k \in \{0, 1\}$ and $r \in \{0, 1, 2, \ldots, n-1\}$ can all be generated from s and sr. □

4. If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only non-identity element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 33 of Section 1.]

Proof. $r^k r^k = r^{2k} = r^n = 1 \implies |r^k| = 2$. We know that $r^k = r^{-1}$ and that $r = r^{-1}$ as it is self inversive [Exercise 33]. Additionally we know that r^k is the only power of r that has this property [Exercise 33]. Thus, using the relation $rs = sr^{-1}$ we see that $rs = sr$ and that it is the only non-identity element that commutes with all the elements of D_{2n}. □

5. If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 33 of Section 1.]

Proof. If n is odd and $n \geq 3$ then we know that none of the elements other than the identity element are equal to their own inverse [Exercise 33 Section 1]. Therefore, the identity element is the only element that will be able to commute with all the elements of D_{2n}. □

6. Let x and y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).

Proof. $|x| = |y| = 2 \implies x^2 = 1, y^2 = 1 \implies x = x^{-1}, y = y^{-1}$. If $t = xy$, then

$$\begin{aligned}tx &= (xy)x \\ &= x(yx) \\ &= x(y^{-1}x^{-1})\end{aligned}$$

$$= x(xy)^{-1}$$
$$= xt^{-1}$$

Therefore, if $t = xy$ then $tx = xt^{-1}$. □

7. Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1\rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s.]

Proof. $a = s$ and $b = sr$ and using the relations $a^2 = 1, b^2 = 1 \implies s^2 = 1, (sr)^2 = 1$. Then

$$\begin{aligned} (sr)(sr) &= ss && [s^2 = 1, (sr)^2 = 1] \\ s^{-1}srsr &= s^{-1}ss \\ rsr &= s \\ rsrr^{-1} &= sr^{-1} \\ rs &= sr^{-1} \end{aligned}$$

Conversely, we can also follow the same steps backwards to arrive at a and b. □

8. Find the order of the cyclic subgroup of D_{2n} generated by r (cf. Exercise 27 of Section 1).

Proof. The cyclic subgroup of D_{2n} is $\{1, r, r^2, \ldots, r^{n-1}\}$ so that the order is n. This is the same as the order for r as $|r| = n$. □

In each of Exercises 9 to 13 you can find the order of the group of rigid motions in $\mathbb{R}^3$ (also called the group of rotations) of the given Platonic solid by following the proof for the order of D_{2n}: find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once a face is fixed, the number of positions to which a vertex on that face may be sent.

9. Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Proof.

vertices and faces - 4 vertices and faces, 4 axes through a vertex and the center of the opposing face with 120 degree rotatio
edges - 6 edges with 3 axes through center of opposite edges with 180 degree rotations = 3 rotations

$|G| = 1 + 8 + 3 = 12$. □

10. Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

Proof.

vertices - 8 vertices with 4 axes with 120 degree rotations = 8 rotations
faces - 6 faces with 3 axes with 90 degree rotations = 9 rotations
edges - 12 edges with 6 axes with 180 degree rotations = 6 rotations

$|G| = 1 + 8 + 9 + 6 = 24$. □

11. Let G be the group of rigid motions in $\mathbb{R}^3$ of a octahedron. Show that $|G| = 24$.

Proof.

vertices - 6 with 3 axis with 90 degree rotations = 9 rotations
faces - 8 with 4 axis with 120 degree rotations = 8 rotations
edges - 12 with 6 axis with 180 degree rotations = 6 rotations

$|G| = 1 + 9 + 8 + 6 = 24$. □

12. Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.

Proof.

vertices - 20 with 10 axis with 120 degree rotations = 20 rotations
faces - 12 with 6 axis with 72 degree rotations = 24 rotations
edges - 30 with 15 axis with 180 degree rotations = 15 rotations

$|G| = 1 + 20 + 24 + 15 = 60$. □

13. Let G be the group of rigid motions in $\mathbb{R}^3$ of a icosahedron. Show that $|G| = 60$.

Proof.

vertices - 12 with 6 axis with 72 degree rotations = 24 rotations
faces - 20 with 10 axis with 120 degree rotations = 20 rotations
edges - 30 with 15 axis with 180 degree rotations = 15 rotations

$|G| = 1 + 24 + 20 + 15 = 60$. □

14. Find a set of generators for $\mathbb{Z}$.

We can generate $\mathbb{Z}$ with $\{-1, 1\}$ as all elements of $\mathbb{Z}$ can be created from different additive combinations of these two numbers.

15. Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ which can be represented with the presentation $< x \mid x^n = 1 >$.

16. Show that the group $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1y_1)^2 = 1\rangle$ is the dihedral group D_4 (where x_1 may be replaced be the letter r and y_1 by s). [Show that the last relation is the same as: $x_1y_1 = y_1x_1^{-1}$.]

Proof. If we replace x_1 with r and y_1 with s we see from the relations that $x_1^2 = r^2 = 1$ and $y_1^2 = s^2 = 1$. Additionally,

$$\begin{aligned}(x_1y_1)^2 &= 1\\ (x_1y_1)(x_1y_1) &= 1\\ (x_1y_1)(x_1y_1)(x_1y_1)^{-1} &= 1(x_1y_1)^{-1}\\ (x_1y_1) &= (x_1y_1)^{-1}\\ x_1y_1 &= y_1^{-1}x_1^{-1}\end{aligned}$$

Therefore, since $y_1^2 = 1 \implies y_1 = y_1^{-1}$ we see that

$$x_1y_1 = y_1^{-1}x_1^{-1}$$

$$\begin{aligned} x_1y_1 &= y_1x_1^{-1} \\ rs &= sr^{-1} \qquad \text{[when replacing } x_1 \text{ with } r \text{ and } y_1 \text{ with } s\text{]} \end{aligned}$$

Since the $r^2 = 1$ we see that this group is the dihedral group D_4. □

17. Let X_{2n} be the group whose presentation is displayed in (1.2).

(a) Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s.

Proof. If $n = 3k$ then $x^{3k} = y^2 = 1$. From the textbook we were shown that X_{2n} yields $x = x^4$ using the relation $xy = yx^2$. Therefore,

$$\begin{aligned} x &= x^4 \\ x^{-1}x &= x^{-1}x^4 \\ 1 &= x^3 \\ y^2 &= x^3 \end{aligned}$$

Therefore, $k = 1$. Thus, the order of D_{2n} is $2(3k) = 2(3) = 6$. Since $x^3 = 1$ we see that $x^{-1} = x^2$ so that when replacing x by r and y by s we see that

$$\begin{aligned} xy &= yx^2 \\ xy &= yx^{-1} \\ rs &= sr^{-1} \end{aligned}$$

Therefore, x_{2n} has been shown to have order 6, and it has the same generators and relations as D_6. □

(b) Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2. [Use the facts that $x^n = 1$ and $x^3 = 1$.]

Proof. Since $x^n = 1$ and $x^3 = 1$ we have that $x^n = x^3$ but $(3, n) = 1 \implies n \neq 3k$ for some $k \in \mathbb{Z}$. Therefore, for this equation to be true and still satisfy $x^n = 1$ we must have that $x = 1$. Thus, $n = 1$ and by deduction this means that X_{2n} has order 2. □

18. Let Y be the group whose presentation is displayed in (1.3).

(a) Show that $v^2 = v^{-1}$. [Use the relation: $v^3 = 1$.]

Proof.

$$\begin{aligned} v^3 &= 1 \\ v^3v^{-1} &= v^{-1} \\ v^2 &= v^{-1} \end{aligned}$$

□

(b) Show that v commutes with u^3. [Show that $v^2u^3v = u^3$ by writing the left hand side as $(v^2u^2)(uv)$ and using the relations to reduce this to the right hand side. Then use part (a).]

Proof.

$$\begin{aligned} v^2u^3v &= u^3 \\ v^2u^2(uv) &= u^3 \\ v^2u^2(uv)(uv)^{-1} &= u^3(uv)^{-1} \\ v^2u^2 &= u^3v^{-1}u^{-1} \\ v^{-1}u^2 &= u^3v^2u^{-1} && \text{[re-written using part (a)]} \\ v^{-1}u^3 &= u^3v^2 \\ u^3 &= vu^3v^2 \end{aligned}$$

Therefore, $v^2u^3v = vu^3v^2$ and we can see that v commutes with u^3. □

(c) Show that v commutes with u. [Show that $u^9 = u$ and then use part (b).]

Proof. $u^9 = u^4u^4u = u$ since $u^4 = 1$.

From part (b) we saw that $u^3 = vu^3v^2$ and $u^3 = v^2u^3v$. Since, $u = u^9 = (u^3)^3 = (vu^3v^2)^3$ and $u = u^9 = (u^3)^3 = (v^2u^3v)^3$, then

$$\begin{aligned} (vu^3v^2)^3 &= (v^2u^3v)^3 \\ (vu^3v^2)(vu^3v^2)(vu^3v^2) &= (v^2u^3v)(v^2u^3v)(v^2u^3v) \end{aligned}$$

Using the fact that $v^3 = 1$ these can be reduced to

$$\begin{aligned} vu^3u^3u^3v^2 &= v^2u^3u^3u^3v \\ vu^9v^2 &= v^2u^9v \\ vuv^2 &= v^2uv \end{aligned}$$

which shows that v commutes with u. □

(d) Show that $uv = 1$. [Use part (c) and the last relation.]

Proof.

$$\begin{aligned} uv &= v^2u^2 \\ uv &= vvuu \\ uv &= (uv)(uv) && \text{[u and v commute]} \\ (uv)(uv)^{-1} &= (uv)(uv)(uv)^{-1} \\ 1 &= uv \end{aligned}$$

□

(e) Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$. [Use part (d) and the equation $u^4v^3 = 1$.]

Proof. Since $u^4 = v^3 = 1 \implies u^4v^3 = (1)(1) = 1$. From part (d) we know that $uv = 1$, therefore

$$\begin{aligned} u^4v^3 &= 1 \\ uuu(uv)vv &= 1 \\ uu(uv)v &= 1 \end{aligned}$$

$$u(uv) = 1$$
$$u = 1$$

Additionally, since $uv = 1$ and $u = 1$ we see that $uv = 1v = 1 \implies v = 1$. □

1.3 SYMMETRIC GROUPS

1. Let σ be the permutation

$$1 \mapsto 3 \qquad 2 \mapsto 4 \qquad 3 \mapsto 5 \qquad 4 \mapsto 2 \qquad 5 \mapsto 1$$

and let τ be the permutation

$$1 \mapsto 5 \qquad 2 \mapsto 3 \qquad 3 \mapsto 2 \qquad 4 \mapsto 4 \qquad 5 \mapsto 1$$

Find the cycle decompositions of each of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma$, and $\tau^2\sigma$.

$$\sigma = (1\ 3\ 5)(2\ 4)$$
$$\tau = (1\ 5)(2\ 3)$$
$$\sigma^2 = (1\ 5\ 3)$$
$$\sigma\tau = (2\ 5\ 3\ 4)$$
$$\tau\sigma = (1\ 2\ 4\ 3)$$
$$\tau^2\sigma = (1\ 3\ 5)(2\ 4)$$

2. Let σ be the permutation

$$\begin{array}{lllll} 1 \mapsto 13 & 2 \mapsto 2 & 3 \mapsto 15 & 4 \mapsto 14 & 5 \mapsto 10 \\ 6 \mapsto 6 & 7 \mapsto 12 & 8 \mapsto 3 & 9 \mapsto 4 & 10 \mapsto 1 \\ 11 \mapsto 17 & 12 \mapsto 9 & 13 \mapsto 5 & 14 \mapsto 11 & 15 \mapsto 8 \end{array}$$

and let τ be the permutation

$$\begin{array}{lllll} 1 \mapsto 14 & 2 \mapsto 9 & 3 \mapsto 10 & 4 \mapsto 2 & 5 \mapsto 12 \\ 6 \mapsto 6 & 7 \mapsto 5 & 8 \mapsto 11 & 9 \mapsto 15 & 10 \mapsto 3 \\ 11 \mapsto 8 & 12 \mapsto 7 & 13 \mapsto 4 & 14 \mapsto 1 & 15 \mapsto 13 \end{array}$$

Find the cycle of decompositions of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma$, and $\tau^2\sigma$.

$$\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$$
$$\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$$
$$\sigma^2 = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13)$$
$$\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14)$$
$$\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)$$
$$\tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$$

3. For each of the permutations whose cycle decompositions were computed in the preceding two exercises compute its order.

Problem 1:

$$|\sigma| = 2\ [\sigma^2 \circ \sigma = (5\ 4\ 1\ 2\ 3)(3\ 4\ 5\ 2\ 1) = (1\ 2\ 3\ 4\ 5)]$$

$$
\begin{aligned}
|\tau| &= 2\ [\tau \circ \tau = (5\ 3\ 2\ 4\ 1)(5\ 3\ 2\ 4\ 1) = (1\ 2\ 3\ 4\ 5)] \\
|\sigma^2| &= 6\ [(\sigma^2)^5 \circ \sigma^2 = (3\ 4\ 5\ 2\ 1)(5\ 4\ 1\ 2\ 3) = (1\ 2\ 3\ 4\ 5)] \\
|\sigma\tau| &= 4\ [(\sigma\tau)^3 \circ \sigma\tau = (1\ 4\ 5\ 3\ 2)(1\ 5\ 4\ 2\ 3) = (1\ 2\ 3\ 4\ 5)] \\
|\tau\sigma| &= 4\ [(\tau\sigma)^3 \circ \tau\sigma = (3\ 1\ 4\ 2\ 5)(2\ 4\ 1\ 3\ 5) = (1\ 2\ 4\ 5)] \\
|\tau\sigma^2| &= 6\ [(\tau\sigma^2)^5 \circ \tau\sigma^2 = (5\ 4\ 1\ 2\ 3)(3\ 4\ 5\ 2\ 1) = (1\ 2\ 3\ 4\ 5)]
\end{aligned}
$$

Problem 2:

These are rather long and are left to the reader.

4. Compute the order of each of the elements in the following groups:

(a) S_3

The elements of S_3 have the cycle decompositions: 1, (1 2), (1 3), (2 3), (1 2 3), and (1 3 2).

$$
\begin{aligned}
|1| &= 1, \text{ since this is the identity element.} \\
|(1\ 2)| &= 2\ [(1\ 2)(1\ 2) = (1)(2)(3) = 1] \\
|(1\ 3)| &= 2\ [(1\ 3)(1\ 3) = (1)(2)(3) = 1] \\
|(1\ 3)| &= 2\ [(2\ 3)(2\ 3) = (1)(2)(3) = 1] \\
|(1\ 2\ 3)| &= 3\ [(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2) \implies (1\ 2\ 3)(1\ 3\ 2) = (1)(2)(3) = 1] \\
|(1\ 3\ 2)| &= 3\ [(1\ 3\ 2)(1\ 3\ 2) = (1\ 2\ 3) \implies (1\ 3\ 2)(1\ 2\ 3) = (1)(2)(3) = 1]
\end{aligned}
$$

(b) S_4

The elements of S_4 have the cycle decompositions: 1, (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2 3), (1 2 4), (1 3 2), (1 3 4), (1 4 2), (1 4 3), (2 3 4), (2 4 3), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2).

$$
\begin{aligned}
|1| &= 1, \text{ since this is the identity element.} \\
|(1\ 3)| &= 2\ [(1\ 3)(1\ 3) = 1] \\
|(1\ 2)| &= 2\ [(1\ 2)(1\ 2) = 1] \\
|(1\ 4)| &= 2\ [(1\ 4)(1\ 4) = 1] \\
|(2\ 3)| &= 2\ [(2\ 3)(2\ 3) = 1] \\
|(2\ 4)| &= 2\ [(2\ 4)(2\ 4) = 1] \\
|(3\ 4)| &= 2\ [(3\ 4)(3\ 4) = 1] \\
|(1\ 2\ 3)| &= 3\ [(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2) \implies (1\ 2\ 3)(1\ 3\ 2) = 1] \\
|(1\ 2\ 4)| &= 3\ [(1\ 2\ 4)(1\ 2\ 4) = (1\ 4\ 2) \implies (1\ 2\ 4)(1\ 4\ 2) = 1] \\
|(1\ 3\ 2)| &= 3\ [(1\ 3\ 2)(1\ 3\ 2) = (1\ 2\ 3) \implies (1\ 3\ 2)(1\ 2\ 3) = 1] \\
|(1\ 3\ 4)| &= 3\ [(1\ 3\ 4)(1\ 3\ 4) = (1\ 4\ 3) \implies (1\ 3\ 4)(1\ 4\ 3) = 1] \\
|(1\ 4\ 2)| &= 3\ [(1\ 4\ 2)(1\ 4\ 2) = (1\ 2\ 4) \implies (1\ 4\ 2)(1\ 2\ 4) = 1] \\
|(1\ 4\ 3)| &= 3\ [(1\ 4\ 3)(1\ 4\ 3) = (1\ 3\ 4) \implies (1\ 4\ 3)(1\ 3\ 4) = 1] \\
|(2\ 3\ 4)| &= 3\ [(2\ 3\ 4)(2\ 3\ 4) = (2\ 4\ 3) \implies (2\ 3\ 4)(2\ 4\ 3) = 1] \\
|(2\ 4\ 3)| &= 3\ [(2\ 4\ 3)(2\ 4\ 3) = (2\ 3\ 4) \implies (2\ 4\ 3)(2\ 3\ 4) = 1] \\
|(1\ 2)(3\ 4)| &= 2\ [((1\ 2)(3\ 4))((1\ 2)(3\ 4)) = 1] \\
|(1\ 3)(2\ 4)| &= 2\ [((1\ 3)(2\ 4))((1\ 3)(2\ 4)) = 1]
\end{aligned}
$$

$|(1\ 4)(2\ 3)| = 2\ [((1\ 4)(2\ 3))((1\ 4)(2\ 3)) = 1]$

$|(1\ 2\ 3\ 4)| = 4\ [(1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 3)(2\ 4) \implies (1\ 2\ 3\ 4)((1\ 3)(2\ 4)) = (1\ 4\ 3\ 2) \implies (1\ 2\ 3\ 4)(1\ 4\ 3\ 2) = 1]$

$|(1\ 2\ 4\ 3)| = 4\ [(1\ 2\ 4\ 3)(1\ 2\ 4\ 3) = (1\ 4)(2\ 3) \implies (1\ 2\ 4\ 3)((1\ 4)(2\ 3)) = (1\ 3\ 4\ 2) \implies (1\ 2\ 4\ 3)(1\ 3\ 4\ 2) = 1]$

$|(1\ 3\ 2\ 4)| = 4\ [(1\ 3\ 2\ 4)(1\ 3\ 2\ 4) = (1\ 2)(3\ 4) \implies (1\ 3\ 2\ 4)((1\ 2)(3\ 4)) = (1\ 4\ 2\ 3) \implies (1\ 3\ 2\ 4)(1\ 4\ 2\ 3) = 1]$

$|(1\ 3\ 4\ 2)| = 4\ [(1\ 3\ 4\ 2)(1\ 3\ 4\ 2) = (1\ 4)(3\ 2) \implies (1\ 3\ 4\ 2)((1\ 4)(3\ 2)) = (1\ 2\ 4\ 3) \implies (1\ 3\ 4\ 2)(1\ 2\ 4\ 3) = 1]$

$|(1\ 4\ 2\ 3)| = 4\ [(1\ 4\ 2\ 3)(1\ 4\ 2\ 3) = (1\ 2)(3\ 4) \implies (1\ 4\ 2\ 3)((1\ 2)(3\ 4)) = (1\ 3\ 2\ 4) \implies (1\ 4\ 2\ 3)(1\ 3\ 2\ 4) = 1]$

$|(1\ 4\ 3\ 2)| = 4\ [(1\ 4\ 3\ 2)(1\ 4\ 3\ 2) = (1\ 3)(2\ 4) \implies (1\ 4\ 3\ 2)((1\ 3)(2\ 4)) = (1\ 2\ 3\ 4) \implies (1\ 4\ 3\ 2)(1\ 2\ 3\ 4) = 1]$

5. Find the order of $(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$.

Let $\gamma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$

$|\gamma| = 30$ because:

$$\begin{aligned}
\gamma^2 &= (1\ 8\ 4\ 12\ 10)(5\ 7\ 11)\\
\gamma^3 &= (1\ 10\ 12\ 4\ 8)(2\ 13)(6\ 9)\\
\gamma^4 &= (1\ 410\ 8\ 12)(5\ 11\ 7)\\
\gamma^5 &= (2\ 13)(5\ 7\ 11)(6\ 9)\\
\gamma^6 &= (1\ 12\ 8\ 10\ 4)\\
\gamma^7 &= (1\ 8\ 4\ 12\ 10)(2\ 13)(\ 11\ 7)(6\ 9)\\
\gamma^8 &= (1\ 10\ 12\ 4\ 8)(5\ 7\ 11)\\
\gamma^9 &= (1\ 4\ 10\ 8\ 12)(2\ 13)(6\ 9)\\
\gamma^{10} &= (5\ 11\ 7)\\
\gamma^{11} &= (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 7\ 11)(6\ 9)\\
\gamma^{12} &= (1\ 8\ 4\ 12\ 10)\\
\gamma^{13} &= (1\ 10\ 12\ 4\ 8)(2\ 13)(5\ 11\ 7)(6\ 9)\\
\gamma^{14} &= (1\ 4\ 10\ 8\ 12)(5\ 711)\\
\gamma^{15} &= (2\ 13)(6\ 9)\\
\gamma^{16} &= (1\ 12\ 8\ 10\ 4)(5\ 11\ 7)\\
\gamma^{17} &= (1\ 8\ 4\ 12\ 10)(2\ 13)(5\ 7\ 11)(6\ 9)\\
\gamma^{18} &= (1\ 10\ 12\ 4\ 8)\\
\gamma^{19} &= (1\ 4\ 10\ 8\ 12)(2\ 13)(6\ 9)\\
\gamma^{20} &= (5\ 7\ 11)\\
\gamma^{21} &= (1\ 12\ 8\ 10\ 4)(2\ 13)(6\ 9)\\
\gamma^{22} &= (1\ 8\ 4\ 12\ 10)(5\ 11\ 7)\\
\gamma^{23} &= (1\ 10\ 12\ 4\ 8)(2\ 13)(5\ 7\ 11)(6\ 9)\\
\gamma^{24} &= (1\ 4\ 10\ 8\ 12)\\
\gamma^{25} &= (2\ 13)(5\ 11\ 7)(6\ 9)\\
\gamma^{26} &= (1\ 12\ 8\ 10\ 4)(5\ 7\ 11)\\
\gamma^{27} &= (1\ 8\ 4\ 12\ 10)(2\ 13)(6\ 9)\\
\gamma^{28} &= (1\ 10\ 12\ 4\ 8)(5\ 11\ 7)
\end{aligned}$$

$$\gamma^{29} = (1\ 4\ 10\ 8\ 12)(2\ 13)(5\ 7\ 11)(6\ 9)$$
$$\gamma^{30} = (1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13) = 1$$

6. Write out the cycle decomposition of each element of order 4 in S_4.

$$(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (1\ 3\ 2\ 4),\ (1\ 3\ 4\ 2),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)$$

7. Write out the cycle decomposition of each element of order 2 in S_4.

$$(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)$$

8. Prove that if $\Omega = \{1, 2, 3, \dots\}$ then S_Ω is an infinite group (do not say $\infty! = \infty$).

Proof. Since $\Omega = \{1, 2, 3, \dots\}$ is a countably infinite set (i.e. this is just $\mathbb{Z}^+$) then there will be an infinite amount of permutations just from the permutation of exchanging two elements and leaving all others fixed. Therefore, we can see that S_Ω is an infinite group as there are many more permutations than the ones we have considered. □

9. (a) Let σ be the 12-cycle (1 2 3 4 5 6 7 8 9 10 11 12). For which positive integers i is σ^i also a 12-cycle?

$i = 5, 7, 11$ (manually checked up to 12)

(b) Let τ be the 8-cycle (1 2 3 4 5 6 7 8). For which positive integers i is τ^i also an 8-cycle?

$i = 3, 5, 7$ (manually checked up to 8)

(c) Let ω be the 14-cycle (1 2 3 4 5 6 7 8 9 10 11 12 13 14). For which positive integers i is ω^i also a 14-cycle?

$i = 3, 5, 11, 13$ (manually checked up to 14)

10. Prove that if σ is the m-cycle $(a_1 a_2 \dots a_m)$, then for all $i \in \{1, 2, \dots, m\}, \sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue mod m when $k + i > m$. Deduce that $|\sigma| = m$.

Proof. We will use induction to prove this.

base case - For $i = 1$ we have $\sigma = \sigma^1$ and we can see for all $a_k \in \sigma^1$ we have that $\sigma(a_k) = a_{k+1}$ since $a_k \mapsto a_{k+1}$.

induction hypothesis - For $1 \leq i \leq m - 1$ suppose that $\sigma^i(a_k) = a_{k+i}$.

induction step - For $i = m$ we have $\sigma^m = \sigma^{m-1}\sigma \implies \sigma^{m-1}(\sigma(a_k)) \implies \sigma^{m-1}(a_{k+1}) \implies a_{(k+1)+(m-1)} \implies a_{k+m}$. Thus, $\sigma^m(a_k) = a_{k+m}$.

Therefore, if $i \in \{1, 2, \dots, m\}, \sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue mod m when $k + i > m$. □

Additionally, it is easy to see that since we are mod m that for σ^m that $a_k \mapsto a_{k+m} = a_k$, therefore $|\sigma| = m$.

11. Let σ be the m-cycle (1 2 ... m). Show that σ^i is also an m-cycle if and only if i is relatively prime to m.

Proof. In an m-cycle we know that the last element must point back to the first element in the cycle, which for an m-cycle must be 1. Thus the last element must be congruent to 1 (mod m).

Suppose that σ^i is an m-cycle. We know that in general $\sigma^i(a_k) = a_{k+i}$ [Exercise 10] so that $\sigma^i : k \mapsto k+i \mapsto k+2i \cdots k+(m-1)i$. Additionally, since σ^i is an m-cycle each $k+xi$ must be unique so that $k+xi \not\equiv k+iy$ for unique $x, y \in \{0, 1, \ldots, m-1\}$. This implies that $(x-y)i \not\equiv 0 \pmod{m} \implies (x-y)i \nmid mn \implies mn \nmid (x-y)i$. Therefore, m and i do not have any common divisors and therefore they must be relatively prime.

Conversely, working backwards, if m and i are relatively prime then they do not have any common divisors so that $(x-y)i \not\equiv 0 \pmod{m} \implies k+xi \not\equiv k+yi$ for unique $x, y \in \{0, 1, \ldots, m-1\}$. Thus, each $k+xi$ must be unique and we know that in general $\sigma^i(a_k) = a_{k+i}$ [Exercise 10]. Thus, since all the elements $k+xi$ are unique modulo m we can see that we have $\sigma^i : k \mapsto k+i \mapsto k+2i \cdots k+(m-1)i$, which is an m-cycle. □

12. (a) If $\tau =$(1 2)(3 4)(5 6)(7 8)(9 10) determine whether there is a n-cycle σ $(n \geq 10)$ with $\tau = \sigma^k$ for some integer k.

Proof. We know that we can only get another n-cycle if n and i are relatively prime [Exercise 10]. However, in this situation we actually want them not to be relatively prime as we want it to equal τ.

If we take the n-cycle for $n = 10$ with $\sigma =$(1 2 3 4 5 6 7 8 9 10), we see that if $i = 5$ then they are not relatively prime as 5 is a divisor of 10 and we get $\sigma^5 =$(1 6)(2 7)(3 8)(4 9)(5 10). Now, we can swap the positions of the numbers to see what σ would need to be in order to make it so $\sigma^5 = \tau$. For example, 2 needs to be in the position of 6, 6 needs to be in the position of 8, 3 needs to be in the position of 2, and so on:

$$\begin{aligned}
\sigma &= (1 \ \cdots \cdot 2 \ \cdot 6 \ \cdot\cdot) \\
\sigma &= (1 \ 3 \ \cdots 2 \ \cdot 6 \ \cdot\cdot) \\
&\cdots \\
\sigma &= (1 \ 3 \ 5 \ 7 \ 9 \ 2 \ 4 \ 6 \ 8 \ 10)
\end{aligned}$$

$\sigma^5 = (\ 2)(3\ 4)(5\ 6)(\ 8)(9\ 10) = \tau$ □

(b) If $\tau =$(1 2)(3 4 5) determine whether there is an n-cycle $\sigma (n \geq 5)$ with $\tau = \sigma^k$ for some integer k.

Proof. Suppose we have an n-cycle $\sigma = (a_1 \ a_2 \cdots a_n)$ such that $\sigma^k = \tau$ for some integer k. Every a_i in an n-cycle is unique and for some i we must have $a_i = 3$. Then, using the fact that for an n-cycle that $sigma^k(a_i) = a_{i+k}$ we see that:

$$\begin{aligned}
\tau(3) &= \sigma^k(3) = \sigma^k(a_i) = a_{i+k} = 4 \\
\tau(4) &= \sigma^k(4) = \sigma^k(a_{i+k}) = a_{i+2k} = 5 \\
\tau(5) &= \sigma^k(5) = \sigma^k(a_{i+2k}) = a_{i+3k} = 3
\end{aligned}$$

Which, means that $a_i = a_{i+3k} \implies \sigma^{3k} = 1$ (where 1 is the identity cycle decomposition). Thus, if we take the cycle element $a_i = 2$ we see that $2 = \sigma^{3k}(2) = (\sigma^k)^3(2) = \tau^3(2) = 1$, which is a contradiction. Therefore, no n-cycle σ exists such that $\sigma^k = \tau$ for some integer k. □

13. Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

Proof. Let τ be an element in S_n with order 2. For an arbitrary m-cycle we know that $\sigma^k(a_i) = a_{i+k}$ and for τ we know that all of its cycles will have $\sigma_i^2(a_i) = a_{i+2} = a_i$ since $\tau^2 = 1$. Therefore, all its cycles will be 2-cycles (up to identity). Additionally, a_i and a_{i+1} only belong to one cycle because if $a_{i+1} \not\mapsto a_i$ we would not have $\sigma_i^2(a_i) = a_{i+2} = a_i$. Therefore, the cycle decomposition of τ must be a product of commuting 2-cycles (up to identity).

Conversely, if a cycle decomposition is a product of commuting 2-cycles then we know that $a_i \mapsto a_{i+1} \mapsto a_i$ so that for all a_i we have $a_{i+2} = a_i$ so that the order of this cycle decomposition is 2. □

14. Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

Proof. Let τ be an element of order p in S_n. Each element of S_n has n elements (these are not always explicitly written with cycle notation but they are still there nonetheless). Since $p \leq n$, if $p = n$ then the element τ would need to be a p-cycle because $|\tau| = p \implies \tau^p(a_i) = a_i$. If $p < n$, then p must a multiple of n so that $pk = n$ for some integer k. Like before, $|\tau| = p \implies \tau^p(a_i) = a_i$ for all $a_i \in \tau$, which implies that we have k p-cycles that are disjoint and can commute with one another.

Conversely, if the cycle decomposition of τ (we don't yet know its order at this point) is a product of commuting p-cycles then we know that $pk = n$ for some integer k since each element of S_n has n elements. Since we have k disjoint p-cycles, and it is know that $\sigma^k(a_i) = a_{i+k}$ for an arbitrary m-cycle, we know that $\tau^p(a_i) = a_i$. Therefore, $|\tau| = p$. □

Example when p is not prime:

The element (1 2)(3 4 5) from S_5 has order 6 and obviously it is not a product of commuting 6-cycles.

15. Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition. [Use Exercise 10 and Exercise 24 of Section 1.]

Proof. Let $\tau \in S_n$. To find the order of τ we need $\tau^t = 1$ for some integer t. In order for this to happen all of the cycles in τ must have the condition that $a_{i+t} = a_i$ for a cycle of length k and where $t = nk$. That is, t must be a multiple of the length of each of the cycles of τ. From , We know that an arbitrary m-cycle σ has the property $\sigma^k(a_i) = a_{i+k}$ [Exercise 10] and that $a_{i+k} = a_i$ if the m-cycle is of length k, i.e., that $m = k$. All of the cycles of τ might not have the same length so in order to have the condition that $a_{i+t} = a_i$ take t to be the least common multiple of the lengths of the cycles of τ. Then $\tau^t = (\sigma_1\sigma_2\cdots\sigma_m)^t = \sigma_1^t\sigma_2^t\cdots\sigma_m^t$ and since t is a multiple of length of each σ_i our condition $a_{i+t} = a_i$ will be met and therefore the order of an element in S_n is equal to the least common multiple of the length of the cycles in its cycle decomposition. □

16. Show that if $n \geq m$ then the number of m-cycles in S_n is given by

$$\frac{n(n-1)(n-1)\cdots(n-m+1)}{m}$$

[Count the number of ways of forming an m-cycle and divide by the number of representations of a particular m-cycle.]

Proof. The number of ways of choosing m items from n items can be found using the multiplicative formula for the binomial coefficient $\binom{n}{m} = \frac{n^{\underline{m}}}{m!} = \frac{n(n-1)(n-2)\cdots(n-m+1)}{m(m-1)(m-2)\cdots 1}$. The numerator gives the number of ways to select a sequence of m distinct objects, retaining the order of selection, from a set of n objects. The denominator counts the number of distinct sequences that define the same m-combination when order is disregarded. Since we don't want to disregard order, as the cycles in a cycle decomposition are dependent on order but not cyclical permutation of the numbers in the cycle themselves, we only want to divide by m here and not $m!$. This then gives us:

$$\frac{n(n-1)(n-1)\cdots(n-m+1)}{m}$$

as intended. □

17. Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$.

Proof. Suppose that $n \geq 4$ and consider the product of two 2-cycles:

$$(a_1\ a_2)(a_3\ a_4)$$

In succession, there are n ways to choose a_1, $n-1$ ways to choose a_2, $n-3$ ways to choose a_3 and $n-3$ ways to choose a_4 such that there are:

$$n(n-1)(n-2)(n-3)$$

such choices. However, since the cycle $(a_1\ a_2) = (a_2\ a_1)$, we see that we have counted twice so we should divide by 2. The same logic applies for $(a_3\ a_4)$.

We aren't done yet. Additionally, the order of the cycles themselves doesn't matter as they are disjoint and can commute. That is, $(a_1\ a_2)(a_3\ a_4) = (a_3\ a_4)(a_1\ a_2)$, so we should divide by 2 once again.

Therefore we have $n(n-1)(n-2)(n-3)/8$. □

18. Find all the numbers n such that S_5 contains an element of order n. [Use Exercise 15.]

It is easy to see that S_5 will have elements with orders 1, 2, 3, 4, and 5. However, since S_5 can also have a cycle decomposition of a 2-cycle and 3-cycle, we know that S_5 will also contain elements with order 6 [Exercise 15]. Therefore, S_5 contains elements with order 1, 2, 3, 4, 5, and 6.

19. Find all the numbers n such that S_7 contains an element of order n. [Use Exercise 15.]

In addition to the orders of the numbers 1 through 7 we can also get combinations of 3-cycle with a 4-cycle as well as combinations of 2-cycle with a 5-cycle [Exercise 18]. Therefore, S_7 contains elements with order 1, 2, 3, 4, 5, 6, 7, 10, and 12.

20. Find a set of generators and relations for S_3.

The elements of S_3 have the cycle decompositions: 1, (1 2), (1 3), (2 3), (1 2 3), and (1 3 2) [Exercise 4].

All of the 2-cycles have order 2 and all of the 3-cycles have order 3 so that we have the relations:

$r^3 = s^2 = 1$, where we have used r for a 3-cycle and s for a 2-cycle. If it already isn't apparent, S_3 is *isomorphic* to the dihedral group of order 6 D_6.

As such we also have the additional relation $rs = sr^{-1}$.

Therefore, for the set of generators and relations for S_3 we have the same presentation as the dihedral group of order 6:

$$\langle r, s \mid r^3 = s^2 = 1, rs = sr^{-1} \rangle$$

1.4 GROUPS

Let F be a field and let $n \in \mathbb{Z}^+$.

1. Prove that $|GL_2(\mathbb{F}_2)| = 6$.

Proof. Since $q = |\mathbb{F}_2| = 2$ and $n = 2$ we see that $|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2^1) = 6$. □

2. Write out all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.

The elements of $GL_2(\mathbb{F}_2)$ are the 2×2 invertible matrices over the field $\mathbb{F}_2$ which are the integers modulo 2. Therefore, the entries in the matrices are either 0 or 1.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\left|\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right| = 1, \text{ since this is the identity matrix.}$$
$$\left|\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right| = 2 \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]$$
$$\left|\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right| = 2 \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]$$
$$\left|\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right| = 2 \left[\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]$$
$$\left|\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right| = 3 \left[\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]$$
$$\left|\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right| = 3 \left[\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]$$

3. Show that $GL_2(\mathbb{F}_2)$ is non-abelian.

Proof. Let $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

$$AB = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ while } BA = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Therefore, $GL_2(\mathbb{F}_2)$ is non-abelian. □

4. Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

contrapositive. Suppose $\mathbb{Z}/n\mathbb{Z}$ is a field. Then for all a such that $0 < a < n$ there exists a b such that $\overline{a}\overline{b} = \overline{1}$. Thus, $ab + kn = 1$. Therefore $\gcd(a, n) = 1$ for $0 < a < n \implies n$ is prime. □

5. Show that $GL_2(F)$ is a finite group if and only if F has a finite number of elements.

Proof. Suppose that $GL_2(F)$ is a finite group. Therefore, $GL_2(F)$ must have a finite number of elements. The only way this can happen is if the field F is finite as the entries of the matrices are over these elements and in the case of an infinite field F we would have infinite elements in $GL_2(F)$.

Conversely, if F has a finite number of elements then since $GL_2(F)$ is composed of matrices using these elements there must be a finite number of matrices constructed using these entries. □

6. If $|F| = q$ is finite prove that $|GL_n(F)| < q^{n^2}$.

Proof. For an $n \times n$ matrix, each of its entries can be q different possibilities giving a total of q^{n^2} possibilities. However, we know that for the general linear group that some of these entries will lead to a matrix that isn't invertible and therefore would not be counted. Therefore, $|GL_n(F)| < q^{n^2}$. □

7. Let p be a prime. Prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$ (do not just quote the order formula in this section). [Subtract the number of 2×2 matrices which are *not* invertible from the total number of 2×2 matrices over $\mathbb{F}_p$. You may use the fact that a 2×2 matrix is not invertible if and only if one row is a multiple of the other.]

Proof. Since $|\mathbb{F}_p| = p$ and $n = 2$ we see that a matrix in $GL_2(\mathbb{F}_p)$ can have p^4 variants [Exercise 6 had q^{n^2} possibilities before subtracting]. Now, we need to subtract the amount of matrices that are not invertible. A 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ will not be invertible if $ad - bc = 0 \implies ad = bc$ Looking at ad first we see that $ad = bc \implies ad = k$ for some $k \in \mathbb{F}_p$.

If $k = 0$, then there are p choices each for a and p but we only need one of the cases when either a or b are zero so we subtract 1. That is, there are $(2p - 1)$ choices for $ad = 0$. From the same reasoning, we have $(2p - 1)$ choices for $bc = 0$. When $k \neq 0$ there are $(p - 1)$ choices of a and d that add up to k. With the same reasoning for $bc = k$ we have another $(p - 1)$ choices. Lastly, we need to take into account that for k itself, there are $(p - 1)$ choices.

Therefore, all together we have

$$(2p-1)^2 + (p-1)^3 = 4p^2 - 4p + 1 + p^3 - 3p^2 + 3p - 1 = p^3 + p^2 - p$$

non-invertible matrices. Subtracting this from the p^4 variants that we calculated before gives the desired formula $p^4 - p^3 - p^2 + p$. □

8. Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F.

Proof. Let $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$.

Then, $AB = \begin{pmatrix} [a_1a_2 + b_1c_2] & [a_1b_2 + b_1d_2] \\ [c_1a_2 + d_1c_2] & [c_1b_2 + d_1d_2] \end{pmatrix}$ and $BA = \begin{pmatrix} [a_2a_1 + b_2c_1] & [a_2b_1 + b_2d_1] \\ [c_2a_1 + d_2c_1] & [c_2b_1 + d_2d_1] \end{pmatrix}$.

Looking at the top left corner entry in AB and BA we see that $[a_1a_2 + b_1c_2] \neq [a_2a_1 + b_2c_1]$ if $b_1c_2 \neq b_2c_1$. As there can obviously be matrices where this condition exists, and that even in the event that $n > 2$ we could still have the condition $b_1c_2 \neq b_2c_1$ in the sum of the entry under investigation. Additionally, as 0 and 1 are elements of any field, we see that this condition can exist with simply having $b_1c_2 = 1$ and $b_2c_1 = 0$ so that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F. □

9. Prove that the binary operation of matrix multiplication of 2×2 matrices with real number entries is associative.

Proof. Let $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ and $C = \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$

Then, $AB = \begin{pmatrix} [a_1a_2 + b_1c_2] & [a_1b_2 + b_1d_2] \\ [c_1a_2 + d_1c_2] & [c_1b_2 + d_1d_2] \end{pmatrix}$ and $BC = \begin{pmatrix} [a_2a_3 + b_2c_3] & [a_2b_3 + b_2d_3] \\ [c_2a_3 + d_2c_3] & [c_2b_3 + d_2d_3] \end{pmatrix}$.

$$A(BC) = \begin{pmatrix} [a_1(a_2a_3 + b_2c_3) + b_1(c_2a_3 + d_2c_3)] & [a_1(a_2b_3 + b_2d_3) + b_1(c_2b_3 + d_2d_3)] \\ [c_1(a_2a_3 + b_2c_3) + d_1(c_2a_3 + d_2c_3)] & [c_1(a_2b_3 + b_2d_3) + d_1(c_2b_3 + d_2d_3)] \end{pmatrix}$$

$$A(BC) = \begin{pmatrix} [a_1a_2a_3 + a_1b_2c_3 + b_1c_2a_3 + b_1d_2c_3] & [a_1a_2b_3 + a_1b_2d_3 + b_1c_2b_3 + b_1d_2d_3] \\ [c_1a_2a_3 + c_1b_2c_3 + d_1c_2a_3 + d_1d_2c_3] & [c_1a_2b_3 + c_1b_2d_3 + d_1c_2b_3 + d_1d_2d_3] \end{pmatrix}$$

$$(AB)C = \begin{pmatrix} [(a_1a_2 + b_1c_2)a_3 + (a_1b_2 + b_1d_2)c_3] & [(a_1a_2 + b_1c_2)b_3 + (a_1b_2 + b_1d_2)d_3] \\ [(c_1a_2 + d_1c_2)a_3 + (c_1b_2 + d_1d_2)c_3] & [(c_1a_2 + d_1c_2)b_3 + (c_1b_2 + d_1d_2)d_3] \end{pmatrix}$$

$$(AB)C = \begin{pmatrix} [a_1a_2a_3 + b_1c_2a_3 + a_1b_2c_3 + b_1d_2c_3] & [a_1a_2b_3 + b_1c_2b_3 + a_1b_2d_3 + b_1d_2d_3] \\ [c_1a_2a_3 + d_1c_2a_3 + c_1b_2c_3 + d_1d_2c_3] & [c_1a_2b_3 + d_1c_2b_3 + c_1b_2d_3 + d_1d_2d_3] \end{pmatrix}$$

Therefore, $(AB)C = A(BC)$. □

10. Let $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, a \neq 0, c \neq 0\}$.

(a) Compute the product of $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ to show that G is closed under matrix multiplication.

Proof. $$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$$

Since both $a_1 \neq 0$ and $a_2 \neq 0 \implies a_1a_2 \neq 0$. Same goes for $c_1 \neq 0$ and $c_2 \neq 0 \implies c_1c_2 \neq 0$. It is also easy to see that $a_1b_2 + b_1c_2 \in \mathbb{R}$ as $\mathbb{R}$ is a field (so closed under addition and multiplication). □

(b) Find the matrix inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduct that G is closed under inverses.

Proof. $A^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix}$

$det(A) = \frac{1}{ac}$ is nonzero so A is invertible. a and c swapped places and are both nonzero. $-b$ is obviously in $\mathbb{R}$. Therefore, $A^{-1} \in G$ and G is closed under inverses. □

(c) Deduce that G is a subgroup of $GL_2(\mathbb{R})$ [Exercise 26, Section 1].

Proof. Since G is closed under multiplication and inverses by parts (a) and (b) we now need to show that it is associative and contains the identity element.

associative -

Let $A = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$

From part (a) we saw that $AB = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$

Let $C = \begin{pmatrix} a_3 & b_3 \\ 0 & c_3 \end{pmatrix}$

$$(AB)C = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \begin{pmatrix} a_3 & b_3 \\ 0 & c_3 \end{pmatrix} = \begin{pmatrix} a_1a_2a_3 & a_1a_2b_3 + a_1b_2c_3 + b_1c_2c_3 \\ 0 & c_1c_2c_3 \end{pmatrix}$$
$$BC = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} a_3 & b_3 \\ 0 & c_3 \end{pmatrix} = \begin{pmatrix} a_2a_3 & a_2b_3 + b_2c_3 \\ 0 & c_2c_3 \end{pmatrix}$$
$$A(BC) = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2a_3 & a_2b_3 + b_2c_3 \\ 0 & c_2c_3 \end{pmatrix} = \begin{pmatrix} a_1a_2a_3 & a_1a_2b_3 + a_1b_2c_3 + b_1c_2c_3 \\ 0 & c_1c_2c_3 \end{pmatrix}$$

Therefore, G is associative.

identity - By part (b) we see that G has inverses and therefore we have that $A^{-1}A = I$.

As an example,

$$A^{-1}A = \tfrac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Therefore, G is a subgroup of $GL_2(\mathbb{R})$. □

(d) Prove that the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $GL_2(\mathbb{R})$.

Proof. Since G is closed under multiplication and inverses by parts (a) and (b) we now need to show that it is associative and contains the identity element.

associative - from part (c) if we set $c_1 \mapsto a_1, c_2 \mapsto a_2, c_3 \mapsto a_3$ then $A(BC) = (AB)C$.

identity - from part (c) if we set $c \mapsto a$, we still see that $A^{-1}A = I$.

Therefore, the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $GL_2(\mathbb{R})$. □

The next exercise introduces the *Heisenberg group* over the field F and develops some of its basic properties. When $F = \mathbb{R}$ this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interpretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally — for example, with entries in $\mathbb{Z}$.

11. Let $H(F) = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \}$ — called the *Heisenberg group* over F. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ be elements of $H(F)$.

(a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

Proof. $XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}$

This shows us that $H(F)$ is closed under matrix multiplication. However, had we had the matrices in reverse order we would have had the product dc as part of the sum for the top right entry of the matrix instead of the product af as we see here. Therefore, as an example, any matrix with $af \neq dc$ will not commute.

$$\text{Let } A = \begin{pmatrix} 1 & 5 & 6 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 3 & 7 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & 5 & 6 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 7 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 8 & 33 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix}$$

$$BA = \begin{pmatrix} 1 & 3 & 7 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 5 & 6 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 8 & 19 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} \square$$

$\square$

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

Proof. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$

$$\text{Then } X^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

$$\text{As, } XX^{-1} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Therefore, $H(F)$ is closed under inverses. $\square$

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative).

Proof. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}$$

$$YZ = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & g+d & h+di+e \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix}$$

$$(XY)Z = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & g+d+a & h+di+ai+e+af+b \\ 0 & 1 & i+c+f \\ 0 & 0 & 1 \end{pmatrix}$$

$$X(YZ) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g+d & h+di+e \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & g+d+a & h+di+ai+e+af+b \\ 0 & 1 & i+c+f \\ 0 & 0 & 1 \end{pmatrix}$$

Since only the 3 positions in the top triangle of the matrix change (a, b, c in the definition), we see that the order of the group is $|F|^3$ since there are $|F|$ choices for each. □

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

The elements of the finite group $H(\mathbb{Z}/2\mathbb{Z})$ are

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}1&1&1\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}, \begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix}, \begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}, \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}$$

and their orders are

$$|\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}| = 1, |\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}| = 2, |\begin{pmatrix}1&1&1\\0&1&0\\0&0&1\end{pmatrix}| = 2, |\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}| = 4, |\begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix}| =$$
$$2, |\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}| = 2, |\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}| = 4, |\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}| = 2$$

(e) Prove that every non-identity element of the group $H(\mathbb{R})$ has infinite order.

Proof. $$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} = \begin{pmatrix}1&2a&2b+ac\\0&1&2c\\0&0&1\end{pmatrix}$$

As we can see, the order will be infinite as the three entries in the top right corner will grow without bound when $a, b, c \in \mathbb{R}$.

Therefore, every non-identity element of the group $H(\mathbb{R})$ has infinite order. □

1.5 THE QUATERNION GROUP

1. Compute the order of each of the elements in Q_8.

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

Since $i \cdot i = -1$ and $(-1)(-1) = 1$ we see that:

$|1| = 1, |-1| = 2, |i| = 4, |-i| = 4, |j| = 4, |-j| = 4, |k| = 4, |-k| = 4$

2. Write out the group tables for S_3, D_8 and Q_8.

$S_3 =$

$*$	1	$(1\ 2)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	$(1\ 2)$
1	1	$(1\ 2)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	1	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 3)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3\ 2$	1	$(1\ 2\ 3)$	$(1\ 3)$	$(1\ 2)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	1	$(1\ 2)$	$(2\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3)$	$(1\ 2)$	$(2\ 3)$	$(1\ 3\ 2)$	1
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2)$	1	$(1\ 2\ 3)$

$$D_8 = \begin{array}{cccccccc} * & 1 & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \\ 1 & 1 & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \\ r & r & r^2 & r^3 & 1 & sr & sr^2 & sr^3 & s \\ r^2 & r^2 & r^3 & 1 & sr & sr^2 & sr^3 & s & sr \\ r^3 & r^3 & 1 & r & r^2 & sr^3 & s & sr & sr^2 \\ s & s & sr & sr^2 & sr^3 & 1 & r & r^2 & r^3 \\ sr & sr & sr^2 & sr^3 & s & r & r^2 & r^3 & 1 \\ sr^2 & sr^2 & sr^3 & s & sr & r^2 & r^3 & 1 & r \\ sr^3 & sr^3 & s & sr & sr^2 & r^3 & 1 & r & r^2 \end{array}$$

$$Q_8 = \begin{array}{cccccccc} * & 1 & -1 & i & -i & j & -j & k & -k \\ 1 & 1 & -1 & i & -i & j & -j & k & -k \\ -1 & -1 & 1 & -i & i & -j & j & -k & k \\ i & i & -i & -1 & 1 & k & -k & -j & j \\ -i & -i & i & 1 & -1 & -k & k & j & -j \\ j & j & -j & -k & k & -1 & 1 & i & -i \\ -j & -j & j & k & -k & 1 & -1 & -i & i \\ k & k & -k & j & -j & -i & i & -1 & 1 \\ -k & -k & k & -j & j & i & -i & 1 & -1 \end{array}$$

3. Find a set of generators and relations for Q_8.

We can generate all of Q_8 with $-1, i, j, k$ and the relations are $(-1)(-1) = 1, i^2 = j^2 = k^2 = ijk = -1$.

Therefore a group presentation for Q_8 is $\langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$.

Note: This is only one of several presentations for Q_8.

1.6 HOMOMORPHISMS AND ISOMORPHISMS

Let G and H be groups.

1. Let $\varphi : G \to H$ be a homomorphism.

(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

Proof. Since φ is a homomorphism we have that $\varphi(x \cdot x) = \varphi(x)\varphi(x)$. We will use this and induction for the proof.

base case - $\varphi(x) = \varphi(x)^1$.

induction hypothesis - Suppose that $\varphi(x^{n-1}) = \varphi(x)^{n-1}$.

induction step - Given $\varphi(x^n)$ we have that

$$\begin{aligned} \varphi(x^n) &= \varphi(xx^{n-1}) \\ &= \varphi(x)\varphi(x^{n-1}) && [\varphi(x \cdot x) = \varphi(x)\varphi(x)] \\ &= \varphi(x)\varphi(x)^{n-1} && [\text{induction hypothesis}] \\ &= \varphi(x)^{1+(n-1)} && [\text{base case}] \\ &= \varphi(x)^n \end{aligned}$$

Therefore, $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$. □

(b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

Proof. For part (a) we proved it for positive n. The case $n = 0$ is taken care of by the property of a homomorphism that $\varphi(1) = 1$ [i.e., anything raised to the power of zero is 1].

Let 1_G and 1_H be the identity elements for the groups G and H, respectively. Then,

$$\begin{aligned}
\varphi(x) &= \varphi(x \cdot 1_G) \\
\varphi(x) &= \varphi(x)\varphi(1_G) \\
\varphi(x)^{-1}\varphi(x) &= \varphi(x)^{-1}\varphi(x)\varphi(1_G) \\
\varphi(x)^{-1}\varphi(x) &= \varphi(1_G) \\
\varphi(x)^{-1}\varphi(x) &= \varphi(xx^{-1}) \\
\varphi(x)^{-1}\varphi(x) &= \varphi(x)\varphi(x^{-1}) \\
\varphi(x)\varphi(x^{-1}) &= \varphi(x)\varphi(x)^{-1} \\
\varphi(x)^{-1}\varphi(x)\varphi(x^{-1}) &= \varphi(x)^{-1}\varphi(x)\varphi(x)^{-1} \\
\varphi(x^{-1}) &= \varphi(x)^{-1}
\end{aligned}$$

base case - $\varphi(x^{-1}) = \varphi(x)^{-1}$

induction hypothesis - $\varphi(x^{-(n-1)}) = \varphi(x)^{-(n-1)}$

induction step - Given $\varphi(x^{-n}) = \varphi(x)^{-n}$ we have that

$$\begin{aligned}
\varphi(x^{-n}) &= \varphi(x^{-1}x^{-(n-1)}) \\
&= \varphi(x^{-1})\varphi(x^{-(n-1)}) && [\varphi(x \cdot x) = \varphi(x)\varphi(x)] \\
&= \varphi(x^{-1})\varphi(x)^{-(n-1)} && [\text{induction hypothesis}] \\
&= \varphi(x)^{-1-(n-1)} = \varphi(x)^{-n} && [\text{base case}]
\end{aligned}$$

Therefore, coupled with proof from part (a) we see that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$. □

2. If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?

Proof. We know that $\varphi(x^n) = \varphi(x)^n$ and also that $\varphi(1_G) = 1_H$ [Exercise 1].

Therefore, $x^k = 1_G \implies |x| = k$ while $\varphi(1_G) = \varphi(x^k) = \varphi(x)^k = 1_H \implies |\varphi(x)| = k$. Since x, and therefore $\varphi(x)$, was arbitrary, this shows that $|x| = |\varphi(x)|$ for all $x \in G \mapsto \varphi(x) \in H$. Thus, since two isomorphic groups have the same number of elements, they will also have the same number of elements of order n for each $n \in \mathbb{Z}^+$.

If φ is only assumed to be a homomorphism then it may not be an injective homomorphism which means that the number of elements with the same orders may not match, so no, the result may not still be true. □

3. If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

Proof. If G is abelian then for $x, y \in G$:

$$xy = yx$$

$$\varphi(xy) = \varphi(yx)$$
$$\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$$

Therefore, H is abelian.

Conversely, if H is abelian then for $\varphi(x), \varphi(y) \in H$:

$$\begin{aligned} \varphi(x)\varphi(y) &= \varphi(y)\varphi(x) \\ \varphi(xy) &= \varphi(yx) \\ xy &= yx \qquad \text{[since } \varphi \text{ is an isomorphism and thus an injection (1-1)]} \end{aligned}$$

Therefore, G is abelian.

If φ is a homomorphism and G is abelian then we do not need any additional conditions on φ as the first part of the proof shows above. □

4. Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Proof. Assume there is an isomorphism $\varphi : \mathbb{C} - \{0\} \to \mathbb{R} - \{0\}$. Then, since $\varphi(1) = 1 \implies 1 = \varphi(1) = \varphi((-1)(-1)) = \varphi(-1)^2$. Therefore, $\varphi(-1) = \pm 1$ but since φ is injective and $\varphi(1) = 1$, we must then have that $\varphi(-1) = -1$.

Thus, we now have

$$-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$$

Since $\varphi(i) \in \mathbb{R} - \{0\}$, $\varphi(i)^2$ must be a positive number. Thus, we have reached a contradiction. Therefore, the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic. □

5. Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Proof. Assume there is an isomorphism $\varphi : \mathbb{R} \to \mathbb{Q}$. Since these are additive groups we have that

$$\begin{aligned} \varphi(2) &= \varphi(1+1) \\ &= \varphi(1) + \varphi(1) \end{aligned}$$

We know that for a homomorphism that we have $1 = \varphi(1)$ so therefore $\varphi(2) = 1 + 1 = 2$. We know that a homomorphism has the property $\varphi(x^n) = \varphi(x)^n$ [Exercise 1], so that

$$2 = \varphi(2) = \varphi(\sqrt{2}\sqrt{2}) = \varphi(\sqrt{2}^2) = \varphi(\sqrt{2})^2$$

However, $\varphi(\sqrt{2}) \in \mathbb{Q}$ so there exist integers m, n with no common factors such that $\frac{m}{n} = \varphi(\sqrt{2})$. Therefore,

$$\begin{gathered} (\tfrac{m}{n})^2 = \varphi(\sqrt{2})^2 = 2 \\ \text{so that} \\ m^2 = 2n^2. \end{gathered}$$

This shows us that m^2 must be even, which means that m is even so that we can write $m = 2t$ for integer t. This leads to

$$\begin{aligned}(2t)^2 &= 2n^2\\ 4t^2 &= 2n^2\\ 2t^2 &= n^2\end{aligned}$$

which shows that n^2 is even and therefore n is even as well.

However, this is a contradiction as we assumed that m, n had no common factors. Therefore, the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic. □

6. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Proof. Assume there is an isomorphism $\varphi : \mathbb{Q} \to \mathbb{Z}$. Since these are additive groups we have that

$$\varphi(1) = \varphi(\tfrac{1}{2} + \tfrac{1}{2}) = \varphi(\tfrac{1}{2}) + \varphi(\tfrac{1}{2})$$

We know that for a homomorphism that we have $1 = \varphi(1)$ so therefore

$$1 = \varphi(\tfrac{1}{2}) + \varphi(\tfrac{1}{2})$$

Since $\varphi(\frac{1}{2}) \in \mathbb{Z}$ this must be an integer but there isn't an integer that when summed with itself that equals 1. Thus, we have reached a contradiction.

Therefore, the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic. □

7. Prove that D_8 and Q_8 are not isomorphic.

Proof. For an isomorphism $\varphi : G \to H$ we know that for all $x \in G, |x| = |\varphi(x)|$. However, D_8 has 5 elements that have order 2 [Exercise 1 of Section 2] while Q_8 only has 1 element with order 2 [Exercise 1 of Section 5]. Therefore, D_8 and Q_8 are not isomorphic. □

8. Prove that if $n \neq m, S_n$ and S_m are not isomorphic.

Proof. The order of S_n and S_m are $|S_n| = n!$ and $|S_m| = m!$. Therefore, since $n \neq m \implies n! \neq m!$. Thus, the orders of these groups are not equal and therefore S_n and S_m are not isomorphic. □

9. Prove that D_{24} and S_4 are not isomorphic.

Proof. For an isomorphism $\varphi : G \to H$ we know that for all $x \in G, |x| = |\varphi(x)|$. Half of a dihedral group's elements have order 2 (all of the the elements that are a multiple of s have order 2 since we can use the relations $s^2 = 1$ and $rs = sr^{-1}$) and there are only 9 elements with order 2 in S_4 [Exercise 4 of Section 3]. Therefore, D_{24} and S_4 are not isomorphic. □

10. Fill in the details of the proof that the symmetric groups $S_\triangle$ and S_Ω are isomorphic if $|\triangle| = |\Omega|$ as follows: let $\theta : \triangle \to \Omega$ be a bijection. Define

$$\varphi : S_\triangle \to S_\Omega \text{ by } \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \text{ for all } \sigma \text{ in } S_\triangle$$

and prove the following:

(a) φ is well-defined, that is, if σ is a permutation of $\triangle$ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.

Proof. Since

$$\begin{aligned} \theta &: \triangle \to \Omega \\ \theta^{-1} &: \Omega \to \triangle \\ \sigma &: \triangle \to \triangle \end{aligned}$$

Hence, $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \implies \varphi(\sigma) : \Omega \to \Omega$ is a permutation of Ω. Therefore, φ is well-defined. □

(b) φ is a bijection from $S_\triangle$ onto S_Ω. [Find a 2-sided inverse for φ.]

Proof. φ^{-1} should be the reverse of φ. Let τ be a permutation of Ω.

$$\begin{aligned} \varphi^{-1}(\tau) &= \theta^{-1} \circ \tau \circ \theta \\ \varphi \circ \varphi^{-1}(\tau) &= \varphi(\theta^{-1} \circ \tau \circ \theta) = \theta \circ (\theta^{-1} \circ \tau \circ \theta) \circ \theta^{-1} = \tau \\ \varphi^{-1} \circ \varphi(\sigma) &= \varphi^{-1}(\theta \circ \sigma \circ \theta^{-1}) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta = \sigma \end{aligned}$$

and so φ indeed has a (2-sided) inverse. □

(c) φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

Proof.

$$\begin{aligned} \varphi(\sigma \circ \tau) &= \theta \circ \sigma\tau \circ \theta^{-1} = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} \\ \varphi(\sigma \circ \tau) &= (\theta \circ \sigma \circ \theta^{-1}) \circ (\theta \circ \tau \circ \theta^{-1}) = \varphi(\sigma) \circ \varphi(\tau) \end{aligned}$$

Therefore, φ is a homomorphism. □

Note the similarity to the *change of basis or similarity* transformations for matrices (we shall see connections between these later in the text).

11. Let A and B be groups. Prove that $A \times B \cong B \times A$.

Proof. Let $a \in A$ and $b \in B$. Let φ be the function that swaps a, b in $(a, b) \in A \times B$ so that $\varphi((a, b)) = (b, a)$. Therefore, φ is a function that maps $A \times B \to B \times A$.

Homomorphism - If $\varphi((a_1, b_1)(a_2, b_2))$, then

$$\begin{aligned} \varphi((a_1, b_1)(a_2, b_2)) &= \varphi((a_1a_2, b_1b_2)) \\ &= (b_1b_2, a_1a_2) \\ &= (b_1, a_1)(b_2, a_2) \\ &= \varphi((a_1, b_1))\varphi((a_2, b_2)) \end{aligned}$$

Therefore, φ is a homomorphism.

injective -

$$\varphi((a_1, b_1)) = \varphi((a_2, b_2))$$

$$(b_1, a_1) = (b_2, a_2)$$

so that $b_1 = b_2$ and $a_1 = a_2$. Therefore, φ is injective.

surjective -

Let $(b_1, a_1) \in B \times A$. Then, we know that

$$\varphi((a_1, b_1)) = (b_1, a_1)$$

Therefore, φ is surjective.

Since we have shown that φ is a homomorphism that is both injective and surjective, φ is a bijection.

Therefore, $A \times B \cong B \times A$. □

12. Let A, B, and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.

Proof. Let $a \in A, b \in B, c \in C$ such that $(a, b) \in G$ and $(b, c) \in H$. Let $\varphi : G \times C \to A \times H$.

homomorphism -

$$\begin{aligned}\varphi(((a_1, b_1), c_1)((a_2, b_2), c_2)) &= \varphi(((a_1a_2, b_1b_2), c_1c_2)) \\ &= (a_1a_2, (b_1b_2, c_1c_2)) \\ &= (a_1, (b_1, c_1))(a_2, (b_2, c_2)) \\ &= \varphi(((a_1, b_1), c_1))\varphi(((a_2, b_2), c_2))\end{aligned}$$

Therefore, φ is a homomorphism.

injective -

$$\begin{aligned}\varphi((a_1, b_1), c_1) &= \varphi((a_2, b_2), c_2) \\ (a_1, (b_1, c_1)) &= (a_2, (b_2, c_2))\end{aligned}$$

so that $a_1 = a_2$ and $(b_1, c_1) = (b_2, c_2) \implies b_1 = b_2$ and $c_1 = c_2$. Therefore, φ is injective.

surjective -

Let $(a_1, (b_1, c_1)) \in A \times H$. Then, we know that

$$\varphi(((a_1, b_1), c_1)) = (a_1, (b_1, c_1))$$

Therefore, φ is surjective.

Since we have shown that φ is a homomorphism that is both injective and surjective, φ is a bijection.

Therefore, $G \times C \cong A \times H$. □

13. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of $\varphi, \varphi(G)$, is a subgroup of H (cf. Exercise 26 of Section 1). Prove that if φ is injective then $G \cong \varphi(G)$.

Proof. To show that $\varphi(G)$ is a subgroup of H we need to show that it contains the identity element, inverses, and its elements are associative.

identity - Since φ is a homomorphism we know that $\varphi(1_G) = 1_H$. Therefore, $1_H \in \varphi(G)$.

inverses - Since $\varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ we know that $\varphi(g^{-1}) = \varphi(g)^{-1}$ [Exercise 1].

Therefore, we see that given $g^{-1} \in G$ we have $\varphi(g)^{-1} \in H$.

associative - Since φ is a homomorphism we know that $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$. Therefore, since the binary relation for the group G is associative we see that

$$\begin{aligned} g_1(g_2g_3) &= (g_1g_2)g_3 \\ \varphi(g_1(g_2g_3)) &= \varphi((g_1g_2)g_3) \\ \varphi(g_1)\varphi((g_2g_3)) &= \varphi((g_1g_2))\varphi(g_3) \\ \varphi(g_1)(\varphi(g_2)\varphi(g_3)) &= (\varphi(g_1)\varphi(g_2))\varphi(g_3) \end{aligned}$$

Thus, $\varphi(G)$ is associative.

Therefore, $\varphi(G)$ is a subgroup of H.

Additionally, if φ is injective then since we already know that it is surjective (since for all $h \in \varphi(G), \exists g \in G$ such that $\varphi(g) = h$, which is trivially true from the definition of this homomorphism), this would make it a bijection and therefore $G \cong \varphi(G)$. □

14. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the *kernel* of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup (cf. Exercise 26 of Section 1) of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

Proof. identity - Since φ is a homomorphism we already know that $1_H = \varphi(1_G)$, therefore $1_G \in \ker\varphi$.

inverses - Suppose that $g \in \ker\varphi, g \neq 1_G$. Then,

$$\begin{aligned} \varphi(g) &= 1_H \\ \varphi(g^{-1})\varphi(g) &= \varphi(g^{-1}) \\ \varphi(g^{-1}g) &= \varphi(g^{-1}) \\ \varphi(1_G) &= \varphi(g^{-1}) \\ 1_H &= \varphi(g^{-1}) \end{aligned}$$

Therefore, $\ker\varphi$ contains inverses.

associative - Suppose that $g_1, g_2, g_3 \in \ker\varphi$. Then

$$\varphi(g_1) = \varphi(g_2) = \varphi(g_3) = 1_H$$

Thus,

$$\begin{aligned} (\varphi(g_1)\varphi(g_2))\varphi(g_3) &= \varphi(g_1)(\varphi(g_2)\varphi(g_3)) \\ (\varphi(g_1g_2))\varphi(g_3) &= \varphi(g_1)(\varphi(g_2g_3)) \\ \varphi((g_1g_2)g_3) &= \varphi(g_1(g_2g_3)) \end{aligned}$$

$$\varphi((g_1g_2)g_3) = \varphi(g_1(g_2g_3))$$

so that $(g_1g_2)g_3 = g_1(g_2g_3)$. Therefore, $\ker\varphi$ is associative.

Since $\ker\varphi$ contains the identity element, inverses, and is associative, it is a subgroup of G. □

Now, prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

Proof. If φ is injective, then there can only be one $g \in G$ such that $\varphi(g) = 1_H$. Therefore, $\ker\varphi$ only contains this one element g and we know that this must be equal to 1_G as homomorphisms map identities to identities (i.e., $\varphi(1_G) = 1_H$).

For the converse direction, we will prove the contrapositive.

If $\ker\varphi$ is *not* the identity subgroup of G then it contains two or more elements that equal 1_G. Let g_1, g_2 be two of these elements. Then,

$$\begin{gathered}\varphi(g_1) = 1_H \text{ and } \varphi(g_2) = 1_H \\ \varphi(g_1) = \varphi(g_2)\end{gathered}$$

but since $g_1 \neq g_2$ we see that we have two elements of G that map to the same element in H. Therefore, φ is *not* injective.

Therefore, φ is injective if and only if the kernel of φ is the identity subgroup of G. □

15. Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 14).

Proof. $\pi((x_1, y_1) + (x_2, y_2)) = \pi((x_1 + x_2, y_1 + y_2)) = x_1 + x_2 = \pi((x_1, y_1)) + \pi((x_2, y_2))$

Since any $y \in \mathbb{R}$ suffices $\pi((0, y)) = 0$, where 0 is the additive identity for $\mathbb{R}$ we see that $\ker\pi = \{(0, y) \mid y \in \mathbb{R}\}$. □

16. Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).

Proof. $\pi_1((a_1, b_1)(a_2, b_2)) = \pi_1((a_1a_2, b_1b_2)) = a_1a_2 = \pi_1((a_1, b_1))\pi_1((a_2, b_2))$

$\ker\pi_1 = \{(1, b) \mid b \in B\}$

$$\pi_2((a_1, b_1)(a_2, b_2)) = \pi_2((a_1a_2, b_1b_2)) = b_1b_2 = \pi_2((a_1, b_1))\pi_1((a_2, b_2))$$

$\ker\pi_2 = \{(a, 1) \mid a \in A\}$ □

17. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Proof. If the map $g \mapsto g^{-1}$ is a homomorphism, then, letting us denote it as φ, we see that

$$\begin{aligned}
\varphi(g_1g_2) &= \varphi(g_1)\varphi(g_2) \\
(g_1g_2)^{-1} &= \varphi(g_1)\varphi(g_2) \\
g_2^{-1}g_1^{-1} &= \varphi(g_1)\varphi(g_2) \\
\varphi(g_2)\varphi(g_1) &= \varphi(g_1)\varphi(g_2) \\
\varphi(g_2g_1) &= \varphi(g_1g_2)
\end{aligned}$$

so that $g_1g_2 = g_2g_1$. Therefore, G is abelian.

Conversely, if G is abelian then

$$\varphi(g_1g_2) = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = g_1^{-1}g_2^{-1} = \varphi(g_1)\varphi(g_2)$$

Therefore, φ is a homomorphism. □

18. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Proof. Let us denote the map $g \mapsto g^2$ as φ.

If φ is a homomorphism, then

$$\begin{aligned}
\varphi(g_1g_2) &= \varphi(g_1)\varphi(g_2) && \text{[definition of homomorphism]} \\
\varphi(g_1g_2) &= g_1^2g_2^2 && \text{[definition of mapping]} \\
(g_1g_2)^2 &= g_1^2g_2^2 && \text{[definition of mapping]} \\
g_1g_2g_1g_2 &= g_1^2g_2^2
\end{aligned}$$

Thus, G is abelian.

Conversely, if G is abelian then

$$\begin{aligned}
\varphi(g_1g_2) &= (g_1g_2)^2 \\
&= g_1g_2g_1g_2 \\
&= g_1g_1g_2g_2 && [G \text{ is abelian}] \\
&= g_1^2g_2^2 \\
&= \varphi(g_1)\varphi(g_2)
\end{aligned}$$

Thus, φ is a homomorphism.

Therefore, the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian. □

19. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

Proof. Let us denote the map $z \mapsto z^k$ as φ.

For $k > 1$ and $\varphi(z) = z^k$ we have that

$$\varphi(z_1z_2) = (z_1z_2)^k$$

$$
\begin{aligned}
&= z_1^k z_2^k && \text{[since complex numbers are commutative]} \\
&= z_1^k z_2^k \\
&= \varphi(z_1)\varphi(z_2)
\end{aligned}
$$

Therefore, φ is a homomorphism.

surjective -

Let $z_1 = z^k \in \varphi(G)$. Then, we know that $z = \sqrt[k]{z_1}$ and

$$
\begin{aligned}
\varphi(z) &= \varphi(\sqrt[k]{z_1}) \\
&= (\sqrt[k]{z_1})^k \\
&= z_1
\end{aligned}
$$

Therefore, φ is surjective.

injective -

Counterexample, let $z_1 = i$ and $z_2 = 1$. Obviously $i \neq 1$ but we have that $z_1^4 = z_2^4$. Therefore, we have multiple elements of G that map to the same element in $\varphi(G)$. Therefore, φ is not injective and thus it is not an isomorphism. □

20. Let G be a group and let $Aut(G)$ be the set of all isomorphisms from G onto G. Prove that $Aut(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $Aut(G)$ are called *automorphisms* of G).

Proof. $Aut(G) = \{\varphi : G \to G \mid \varphi \text{ is an isomorphism}\}$.

identity - the isomorphism $\varphi(g) = g$ is the identity.

inverses - by definition every isomorphism has an inverse (bijections have inverses that are themselves bijections), which is also an isomorphism.

associative - function composition is associative by definition.

closure - composition of two isomorphisms is another isomorphism.

Therefore, $Aut(G)$ is a group under function composition. □

21. Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from $\mathbb{Q}$ to itself defined by $q \mapsto kq$ is an automorphism of $\mathbb{Q}$ (cf. Exercise 20).

Proof. Let $\varphi : \mathbb{Q} \to \mathbb{Q}$ such that $\varphi(q) = kq$ for some nonzero $k \in \mathbb{Q}$.

homomorphism -

$$
\begin{aligned}
\varphi(q_1 + q_2) &= k(q_1 + q_2) \\
&= kq_1 + kq_2 \\
&= \varphi(q_1) + \varphi(q_2)
\end{aligned}
$$

Therefore, φ is a homomorphism.

injective -

$$\begin{aligned}\varphi(q_1) &= \varphi(q_2)\\ k_1 q_1 &= k_2 q_2\end{aligned}$$

so that $q_1 = q_2$ since k is fixed. Therefore, φ is injective.

surjective -

Let $t \in \mathbb{Q}$ and note that tk^{-1} is also in $\mathbb{Q}$.

$$\begin{aligned}\varphi(tk^{-1}) &= ktk^{-1}\\ &= tkk^{-1}\\ &= t\end{aligned}$$

Therefore, φ is surjective.

Since we have shown that φ is a homomorphism that is both injective and surjective, φ is a bijection on to itself, making it an automorphism. □

22. Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).

Proof. Let $\varphi : A \to A$ such that $\varphi(a) = a^k$ for some fixed $k \in \mathbb{Z}$.

homomorphism -

$$\begin{aligned}\varphi(a_1 a_2) &= (a_1 a_2)^k\\ &= a_1^k a_2^k && \text{[since } A \text{ is abelian]}\\ &= \varphi(a_1)\varphi(a_2)\end{aligned}$$

Therefore, φ is a homomorphism. Since $a^k \in A$ it is from A to itself.

If $k = -1$, then

injective -

$$\begin{aligned}\varphi(a_1) &= \varphi(a_2)\\ a_1^{-1} &= a_2^{-1}\\ a_1 a_1^{-1} &= a_1 a_2^{-1}\\ 1 &= a_1 a_2^{-1}\\ 1a_2 &= a_1 a_2^{-1} a_2\\ a_2 &= a_1\end{aligned}$$

Therefore, φ is injective.

surjective -

Let $a \in A$ and note that a^{-1} is also in A.

$$\varphi(a^{-1}) = (a^{-1})^{-1} = a$$

Therefore, φ is surjective.

Since we have shown that φ is a homomorphism from A to itself that is both injective and surjective when $k = -1$, it is therefore an automorphism of A. □

23. Let G be a finite group which possesses an automorphism σ (cf. Exercise 20) such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism is called *fixed point free* of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]

Proof. The hints suggest showing that every element in G can be represented as $x^{-1}\sigma(x)$. Therefore, we need to prove that the map $x \mapsto x^{-1}\sigma(x)$ is a bijection. If we show that this map is injective, since the group G is finite and domain and codomain are the same, this will show that it is bijective.

$$\begin{aligned}
g_1^{-1}\sigma(g_1) &= g_2^{-1}\sigma(g_2) \\
g_1 g_1^{-1}\sigma(g_1) &= g_1 g_2^{-1}\sigma(g_2) \\
\sigma(g_1) &= g_1 g_2^{-1}\sigma(g_2) \\
\sigma(g_1)\sigma(g_2)^{-1} &= g_1 g_2^{-1}\sigma(g_2)^{-1} \\
\sigma(g_1)\sigma(g_2)^{-1} &= g_1 g_2^{-1} \\
\sigma(g_1 g_2^{-1}) &= g_1 g_2^{-1} \\
\sigma(g_1 g_2^{-1}) &= 1
\end{aligned}$$

so that $g_1 = g_2$, which shows that the map $x \mapsto x^{-1}\sigma(x)$ is a bijection.

Now following the second suggestion in the hints

$$\sigma(g^{-1}\sigma(g)) = \sigma(g^{-1})\sigma(\sigma(g)) = \sigma(g^{-1})g$$

Therefore, σ maps elements to their inverses as $g^{-1}\sigma(g)$ and $\sigma(g^{-1})g$ are inverses. Now we see that,

$$\begin{aligned}
\sigma(g_1 g_2) &= \sigma(g_1 g_2) \\
(g_1 g_2)^{-1} &= \sigma(g_1)\sigma(g_2) \\
g_2^{-1} g_1^{-1} &= g_1^{-1} g_2^{-1}
\end{aligned}$$

Therefore, G is abelian. □

24. Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$. [See Exercise 6 in Section 2.]

Proof. Since G has generators x and y with $x^2 = y^2 = 1$ then the elements of G are $x, xy, xyx, \ldots$ and $y, yx, yxy, \ldots$ and since G is finite, at some point one of these will equal the identity element, so we will be done. The identity element cannot be an element like $xyxyx$, because we can multiple both sides by x (or y when appropriate) so that

$$\begin{aligned}
xyxyx &= 1 \\
xxyxyxx &= xx = 1 \\
yxy &= 1 \\
yyxyy &= yy = 1
\end{aligned}$$

$$x = 1$$

where the same logic can be applied for $yxyxy$ as well. Therefore, the identity element will be of the form $(xy)^n$.

Therefore, the presentation for G is

$$\langle x, y \mid x^2 = y^2 = (xy)^n = 1 \rangle$$

Additionally, since $x^2 = 1, y^2 = 1 \implies x = x^{-1}, y = y^{-1}$ we see that if we let $r = xy$ then

$$\begin{aligned} rx &= (xy)x \\ &= x(yx) \\ &= x(y^{-1}x^{-1}) \\ &= x(xy)^{-1} \\ &= xr^{-1} \end{aligned}$$

The presentation of G can now be shown to be isomorphic to D_{2n} by letting $r = xy$ and $s = x$. We showed that D_{2n} can also be generated by s and sr [Exercise 3 of Section 2] which maps to x and xxy, respectively. But $xxy = y$ since $x^2 = 1$. Thus, we can denote the presentation for G as

$$\langle s, sr \mid s^2 = (sr)^2 = (r)^n = 1, rs = sr^{-1} \rangle$$

Therefore, $G \cong D_{2n}$, where $n = |xy|$. □

25. Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.

(a) Prove that the matrix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is the matrix of the linear transformation which rotates the x, y plane about the origin in a counterclockwise direction by θ radians.

Proof. A point in the x, y plane can be represented by a column vector $\begin{pmatrix} x \\ y \end{pmatrix}$.

We can see that this transformation does not move the origin

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

and that it moves the x-axis (unit vector pointing in the x direction) to

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

and that it moves the y-axis (unit vector pointing in the y direction) to

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

and finally, for any general point (x, y) to

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}$$

This shows that the matrix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is the matrix of the linear transformation which rotates the x, y plane about the origin in a counterclockwise direction by θ radians. □

(b) Prove that the map $\varphi : D_{2n} \to GL_2(\mathbb{R})$ defined on generators by

$$\varphi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ and } \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.

Proof. For φ to be a homomorphism we need $\varphi(rr) = \varphi(r)\varphi(r)$ and $\varphi(ss) = \varphi(s)\varphi(s)$.

$$\varphi(rr) = \varphi(r^2) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^2 = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \varphi(r)\varphi(r)$$

Additionally, $\varphi(r^2) \in GL_2(\mathbb{R})$ because

$$\varphi(r^2) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos^2\theta\text{-}\sin^2\theta & -2\cos\theta\sin\theta \\ 2\cos\theta\sin\theta & \cos^2\theta\text{-}\sin^2\theta \end{pmatrix}$$

and $\det(\varphi(r^2)) = \cos^4\theta + 2\cos^2\theta\sin^2\theta + \sin^4\theta \neq 0$

$$\varphi(ss) = \varphi(s^2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \varphi(s)\varphi(s)$$

Additionally, $\varphi(s^2) \in GL_2(\mathbb{R})$ because $\varphi(s^2) = \varphi(1) = 1$ as we can see here

$$\varphi(s^2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$$

Therefore, $\varphi : D_{2n} \to GL_2(\mathbb{R})$ extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$. □

(c) Prove that the homomorphism φ in part (b) is injective.

Proof. $\varphi(r_1) = \varphi(r_2)$

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}_1 = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}_2$$

$r_1 = r_2$

as the *rotation* of θ radians is the same for both matrices so they represent the same *rotation*.

$$\varphi(s_1) = \varphi(s_2)$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_2$$
$$s_1 = s_2$$

Therefore, φ is injective. □

26. Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $GL_2(\mathbb{C})$ defined on generators by

$$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \text{ and } \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism. Prove that φ is injective.

Proof. homomorphism -

$$\varphi(ii) = \varphi(i^2) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}^2 = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} = \varphi(i)\varphi(i)$$
$$\varphi(jj) = \varphi(j^2) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \varphi(j)\varphi(j)$$

injective -

$$\varphi(i_1) = \varphi(i_2)$$
$$\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}_1 = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}_2$$
$$i_1 = i_2$$

as the matrices are constants, this trivially shows there is only one i.

The same argument suffices for $\varphi(j)$. □

1.7 GROUP ACTIONS

1. Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a = ga$, where $g \in F^\times, a \in F$ and ga is the usual product in F of the two field elements (state clearly which axioms in the definition of a field are used).

Proof. Let $f_1, f_2 \in F^\times$ and $a \in F$, then

$$f_1 \cdot (f_2 \cdot a) = (f_1 f_2) \cdot a \qquad \text{[field elements are associative]}$$
$$1 \cdot a = a, \text{ for all } a \in F \qquad \text{[1 is the multiplicative identity of } F^\times\text{]}$$

This shows that the multiplicative group $F^\times$ *acts* on F. □

2. Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

Proof. Let $z_1, z_2, a \in \mathbb{Z}$, then

$$\begin{aligned} z_1 \cdot (z_2 \cdot a) = z_1 + (z_2 + a) = (z_1 + z_2) + a \qquad & \text{[addition is commutative in } \mathbb{Z}\text{]} \\ 0 \cdot a = 0 + a = a, \text{ for all } a \in \mathbb{Z} \qquad & \text{[0 is the identity element of the additive group } \mathbb{Z}\text{]} \end{aligned}$$

This shows that the additive group $\mathbb{Z}$ *acts* on itself. □

3. Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Proof. Let $r_1, r_2 \in \mathbb{R}$ and $(x, y) \in \mathbb{R} \times \mathbb{R}$, then

$$\begin{aligned} r_1 \cdot (r_2 \cdot (x, y)) &= r_1 \cdot (x + r_2 y, y) \\ &= ((x + r_2 y) + r_1 y, y) \\ &= (x + (r_2 + r_1) y, y) \\ &= (r_2 \cdot r_1) \cdot (x, y) \end{aligned}$$

where $\cdot$ in $(r_1 \cdot r_2)$ is the group operation of the additive group $\mathbb{R}$.

$$0 \cdot (x, y) = (x + 0y, y) = (x, y)$$

This shows that the additive group $\mathbb{R}$ *acts* on the x, y plane $\mathbb{R} \times \mathbb{R}$. □

4. Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G (cf. Exercise 26 of Section 1):

(a) the kernel of the action.

Proof. The kernel of the action is the group $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.

Let g_1, g_2 in the kernel of the action and $a \in A$, then

identity - Since G is a group that acts on A we know that $1 \cdot a = a$ by definition. Therefore, by definition, the kernel of the action always contains the identity element.

associative - Since G is a group that acts on A we know that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ by definition. Since g_1, g_2 are in the kernel of the action this becomes $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (a) = a$ so that the kernel of the action is associative.

inverses - Since $1 \cdot a = a$

$$\begin{aligned} 1 \cdot a &= (g^{-1} g) \cdot a \\ &= g^{-1} \cdot (g \cdot a) \\ &= g^{-1} \cdot a \\ &= a \end{aligned}$$

Thus, the kernel of the action contains inverses.

Therefore, the kernel of the action is a subgroup of G. □

(b) $\{g \in G \mid ga = a\}$ — this subgroup is called the *stabilizer* of a in G.

Proof. We can use the same proof as part (a) above. That proof used an arbitrary a to account for *all* $a \in A$, whereas for the *stabilizer* of a in G we would use a *specific* a. The proofs are therefore the same. □

5. Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$ (cf. Exercise 14 in Section 6).

Proof. The identity element of S_A is the permutation that does nothing to the elements of A and leaves them *all* fixed. The kernel of $G \to S_A$ is all of the elements of G that map to the identity of element of S_A which is the permutation that does nothing and keep the elements of A fixed (i.e., it is the fiber over the identity of A). This is exactly what the kernel of an action of the group G on the set A is, by definition. Therefore, they must be equal. □

6. Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.

Proof. If a group G acts faithfully on a set A then we know it is an action in which the associated permutation representation is injective. Therefore, the kernel of the corresponding permutation representation $G \to S_A$ only contains the identity element [Exercise 14 of Section 6] and therefore the kernel of the action only contains the identity element [Exercise 5].

Conversely, if the kernel of the action only contains the identity element then so too does the kernel of the corresponding permutation representation $G \to S_A$ [Exercise 5]. Since the kernel of the corresponding permutation only contains the identity element it is injective [Exercise 14 of Section 6] and therefore the group G acts faithfully on the set A. □

7. Prove that in Example 2 in this section the action is faithful.

Proof. In Example 2 we have $V = \mathbb{R}^n$ and $F = \mathbb{R}$ where the group action is specified by

$$\alpha(r_1, r_2, \ldots, r_n) = (\alpha r_1, \alpha r_2, \ldots, \alpha r_n)$$

for all $\alpha \in \mathbb{R}, (r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$, where αr_i is just multiplication of two real numbers.

The kernel of the associated permutation representation $\mathbb{R} \to \mathbb{R}^n$ is the elements of $\mathbb{R}$ that map to the identity permutation. The identity permutation is the permutation that does nothing to the elements of $\mathbb{R}^n$ and leaves them *fixed*.

The only element in $\mathbb{R}$ that has this capability is the multiplicative identity of $\mathbb{R}^\times$, i.e. 1. Since this is the only element in the kernel of the associated permutation representation we know that the kernel of the group action only contains the identity element as these two groups are equal [Exercise 5] and therefore the action is *faithful* [Exercise 6]. □

8. Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}$.

(a) Prove that this is a group action.

Proof. Let $\sigma_1, \sigma_2 \in S_A$ and $\{a_1, \ldots, a_k\} \in B$.

Since symmetric groups are groups under function composition we see that

$$\sigma_1 \cdot (\sigma_2 \cdot \{a_1, \ldots, a_k\}) \implies \sigma_1 \circ (\sigma_2 \circ \{a_1, \ldots, a_k\})$$
$$\sigma_1 \circ (\sigma_2 \circ \{a_1, \ldots, a_k\}) = (\sigma_1 \circ \sigma_2) \circ \{a_1, \ldots, a_k\} \qquad \text{[function composition is associative]}$$

Let 1 be the identity permutation of S_A, then

$$1 \cdot \{a_1, \ldots, a_k\} = \{1(a_1), \ldots, 1(a_k)\} = \{a_1, \ldots, a_k\}$$

Therefore, this is a group action. □

(b) Describe explicitly how the elements (1 2) and (1 2 3) act on the six 2-element subsets of $\{1, 2, 3, 4\}$.

The six 2-element subsets of $\{1, 2, 3, 4\}$ are $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$.

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

9. Do both parts of the preceding exercise with "ordered k-tuples" in place of "k-element subsets", where the action k-tuples is defined as above but with set braces replaced by parentheses (note that, for example, the 2-tuples $(1, 2)$ and $(2, 1)$ are different even though the sets $\{1, 2\}$ and $\{2, 1\}$ are the same, so the sets being acted upon are different).

(a) Prove that this is a group action.

Proof. Let $\sigma_1, \sigma_2 \in S_A$ and $(a_1, \ldots, a_k) \in B$.

Since symmetric groups are groups under function composition we see that

$$\sigma_1 \cdot (\sigma_2 \cdot (a_1, \ldots, a_k)) \implies \sigma_1 \circ (\sigma_2 \circ (a_1, \ldots, a_k))$$
$$\sigma_1 \circ (\sigma_2 \circ (a_1, \ldots, a_k)) = (\sigma_1 \circ \sigma_2) \circ (a_1, \ldots, a_k) \qquad \text{[function composition is associative]}$$

Let 1 be the identity permutation of S_A, then

$$1 \cdot (a_1, \ldots, a_k) = (1(a_1), \ldots, 1(a_k)) = (a_1, \ldots, a_k)$$

Therefore, this is a group action. □

(b) Describe explicitly how the elements (1 2) and (1 2 3) act on the twelve 2-element subsets of $(1, 2, 3, 4)$.

The twelve 2-element subsets of $(1, 2, 3, 4)$ are:

$(1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1), (2, 3), (3, 2), (2, 4), (4, 2), (3, 4), (4, 3)$.

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

10. With reference to the preceding two exercises determine:

(a) for which values of k the action of S_n on k-element subsets is faithful, and

If $k = n$, then the only subset is the set itself. All permutations of this set, S_n, leave the set fixed. Therefore, the kernel of the action is S_n, which is obviously not faithful.

If $k = 1$, then the subsets are the singletons of n. The only permutation that can keep these subsets all fixed is the identity permutation of S_n. Therefore, this value of k is faithful.

If $k > 1$ and $k \neq n$, then the there will be subsets that share the same elements among themselves which means there will not be a single permutation that can fix all the subsets, except for the identity permutation of S_n. Therefore, this value of k is faithful.

Thus, for $k < n$ the action of S_n on k-element subsets is faithful.

(b) for which values of k the action of S_n on ordered k-tuples is faithful.

If $k = n$, we would have n ordered n-tuples. As theses tuples are all distinct, any permutation other than the identity permutation would change them, which means they would not be fixed. Therefore, this value of k is faithful.

If $k = 1$, then the ordered tuples are the singletons of n. The only permutation that can keep these tuples all fixed is the identity permutation of S_n. Therefore, this value of k is faithful.

If $k > 1$ and $k \neq n$, then the there will be tuples that share the same elements among themselves which means there will not be a single permutation that can fix all these tuples, except for the identity permutation of S_n. Therefore, this value of k is faithful.

Thus, for $k \leq n$ the action of S_n on k-element subsets is faithful.

11. Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square (where the vertices of the square are labeled as in Section 2).

In Section 2 the text states (there is also a figure of the labeled square that makes up D_8)

> Fix a regular n-gon centered at the origin in an x, y plane and label the vertices consecutively from 1 to n in a clockwise manner. Let r be the rotation clockwise about the origin through $2\pi/n$ radian. Let s be the reflection about the line of symmetry through vertex 1 and the origin.

The elements of D_8 are $\{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ and the corresponding permutations in S_4 are:

$$\{1,(1\ 2\ 3\ 4),(1\ 3)(2\ 4),(1\ 4\ 3\ 2),(2\ 4),(1\ 4)(2\ 3),(1\ 3),(1\ 2)(3\ 4)\}$$

12. Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action (label vertices as usual).

Proof. Let n be even and let the n-gon be labeled clockwise as $0, 2, \ldots, n-1$ and let us denote the set of ordered pairs as:

$$\{a_i\} = \{(i, i + \tfrac{n}{2}) \mid 0 \leq i < \tfrac{n}{2}\}$$

Since D_{2n} is generated from r and s, where r a clockwise rotation (n rotations) and s is a reflection about an axis through two vertices ($n/2$ axes of reflection) we see that we can represent the action of D_{2n} on the elements of $\{a_i\}$ as:

$$\begin{aligned} r^k a_i &\equiv a_{(i-k)} \pmod{n} \\ s^k a_i &\equiv a_{(i-kn/2)} \pmod{n} \end{aligned}$$

Now we will show that these meet the properties of a group action:

Let $g_1, g_2 \in D_{2n}$ such that $g_1 = s^a r^b$ and $g_2 = s^c r^d$

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &\implies s^a r^b \cdot (s^c r^d \cdot a_i) \\ &\implies s^a r^b \cdot a_{((i-d)-cn/2)} \\ &\implies a_{((((i-d)-cn/2)-b)-an/2)} \\ &\implies (s^a r^b s^c r^c) \cdot a_i \\ &\implies (g_1 g_2) \cdot a_i \end{aligned}$$

$$\begin{aligned} r^n \cdot a_i \equiv a_{(i-n)} \pmod{n} &\implies 1 \cdot a_i \equiv a_i \pmod{n} \\ s^2 \cdot a_i \equiv a_{(i-2n/2)} \pmod{n} &\implies 1 \cdot a_i \equiv a_i \pmod{n} \end{aligned}$$

Therefore, $1 \cdot a_i = a_i$ for all $a_i \in \{a_i\}$. Thus, we have shown this a group action.

The kernel of this action is $r^n = s^2 = 1 \implies \{1\}$. □

13. Find the kernel of the left regular action.

Proof. The left regular action is when the group G acts on itself with the map $g : a \mapsto ga$ for all $a \in G$.

Therefore, the kernel of the left regular action is the identity element of G as all other elements of G will not have this property for *all* $a \in G$. □

14. Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.

Proof. The first property of a group action (left) would give:

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (ag_2) = (ag_2g_1)$$
$$\text{but}$$
$$(g_1g_2) \cdot a = (ag_1g_2).$$

However, since G is non-abelian we see that

$$(ag_2g_1) \neq (ag_1g_2) \implies g_1 \cdot (g_2 \cdot a) \neq (g_1g_2) \cdot a.$$

Therefore, these maps do not satisfy the axioms of a (left) group action of G on itself. □

15. Let G be a group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action of G on itself.

Proof.

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot (ag_2^{-1}) \\ &= (ag_2^{-1}g_1^{-1}) \\ &= (a(g_1g_2)^{-1}) \\ &= (g_1g_2) \cdot a \end{aligned}$$

Thus, $g = 1 \implies 1 \cdot a = a1^{-1} = a$.

Therefore, these maps do satisfy the axioms of a (left) group action of G on itself. □

16. Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action (this action of G on itself is called *conjugation*).

Proof.

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot (g_2ag_2^{-1}) \\ &= g_1(g_2ag_2^{-1})g_1^{-1} \\ &= (g_1g_2)a(g_1g_2)^{-1} \\ &= (g_1g_2) \cdot a \end{aligned}$$

Thus, $g = 1 \implies 1 \cdot a = 1a1^{-1} = a$.

Therefore, these maps do satisfy the axioms of a (left) group action of G on itself. □

17. Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by

$$x \mapsto gxg^{-1}$$

For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an automorphism of G — [Exercise 20 of Section 6]). Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).

Proof. Let the map for the conjugation by g $x \mapsto gxg^{-1}$ be denoted by φ. To prove this is an automorphism we must show that it is a bijective homomorphism.

homomorphism -

$$\begin{aligned}\varphi(x \cdot y) &= g(xy)g^{-1} \\ &= g(x1y)g^{-1} \\ &= g(xg^{-1}gy)g^{-1} \\ &= (gxg^{-1})(gyg^{-1}) \\ &= \varphi(x)\varphi(y)\end{aligned}$$

Therefore, φ is a homomorphism.

injective -

$$\begin{aligned}\varphi(x_1) = \varphi(x_2) \\ gx_1g^{-1} = gx_2g^{-1} \\ g^{-1}(gx_1g^{-1}) = g^{-1}(gx_2g^{-1}) \\ x_1g^{-1} = x_2g^{-1} \\ (x_1g^{-1})g = (x_2g^{-1})g \\ x_1 = x_2\end{aligned}$$

Therefore, φ is injective.

surjective -

Let $z_1 = z^k \in \varphi(G)$. Then, we know that $z = \sqrt[k]{z_1}$ and

$$\varphi(z) = \varphi(\sqrt[k]{z_1}) = (\sqrt[k]{z_1})^k = z_1$$

Therefore, φ is surjective.

Let $x_1 = gxg^{-1} \in \varphi(G)$. Then, we know that $x = g^{-1}x_1g$ and

$$\varphi(x) = g(g^{-1}x_1g)g^{-1} = x_1$$

Therefore, φ is surjective.

Since, φ is a bijective homomorphism from G onto itself, it is an automorphism. □

$|x|$ and $|gxg^{-1}|$ have the same order for all of x because $|x| \implies$

$$\begin{aligned}x^n = 1 \\ g^nx^n = g^n\end{aligned}$$

$$g^n x^n g^{-n} = g^n g^{-n} = 1$$
$$(gxg^{-1})n = 1$$

Thus, $|gxg^{-1}| = 1$.

Additionally, for any subset A of G since we know that the map $x \mapsto gxg^{-1}$ is a bijection then $a \mapsto gag^{-1}$ is a 1-1 map and therefore the cardinality of A and gAg^{-1} must be the same.

18. Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \text{ if and only if } a = hb \text{ for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence class of x under $\sim$ is called the *orbit* of x under the action of H. The orbits under the action of H partition the set A.)

Proof. To prove that $\sim$ is an equivalence relation we need to show that that it is reflexive, symmetric, and transitive.

Let h, h^{-1} be elements in H, then

reflexive -

$$\text{If } a \sim a, \text{ then } a = ha.$$

Therefore, $\sim$ is reflexive.

symmetric -

$$\text{If } a \sim b, \text{ then } a = hb \implies h^{-1}a = b \implies b \sim a.$$

Therefore, $\sim$ is symmetric.

transitive -

$$\text{If } a \sim b \text{ and } b \sim c \text{ then, } a = hb \text{ and } b = hc \text{ so that } a = h(hc) \implies a = h^2c \implies a \sim c.$$

Therefore, $\sim$ is an equivalence relation. □

19. Let H be a subgroup (cf. Exercise 26 of Section 1) of the finite group G and let H act on G (here $A+G$) by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map

$$H \to \mathcal{O} \text{ defined by } h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exercise deduce *Lagrange's Theorem*:

if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

Proof. Let us denote the map $h \mapsto hx$ as φ.

To show that it is a bijection we need to show that it is injective and surjective.

injective -

$$\begin{aligned} \varphi(h_1) &= \varphi(h_2) \\ h_1 x &= h_2 x \\ h_1 x x^{-1} &= h_2 x x^{-1} \\ h_1 &= h_2 \end{aligned}$$

Therefore, φ is injective.

surjective -

Let $o = hx \in \mathcal{O}$. Then, we know that $h = ox^{-1}$ and

$$\varphi(h) = \varphi(ox^{-1}) = ox^{-1}x = ox$$

Therefore, φ is surjective.

Since φ is a bijection, all orbits have the same cardinality as $|H|$. Since orbits are for all $x \in G$ and since orbits are an equivalence relation from Exercise 18, the orbits under the action of H partition the set G. Therefore we must have that $|G| = n|H|$, where n is the number of orbits that partition G. Since this is the equation for $|H| \mid |G|$ we do indeed see that $|H|$ divides $|G|$. □

20. Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4.

Proof. The total amount of rigid motions for a tetrahedron is 12 [Exercise 9 of Section 2].

To show that these rigid motions are isomorphic to a subgroup of S_4 we can show there is subgroup which consists of these rigid motions. First, for a tetrahedron there are 4 axes of rotation through the center of a face and the opposite side vertex which give 8 permutations. Second, there are 3 axes of rotation through the center of opposing edges which give 3 permutations. These rotations, coupled with the identity rotation gives us 12 rigid motions. Now let's see what rigid motions map to which permutations of S_4:

The permutations about the center of a face and opposite side vertex are: (1 2 3), (1 3 2), (2 3 4), (2 4 3), (1 3 4), (1 4 3), (1 2 4), (1 4 2)

The permutations about the centers of opposing edges are: (1 4)(2 3), (1 3)(2 4), (1 2)(3 4)

Thus, the group of rigid motions are:

{1, (1 2 3), (1 3 2), (2 3 4), (2 4 3), (1 3 4), (1 4 3), (1 2 4), (1 4 2), (1 4)(2 3), (1 3)(2 4), (1 2)(3 4)}

Therefore, the group of rigid motions of a tetrahedron is isomorphic to a subgroup of S_4. □

21. Show that the group of rigid motions of a cube is isomorphic to S_4. [This group acts on the set of four pairs of opposite vertices.]

Proof. The total amount of rigid motions for a cube is 24 [Exercise 10 of Section 2].

To show that these rigid motions are isomorphic to S_4 we can show that the rigid motions are all of the permutations of S_4 where we will use the permutation on the 4 pairs of opposing vertices. Let us label them $(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)$, where all of the a_i are on a single face and where all of the b_i are all

on the opposite face. First, for a cube there are 3 axes of rotation through the centers of opposing faces which give 9 rotations. Second, there are 4 axes of rotation through the opposing vertices (a_i, b_i) which gives us 8 rotations. Third, there are 6 axes of rotation through the center of opposing edges which give 6 rotations. These rotations, coupled with the identity rotation gives us 24 rigid motions. Now let's see what rigid motions map to which permutations of S_4:

Let $1 = (a_1, b_1), 2 = (a_2, b_2), 3 = (a_3, b_3), 4 = (a_4, b_4)$.

The permutations about the center of opposing faces are: (1 2 3 4), (1 3)(2 4), (1 4 3 2), (1 2 4 3), (1 4)(2 3), (1 3 4 2), (1 4 2 3), (1 2)(3 4), (1 3 2 4)

The permutations about opposing vertices are: (2 3 4), (2 4 3), (1 3 4), (1 4 3), (1 2 4), (1 4 2), (1 3 2), (1 2 3)

The permutations about the centers of opposing edges are: (1 3), (2 4), (1 4), (2 3), (1 2), (3 4)

Therefore, including the identity rotation, the group of rigid motions of a cube are all of S_4 and thus they are obviously isomorphic. □

22. Show that the group of rigid motions of an octahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4. [This group acts on the set of four pairs of opposite faces.] Deduce that the groups of rigid motions of a cube and an octahedron are isomorphic. (These groups are isomorphic because these solids are "dual" — see *Introduction to Geometry* by H. Coxeter, Wiley, 1961. We shall see later that the groups of rigid motions of the dodecahedron and icosahedron are isomorphic as well — these solids are also dual.)

Proof. Let us denote the 4 opposite pairs of faces of the octahedron as $(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)$.

To show that these rigid motions are isomorphic to a subgroup of S_4 we can show there is subgroup which consists of these rigid motions. We will use the permutation on the 4 pairs of opposing faces. Let us label them $(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)$, where all of the a_i are on a single pyramid and where all of the b_i are all on the opposite pyramid. First, for an octahedron there are 3 axes of rotation through the centers of opposing vertices which give 9 rotations. Second, there are 4 axes of rotation through the opposing faces (a_i, b_i) which gives us 8 rotations. Third, there are 6 axes of rotation through the center of opposing edges which give 6 rotations. These rotations, coupled with the identity rotation gives us 24 rigid motions. Now let's see what rigid motions map to which permutations of S_4:

Let $1 = (a_1, b_1), 2 = (a_2, b_2), 3 = (a_3, b_3), 4 = (a_4, b_4)$.

The permutations about the center of opposing vertices are: (1 2 3 4), (1 3)(2 4), (1 4 3 2), (1 2 4 3), (1 4)(2 3), (1 3 4 2), (1 4 2 3), (1 2)(3 4), (1 3 2 4)

The permutations about opposing faces are: (2 3 4), (2 4 3), (1 3 4), (1 4 3), (1 2 4), (1 4 2), (1 3 2), (1 2 3)

The permutations about the centers of opposing edges are: (1 3), (2 4), (1 4), (2 3), (1 2), (3 4)

Therefore, including the identity rotation, the group of rigid motions of an octahedron are all of S_4 and thus they are obviously isomorphic. Since the group of rigid motions of a cube is also isomorphic to S_4, we therefore have that the group of rigid motions of a cube and octahedron are isomorphic. □

23. Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.

Proof. The group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful because

there are multiple rotations that map to the identity element. For example, the rotations about the axes through the center of the faces all have order 2. Let us denote these rotations about the three different axes as r_1, r_2, r_3. That is,

$$|r_1| = |r_2| = |r_3| = 2$$

Therefore, the kernel of this action is $\{1, r_1^2, r_2^2, r_3^2\}$. □