Group Theory Exercises 1

Jason Sass

July 17, 2023

Binary Operations

Exercise 1. Let $a, b, c, x \in \mathbb{R}$.

If $ax^2 + bx + c = 0$ and $a \neq 0$, then $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

Proof. Suppose $ax^2 + bx + c = 0$ and $a \neq 0$.

Since $a \neq 0$ we can divide by a and simplify to get $x^2 + \frac{bx}{a} = \frac{-c}{a}$.

Completing the square we get $x^2 + 2(\frac{b}{2a})x + (\frac{b}{2a})^2 = \frac{-c}{a} + (\frac{b}{2a})^2$.

We simplify to obtain $(x + \frac{b}{2a})^2 = \frac{b^2-4ac}{4a^2}$.

Taking the square root and simplifying we obtain $x + \frac{b}{2a} = \pm\frac{\sqrt{b^2-4ac}}{2a}$.

Therefore, $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$. □

Exercise 2. If $*$ is an associative and commutative binary operation on a set S, then $(a * b) * (c * d) = [(d * c) * a] * b$ for all $a, b, c, d \in S$.

Proof. Suppose $*$ is an associative and commutative binary operation on a set S.

Let $a, b, c, d \in S$.

Then

$$\begin{aligned} (a * b) * (c * d) &= (c * d) * (a * b) \\ &= [(c * d) * a] * b \\ &= [(d * c) * a] * b. \end{aligned}$$

□

Exercise 3. Let $*$ be defined by $a * b = ab + 1$ for all $a, b \in \mathbb{Q}$.

Is $*$ a binary operation on $\mathbb{Q}$?

If so, is $*$ associative or commutative?

Proof. We prove $*$ is a binary operation on $\mathbb{Q}$.

Let $a, b \in \mathbb{Q}$.

Then $a * b = ab + 1$.

Since $\mathbb{Q}$ is closed under addition and multiplication, then $ab + 1 \in \mathbb{Q}$.

Therefore, $a * b \in \mathbb{Q}$.

Since $ab + 1$ is uniquely determined by a and b, then $a * b$ is unique.

Since $a * b \in \mathbb{Q}$ and $a * b$ is unique, then $*$ is a binary operation on $\mathbb{Q}$.

We prove $*$ is not associative.

Since $(1 * 2) * 3 = 3 * 3 = 10$, but $1 * (2 * 3) = 1 * 7 = 8$ and $10 \neq 8$, then $*$ is not associative.

We prove $*$ is commutative.

Let $a, b \in \mathbb{Q}$.

Since $a * b = ab + 1 = ba + 1 = b * a$, then $a * b = b * a$.

Therefore $a * b = b * a$ for all $a, b \in \mathbb{Q}$, so $*$ is commutative. □

Exercise 4. Let $*$ be defined by $a * b = a - b$ for all $a, b \in \mathbb{Q}$.

Is $*$ a binary operation on $\mathbb{Q}$?

If so, is $*$ associative or commutative?

Solution. We observe that $*$ is subtraction defined on $\mathbb{Q}$. □

Proof. We prove $*$ is a binary operation on $\mathbb{Q}$.

Let $a, b \in \mathbb{Q}$.

Since $a \in \mathbb{Q}$, then $a = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ and $n \neq 0$.

Since $b \in \mathbb{Q}$, then $b = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$ and $q \neq 0$.

Observe that $a * b = a - b = \frac{m}{n} - \frac{p}{q} = \frac{mq-np}{nq}$.

Since $\mathbb{Z}$ is closed under multiplication and subtraction, then $mq - np \in \mathbb{Z}$ and $nq \in \mathbb{Z}$.

Since $n \neq 0$ and $q \neq 0$, then $nq \neq 0$.

Since $mq - np \in \mathbb{Z}$ and $nq \in \mathbb{Z}$ and $nq \neq 0$, then $\frac{mq-np}{nq} \in \mathbb{Q}$, so $a * b \in \mathbb{Q}$.

Since $\frac{mq-np}{nq}$ is uniquely determined by m, n, p, q, then $a * b$ is uniquely determined by a and b, so $a * b$ is unique.

Since $a * b \in \mathbb{Q}$ and $a * b$ is unique, then $*$ is a binary operation on $\mathbb{Q}$.

We prove $*$ is not associative.

Since $(1 * 2) * 3 = (1 - 2) - 3 = -4$, but $1 * (2 * 3) = 1 - (2 - 3) = 2$ and $-4 \neq 2$, then $*$ is not associative.

We prove $*$ is not commutative.

Since $1 * 5 = 1 - 5 = -4$, but $5 * 1 = 5 - 1 = 4$ and $-4 \neq 4$, then $*$ is not commutative. □

Exercise 5. Let $(S, *)$ be an associative binary structure.

If $*$ is commutative, then $\{a \in S : a * a = a\}$ is closed under $*$.

Solution. Let $T = \{a \in S : a * a = a\}$.

We note the condition $a * a = a$ means each element of T is an idempotent for the binary operation *. □

Proof. Suppose $*$ is commutative.

Let $T = \{a \in S : a * a = a\}$.

To prove T is closed under $*$, let $x, y \in T$.

We must prove $x * y \in T$.

Since $x \in T$, then $x \in S$ and $x * x = x$.

Since $y \in T$, then $y \in S$ and $y * y = y$.

Since $(S, *)$ is a binary structure, then S is closed under $*$.

Since $x \in S$ and $y \in S$, then this implies $x * y \in S$.

Observe that

$$\begin{aligned} x * y &= (x * x) * (y * y) \\ &= x * (x * y) * y \\ &= x * (y * x) * y \\ &= (x * y) * (x * y). \end{aligned}$$

Since $x * y \in S$ and $(x * y) * (x * y) = x * y$, then $x * y \in T$. □

Exercise 6. How many different binary operations exist on a finite set?

Solution. Let S be a finite set.

Then there exists $n \in \mathbb{Z}^+$ such that $|S| = n$.

Let t represent the number of different binary operations on S.

Let $T = \{* | *$ is a binary operation defined on $S\}$.

Then $t = |T|$.

Observe that $t =$ the number of different binary structures on $S =$ the number of different ways to create a binary structure on $S =$ the number of different binary structure tables.

We enumerate each element of S.

Thus, let $S = \{a_1, a_2, a_3, ..., a_n\}$.

How many different ways exist to create a binary structure table ?

The task is to assign a value to each pair of elements in the table of n rows and n columns.

The total number of ways to assign a value to each pair = number of different ways to create a binary structure.

We assign a value to first pair, then assign a value to 2nd pair,... assign value to n^2 pair.

Thus, we use multiplication principle for this sequence of tasks.

Each pair can be assigned one of n possible values.

Thus, the total number of assignments is $n * n * n * ...n = n^{n^2}$.

Hence, there are n^{n^2} different binary structures that can be formed.

Therefore, the number of different binary operations on a finite set of size n is n^{n^2}. □

Exercise 7. How many different commutative binary operations exist on a finite set?

Solution. Let S be a finite set.

Then there exists $n \in \mathbb{Z}^+$ such that $|S| = n$.

Let t represent the number of different commutative binary operations on S.

Let $T = \{*| *$ is a commutative binary operation defined on $S\} = \{* : S \times S \to S| *$ is commutative$\}$.

Observe that $t =$ the number of different ways to create a commutative binary operation on $S =$ the number of different binary structure tables that preserve commutativity $=$ the number of different ways to create a binary structure table that preserves commutativity of $*$.

We enumerate each element of S.

Thus, let $S = \{a_1, a_2, a_3, ..., a_n\}$.

How many different ways exist to create a binary structure table such that commutativity of $*$ is preserved?

The number of ways to create such a binary structure $=$ number of ways to assign a value to each pair of elements in the table of n rows and n columns such that commutativity is preserved.

To preserve commutativity, each $a_i * a_j = a_j * a_i$ for all $i, j \in \{1, 2, .., n\}$.

Thus once we assign values to half of the table, the other half of the table is fixed and completely determined.

Therefore we only have to assign values to half of the table.

Each pair can be assigned one of n values.

Since it doesn't matter which half of the table to choose, we do the bottom half, including the main diagonal.

How many pairs exist in half of the table?

There are 1 pair in first row, 2 pairs in 2nd row, 3 pairs in 3rd row, ... k pairs in k^{th} row, n pairs in n^{th} row.

Therefore, the total number of pairs in half of the table $= 1+2+3+...+n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Since each pair has n possible choices for the assigned value, by the multiplication principle, the total number of assignments is $n^{\frac{n(n+1)}{2}}$.

Therefore, the number of different commutative binary operations on a finite set of size n is $n^{\frac{n(n+1)}{2}}$. □

Groups

Exercise 8. The set of integers $\mathbb{Z}$ under subtraction is not a group.

Solution. Subtraction is a binary operation on $\mathbb{Z}$, but subtraction is not associative.

For example, $(1 - 2) - 3 = -4$, but $1 - (2 - 3) = 2$ and $-4 \neq 2$. □

Exercise 9. The set of integers $\mathbb{Z}$ under multiplication is not a group.

Solution. Multiplication is a binary operation on $\mathbb{Z}$ and multiplication is associative and $1 \in \mathbb{Z}$ is multiplicative identity.

Since $0 \in \mathbb{Z}$ and $0x = 0 = x0$ for all $x \in \mathbb{Z}$, then there is no $x \in \mathbb{Z}$ such that $0x = 1$, so 0 does not have a multiplicative inverse.

Therefore, $\mathbb{Z}$ under multiplication is not a group. □

Exercise 10. The set of non-zero integers $\mathbb{Z}^*$ under multiplication is not a group.

Solution. Let $a, b \in \mathbb{Z}^*$.

Then $a, b \in \mathbb{Z}$ and $a \neq 0$ and $b \neq 0$.

Since $\mathbb{Z}$ is closed under multiplication and $a, b \in \mathbb{Z}$, then $ab \in \mathbb{Z}$.

Since $a, b \in \mathbb{Z}$ and $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

Since $ab \in \mathbb{Z}$ and $ab \neq 0$, then $ab \in \mathbb{Z}^*$, so $\mathbb{Z}^*$ is closed under multiplication.

Therefore, multiplication is a binary operation on $\mathbb{Z}^*$.

Multiplication is associative in $\mathbb{Z}$.

Since $\mathbb{Z}^* \subset \mathbb{Z}$, then multiplication is associative in $\mathbb{Z}^*$.

Since $1 \in \mathbb{Z}$ and $1 \neq 0$, then $1 \in \mathbb{Z}^*$.

Since $1x = 1 = x1$ for all $x \in \mathbb{Z}$ and $\mathbb{Z}^* \subset \mathbb{Z}$, then $1x = 1 = x1$ for all $x \in \mathbb{Z}^*$.

Since $1 \in \mathbb{Z}^*$ and $1x = 1 = x1$ for all $x \in \mathbb{Z}^*$, then 1 is a multiplicative identity in $\mathbb{Z}^*$.

Not every non-zero integer has a multiplicative inverse.

For example, $2 \in \mathbb{Z}^*$, but there is no $n \in \mathbb{Z}^*$ such that $2n = 1$. □

Exercise 11. The set of positive integers $\mathbb{Z}^+$ under multiplication is not a group.

Solution. Let $a, b \in \mathbb{Z}^+$.

Then $a, b \in \mathbb{Z}$ and $a > 0$ and $b > 0$.

Since $\mathbb{Z}$ is closed under multiplication and $a, b \in \mathbb{Z}$, then $ab \in \mathbb{Z}$.

Since $a, b \in \mathbb{Z}$ and $a > 0$ and $b > 0$, then $ab > 0$.

Since $ab \in \mathbb{Z}$ and $ab > 0$, then $ab \in \mathbb{Z}^+$, so $\mathbb{Z}^+$ is closed under multiplication.

Therefore, multiplication is a binary operation on $\mathbb{Z}^+$.

Multiplication is associative in $\mathbb{Z}$.

Since $\mathbb{Z}^+ \subset \mathbb{Z}$, then multiplication is associative in $\mathbb{Z}^+$.

Since $1 \in \mathbb{Z}^+$ and $1 > 0$, then $1 \in \mathbb{Z}^+$.

Since $1x = 1 = x1$ for all $x \in \mathbb{Z}$ and $\mathbb{Z}^+ \subset \mathbb{Z}$, then $1x = 1 = x1$ for all $x \in \mathbb{Z}^+$.

Since $1 \in \mathbb{Z}^+$ and $1x = 1 = x1$ for all $x \in \mathbb{Z}^+$, then 1 is a multiplicative identity in $\mathbb{Z}^+$.

Not every positive integer has a multiplicative inverse.

For example, $2 \in \mathbb{Z}^+$, but there is no $n \in \mathbb{Z}^+$ such that $2n = 1$. □

Exercise 12. The set of nonzero rational numbers $\mathbb{Q}^*$ under addition is not a group.

Solution. Addition is not a binary operation on $\mathbb{Q}^*$ because $\mathbb{Q}^*$ is not closed under addition.

For example, $\frac{1}{2} \in \mathbb{Q}^*$ and $\frac{-1}{2} \in \mathbb{Q}^*$, but the sum is $\frac{1}{2} + \frac{-1}{2} = 0$ and $0 \notin \mathbb{Q}^*$. □

Exercise 13. The set of elements of $\mathbb{Z}_6$ under multiplication modulo 6 is not a group.

Solution. Observe that $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and $|\mathbb{Z}_6| = 6$.

The Cayley table is shown below.

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Observe that $1 \cdot x = x \cdot 1 = x$ for all $x \in \mathbb{Z}_6$, so $1 \in \mathbb{Z}_6$ is multiplicative identity.

Since $0 \cdot x = 0 = x \cdot 0$ for all $x \in \mathbb{Z}_6$, then $0 \in \mathbb{Z}_6$ does not have a multiplicative inverse.

Therefore, not every element of $\mathbb{Z}_6$ has a multiplicative inverse, so $\mathbb{Z}_6$ under multiplication modulo 6 is not a group. □

Exercise 14. The set of nonzero elements of $\mathbb{Z}_6$ under multiplication modulo 6 is not a group.

Solution. Let S be the set of nonzero elements of $\mathbb{Z}_6$.

Then $S = \{1, 2, 3, 4, 5\}$ and $|S| = 5$.

The Cayley table is shown below.

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Since $2 \in S$ and $3 \in S$ and $2 \cdot 3 = 0$ but $0 \notin S$, then S is not closed under multiplication modulo 6.

Therefore, multiplication modulo 6 is not a binary operation on $\mathbb{Z}_6$, so $\mathbb{Z}_6$ under multiplication modulo 6 is not a group. □

Exercise 15. The set of rational numbers $\mathbb{Q}$ under multiplication is not a group.

Solution. Since $1 = \frac{1}{1} \in \mathbb{Q}$ and $1x = x1 = x$ for all $x \in \mathbb{Q}$, then 1 is a multiplicative identity for $\mathbb{Q}$.

Since $0 = \frac{0}{1} \in \mathbb{Q}$ and $0x = 0 = x0$ for all $x \in \mathbb{Q}$, then there is no $x \in \mathbb{Q}$ such that $0x = 1 = x0$.

Therefore, $0 \in \mathbb{Q}$ does not have a multiplicative inverse, so $\mathbb{Q}$ is not a group under multiplication. □

Exercise 16. The set of real numbers $\mathbb{R}$ under multiplication is not a group.

Solution. Since $1 \in \mathbb{R}$ and $1x = x1 = x$ for all $x \in \mathbb{R}$, then 1 is a multiplicative identity for $\mathbb{R}$.

Since $0 \in \mathbb{R}$ and $0x = 0 = x0$ for all $x \in \mathbb{R}$, then there is no $x \in \mathbb{R}$ such that $0x = 1 = x0$.

Therefore, $0 \in \mathbb{R}$ does not have a multiplicative inverse, so $\mathbb{R}$ is not a group under multiplication. □

Exercise 17. The set of complex numbers $\mathbb{C}$ under multiplication is not a group.

Solution. Since $1 = 1 + 0i \in \mathbb{C}$ and $1z = z1 = z$ for all $z \in \mathbb{C}$, then 1 is a multiplicative identity for $\mathbb{C}$.

Since $0 = 0 + 0i \in \mathbb{C}$ and $0z = 0 = z0$ for all $z \in \mathbb{C}$, then there is no $z \in \mathbb{C}$ such that $0z = 1 = z0$.

Therefore, $0 \in \mathbb{C}$ does not have a multiplicative inverse, so $\mathbb{C}$ is not a group under multiplication. □

Exercise 18. The 4^{th} roots of unity $U_4 = \{1, i, -1, -i\}$ under complex multiplication is an abelian group.

Solution. The Cayley table for U_4 is shown below.

·	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

□

Exercise 19. Let $(G, +)$ be an additive group.

Let $a, b \in G$.

If $a + b = 0$, then $b = -a$.

Proof. Suppose $a + b = 0$.

Then

$$\begin{aligned} b &= 0 + b \\ &= (-a + a) + b \\ &= -a + (a + b) \\ &= -a + 0 \\ &= -a. \end{aligned}$$

□

Exercise 20. Let $(G, +)$ be an additive group.
Let $a, b \in G$.
If $a + b = b$, then $a = 0$.

Proof. Suppose $a + b = b$.
Then

$$\begin{aligned} a &= a + 0 \\ &= a + [b + (-b)] \\ &= (a + b) + (-b) \\ &= b + (-b) \\ &= 0. \end{aligned}$$

□

Exercise 21. Analyze the inverses of the group of units of $\mathbb{Z}_3$ under multiplication modulo 3.

Solution. The integers modulo 3 is $\mathbb{Z}_3 = \{0, 1, 2\}$ and $|\mathbb{Z}_3| = 3$.
The group of units of $\mathbb{Z}_3$ under multiplication modulo 3 is $\mathbb{Z}_3^*$.
The order of $\mathbb{Z}_3^*$ is $|\mathbb{Z}_3^*| = \phi(3) = 2$ and $\gcd(a, 3) = 1$ for each $a \in \mathbb{Z}_3^*$.
Hence, $\mathbb{Z}_3^* = \{1, 2\}$.

The Cayley table is shown below.

$\cdot$	1	2
1	1	2
2	2	1

The inverse of each element is shown below.
$1^{-1} = 1$
$2^{-1} = 2$

□

Exercise 22. Analyze the inverses of the group of units of $\mathbb{Z}_5$ under multiplication modulo 5.

Solution. The integers modulo 5 is $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ and $|\mathbb{Z}_5| = 5$.
The group of units of $\mathbb{Z}_5$ under multiplication modulo 5 is $\mathbb{Z}_5^*$.
The order of $\mathbb{Z}_5^*$ is $|\mathbb{Z}_5^*| = \phi(5) = 4$ and $\gcd(a, 5) = 1$ for each $a \in \mathbb{Z}_5^*$.
Hence, $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$.

The Cayley table is shown below.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The inverse of each element is shown below.
$1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$
$4^{-1} = 4$

□

Exercise 23. Analyze the inverses of the group of units of $\mathbb{Z}_7$ under multiplication modulo 7.

Solution. The integers modulo 7 is $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and $|\mathbb{Z}_7| = 7$.
The group of units of $\mathbb{Z}_7$ under multiplication modulo 7 is $\mathbb{Z}_7^*$.
The order of $\mathbb{Z}_7^*$ is $|\mathbb{Z}_7^*| = \phi(7) = 6$ and $\gcd(a, 7) = 1$ for each $a \in \mathbb{Z}_7^*$.
Hence, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

The Cayley table is shown below.

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

The inverse of each element is shown below.
$1^{-1} = 1$
$2^{-1} = 4$
$3^{-1} = 5$
$4^{-1} = 2$
$5^{-1} = 3$
$6^{-1} = 6$

□

Exercise 24. Let $G = \{2, 4, 6, 8\}$ be a subset of $\mathbb{Z}_{10}$.
Define $a * b = ab$ for all $a, b \in G$.
Then $(G, *)$ is a group.

Solution. We can draw the Cayley table for $\mathbb{Z}_{10}$ and G.

The Cayley table for $\mathbb{Z}_{10}$ under multiplication modulo 10 is shown below.

·	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

The Cayley table for G under multiplication modulo 10 is shown below.

·	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

The table shows that G is closed under multiplication modulo 10 and the identity is 6.

Multiplication modulo is associative, so multiplication modulo 10 is associative in G.

The inverse of each element is shown below.
$2^{-1} = 8$
$4^{-1} = 4$
$6^{-1} = 6$
$8^{-1} = 2$

Since G is closed under multiplication modulo 10 and multiplication modulo 10 is associative and $6 \in G$ is a multiplicative identity and each element of G has an inverse in G, then $(G, *)$ is a group.

Since $*$ has symmetry along the main diagonal of the Cayley table, then $*$ is commutative, so $(G, *)$ is an abelian group. □

Exercise 25. Let $G = \{n \in \mathbb{Z} : \text{is odd}\}$.

Then $(G, +)$ is not a group.

Solution. The set of odd integers G under addition is not a group because G is not closed under addition.

For example, both 3 and 5 are odd integers, but the sum $3 + 5 = 8$ is even, not odd. □

Exercise 26. Let $G = \{2^x : x \in \mathbb{Q}\}$.

Then $(G, \cdot)$ is a group.

Proof. We prove $\cdot$ is a binary operation on G.

Let $2^x \in G$ and $2^y \in G$.

Since $2^x \in G$, then $x \in \mathbb{Q}$, so $x = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ and $b \neq 0$.

Since $2^y \in G$, then $y \in \mathbb{Q}$, so $y = \frac{c}{d}$ for $c, d \in \mathbb{Z}$ and $d \neq 0$.

The product is $2^x \cdot x^y = 2^{x+y} = 2^{\frac{a}{b}+\frac{c}{d}} = 2^{\frac{ad+bc}{bd}}$.

Since $\mathbb{Z}$ is closed under addition and multiplication then $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{Z}$.

Since $b \neq 0$ and $d \neq 0$, then $bd \neq 0$.

Thus, $\frac{ad+bc}{bd} \in \mathbb{Q}$, so $2^{x+y} \in G$.

Therefore,, G is closed under multiplication.

Since $2^{x+y} \in G$ is unique, then $\cdot$ is a binary operation on G.

We prove $\cdot$ is associative.

Let $2^x \in G$ and $2^y \in G$ and $2^z \in G$.

Then $x, y, z \in \mathbb{Q}$.

Since addition in $\mathbb{Q}$ is associative, we have

$$\begin{aligned}(2^x \cdot 2^y) \cdot 2^z &= (2^{x+y}) \cdot 2^z \\ &= 2^{(x+y)+z} \\ &= 2^{x+(y+z)} \\ &= 2^x \cdot 2^{y+z} \\ &= 2^x \cdot (2^y \cdot 2^z).\end{aligned}$$

Therefore, $\cdot$ is associative in G.

We prove $1 \in G$ is a multiplicative identity in G.

Since $0 \in \mathbb{Q}$, then $1 = 2^0 \in G$.

Let $2^x \in G$.

Then $x \in \mathbb{Q}$.

Since $\mathbb{Q}$ is closed under addition, we have $2^x \cdot 2^0 = 2^{x+0} = 2^x = 2^{0+x} = 2^0 \cdot 2^x$.

Since $2^0 \in G$ and $2^x \cdot 2^0 = 2^x = 2^0 \cdot 2^x$, then 2^0 is an identity for $*$.

We prove every element of G has an inverse in G.

Let $2^x \in G$.

Then $x \in \mathbb{Q}$, so $-x \in \mathbb{Q}$.

Hence, $2^{-x} \in G$.

Observe that $2^x \cdot 2^{-x} = 2^{x-x} = 2^0 = 2^{-x+x} = 2^{-x} \cdot 2^x$.

Thus, $2^{-x} \in G$ is an inverse of 2^x.

Therefore, the inverse of each element $2^x \in G$ is the element $2^{-x} \in G$.

Since $\cdot$ is a binary operation on G and $\cdot$ is associative and $2^0 \in G$ is a multiplicative identity and the inverse of each element $2^x \in G$ is $2^{-x} \in G$, then $(G, \cdot)$ is a group.

We prove $\cdot$ is commutative.

Let $2^x, 2^y \in G$.

Then $x, y \in \mathbb{Q}$.

Since $2^x \cdot 2^y = 2^{x+y} = 2^{y+x} = 2^y \cdot 2^y$, then $\cdot$ is commutative.

Therefore, $(G, \cdot)$ is an abelian group. □

Exercise 27. Compute the multiplicative inverse of the element $A \in GL_2(\mathbb{Z}_3)$ below.

$$A = \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix}$$

Solution. We solve the equation $AA^{-1} = I$, where I is identity matrix and A^{-1} is the multiplicative inverse of matrix A over $\mathbb{Z}_3$.

After solving this equation, we find that

$$A^{-1} = \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix}$$

We verify that $AA^{-1} = I = A^{-1}A$. □

Exercise 28. Compute the multiplicative inverse of the element $A \in GL_2(\mathbb{Z}_5)$ below.

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

Solution. We solve the equation $AA^{-1} = I$, where I is identity matrix and A^{-1} is the multiplicative inverse of matrix A over $\mathbb{Z}_5$.

After solving this equation, we find that

$$A^{-1} = \begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix}$$

We verify that $AA^{-1} = I = A^{-1}A$. □

Exercise 29. Compute the multiplicative inverse of the element $A \in GL_2(\mathbb{Z}_7)$ below.

$$A = \begin{bmatrix} 3 & 5 \\ 4 & 6 \end{bmatrix}$$

Solution. We solve the equation $AA^{-1} = I$, where I is identity matrix and A^{-1} is the multiplicative inverse of matrix A over $\mathbb{Z}_7$.

After solving this equation, we find that

$$A^{-1} = \begin{bmatrix} 4 & 6 \\ 2 & 2 \end{bmatrix}$$

We verify that $AA^{-1} = I = A^{-1}A$. □

Exercise 30. Analyze the group $GL_2(\mathbb{Z}_2)$.

Solution. Observe that $GL_2(\mathbb{Z}_2)$ is a subset of $M_2(\mathbb{Z}_2)$.

We first enumerate all elements of $M_2(\mathbb{Z}_2)$.

Note that $|M_2(\mathbb{Z}_2)| = 2^4 = 16$, so there are 16 2×2 matrices with entries in $\mathbb{Z}_2 = \{0, 1\}$.

Invertible matrices have non-zero determinant, so we compute the determinant of each matrix and determine if it is non-zero.

$$A_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_3 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_4 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_5 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_6 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_7 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_8 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_9 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ does not have an inverse.}$$

$$A_{10} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = A_{10}^{-1} \text{ . Therefore, } A_{10} \text{ is its own inverse and } A_{10} \text{ is identity matrix.}$$

$$A_{11} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = A_{11}^{-1} \text{ . Therefore, } A_{11} \text{ is its own inverse.}$$

$$A_{12} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = A_{15}^{-1} \text{ . Therefore, } A_{12} \text{ and } A_{15} \text{ are inverses of each other.}$$

$$A_{13} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = A_{13}^{-1} \text{ . Therefore, } A_{13} \text{ is its own inverse.}$$

$$A_{14} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = A_{14}^{-1} \text{ . Therefore, } A_{14} \text{ is its own inverse.}$$

$$A_{15} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = A_{12}^{-1} \text{ . Therefore, } A_{12} \text{ and } A_{15} \text{ are inverses of each other.}$$

$$A_{16} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \text{ does not have an inverse.}$$

Since there are 6 matrices of $M_2(\mathbb{Z}_2)$ that are invertible, then the order of $GL_2(\mathbb{Z}_2)$ is 6.

Therefore, $|GL_2(\mathbb{Z}_2)| = 6$.

The elements of $GL_2(\mathbb{Z}_2)$ are shown below.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I^{-1} \text{ . Therefore, } I \text{ is its own inverse and } I \text{ is identity matrix.}$$

$$B_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = B_1^{-1}\text{ . Therefore, } B_1 \text{ is its own inverse.}$$

$$B_2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = B_5^{-1}\text{ . Therefore, } B_2 \text{ and } B_5 \text{ and are inverses of each other.}$$

$$B_3 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = B_3^{-1}\text{ . Therefore, } B_3 \text{ is its own inverse.}$$

$$B_4 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = B_4^{-1}\text{ . Therefore, } B_4 \text{ is its own inverse.}$$

$$B_5 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = B_2^{-1}\text{ . Therefore, } B_2 \text{ and } B_5 \text{ and are inverses of each other.}$$

We show that $GL_2(\mathbb{Z}_2)$ is non-abelian.

We compute B_1B_2 and B_2B_1.

Observe that

$$B_1B_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

and

$$B_2B_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Since $B_1B_2 \neq B_2B_1$, then matrix multiplication is not commutative in $GL_2(\mathbb{Z}_2)$, so $GL_2(\mathbb{Z}_2)$ is non-abelian.

□

Exercise 31. The group $GL_2(\mathbb{R})$ is non-abelian.

Solution.

$$\text{Let } A = \begin{bmatrix} \frac{1}{2} & \pi \\ \frac{1}{3} & -5 \end{bmatrix}$$

$$\text{Let } B = \begin{bmatrix} 4 & -3 \\ \frac{2}{5} & -7 \end{bmatrix}$$

Then

$$A^{-1} = \begin{bmatrix} 2 - \frac{4\pi}{2\pi+15} & \frac{6\pi}{2\pi+15} \\ \frac{2}{2\pi+15} & -\frac{3}{2\pi+15} \end{bmatrix}$$

and

$$B^{-1} = \begin{bmatrix} \frac{35}{134} & -\frac{15}{134} \\ \frac{1}{67} & -\frac{10}{67} \end{bmatrix}$$

Therefore, $A, B \in GL_2(\mathbb{R})$.

Observe that

$$AB = \begin{bmatrix} \frac{2\pi}{5} + 2 & -7\pi - \frac{3}{2} \\ -\frac{2}{3} & 34 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 4\pi + 15 \\ -\frac{32}{15} & \frac{2\pi}{5} + 35 \end{bmatrix}$$

Since $AB \neq BA$, then matrix multiplication is not commutative, so $GL_2(\mathbb{R})$ is not abelian. □

Exercise 32. List the elements of the multiplicative group of units $(\mathbb{Z}_4^*, \cdot)$.

Solution. The order of $\mathbb{Z}_4^*$ is $|\mathbb{Z}_4^*| = \phi(4) = 2$, so there are 2 elements $a \in \mathbb{Z}_4^*$ that are relatively prime to the modulus 4.

The elements of $\mathbb{Z}_4^*$ are in the set $\{1, 3\}$.

The Cayley table for $\mathbb{Z}_4 *^*$ is shown below.

$\cdot$	1	3
1	1	3
3	3	1

□

Exercise 33. List the elements of the multiplicative group of units $(\mathbb{Z}_6^*, \cdot)$.

Solution. The order of $\mathbb{Z}_6^*$ is $|\mathbb{Z}_6^*| = \phi(6) = 2$, so there are 2 elements $a \in \mathbb{Z}_6^*$ that are relatively prime to the modulus 6.

The elements of $\mathbb{Z}_6^*$ are in the set $\{1, 5\}$.

The Cayley table for $\mathbb{Z}_6 *^*$ is shown below.

$\cdot$	1	5
1	1	5
5	5	1

□

Exercise 34. List the elements of the multiplicative group of units $(\mathbb{Z}_8^*, \cdot)$.

Solution. The order of $\mathbb{Z}_8^*$ is $|\mathbb{Z}_8^*| = \phi(8) = 4$, so there are 4 elements $a \in \mathbb{Z}_8^*$ that are relatively prime to the modulus 8.

The elements of $\mathbb{Z}_8^*$ are in the set $\{1, 3, 5, 7\}$.

The Cayley table for $\mathbb{Z}_8*^*$ is shown below.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

□

Exercise 35. List the elements of the multiplicative group of units $(\mathbb{Z}_{10}^*, \cdot)$.

Solution. The order of $\mathbb{Z}_{10}^*$ is $|\mathbb{Z}_{10}^*| = \phi(10) = 4$, so there are 4 elements $a \in \mathbb{Z}_{10}^*$ that are relatively prime to the modulus 10.

The elements of $\mathbb{Z}_{10}^*$ are in the set $\{1, 3, 7, 9\}$.

The Cayley table for $\mathbb{Z}_{10}*^*$ is shown below.

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

□

Exercise 36. List the elements of the multiplicative group of units $(\mathbb{Z}_{15}^*, \cdot)$.

Solution. The order of $\mathbb{Z}_{15}^*$ is $|\mathbb{Z}_{15}^*| = \phi(15) = 8$, so there are 8 elements $a \in \mathbb{Z}_{15}^*$ that are relatively prime to the modulus 15.

The elements of $\mathbb{Z}_{15}^*$ are in the set $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

The Cayley table for $\mathbb{Z}_{15}*^*$ is shown below.

$\cdot$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

□

Exercise 37. List the elements of the multiplicative group of units $(\mathbb{Z}_{20}^*, \cdot)$.

Solution. The order of $\mathbb{Z}_{20}^*$ is $|\mathbb{Z}_{20}^*| = \phi(20) = 8$, so there are 8 elements $a \in \mathbb{Z}_{20}^*$ that are relatively prime to the modulus 20.

The elements of $\mathbb{Z}_{20}^*$ are in the set $\{1, 3, 7, 9, 11, 13, 17, 19\}$.

The Cayley table for $\mathbb{Z}_{20}*^*$ is shown below.

$\cdot$	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

□

Exercise 38. List the elements of the multiplicative group of units $(\mathbb{Z}_{30}^*, \cdot)$.

Solution. The order of $\mathbb{Z}_{30}^*$ is $|\mathbb{Z}_{30}^*| = \phi(30) = 8$, so there are 8 elements $a \in \mathbb{Z}_{30}^*$ that are relatively prime to the modulus 30.

The elements of $\mathbb{Z}_{30}^*$ are in the set $\{1, 7, 11, 13, 17, 19, 23, 29\}$.

The Cayley table for $\mathbb{Z}_{30}*^*$ is shown below.

$\cdot$	1	7	11	13	17	19	23	29
1	1	7	11	13	17	19	23	29
7	7	19	17	1	29	13	11	23
11	11	17	1	23	7	29	13	19
13	13	1	23	19	11	7	29	17
17	17	29	7	11	19	23	1	13
19	19	13	29	7	23	1	17	11
23	23	11	13	29	1	17	19	7
29	29	23	19	17	13	11	7	1

□

Exercise 39. Define $a * b = a + b + 3$ over $\mathbb{Q}$.

Then $(\mathbb{Q}, *)$ an abelian group.

Proof. We prove $*$ is a binary operation on $\mathbb{Q}$.

Since addition is well-defined on $\mathbb{Q}$, then $a * b = a + b + 3 \in \mathbb{Q}$ is unique for any $a, b \in \mathbb{Q}$, so $\mathbb{Q}$ is closed under $*$.

Since $a * b$ is unique and $\mathbb{Q}$ is closed under $*$, then $*$ is a binary operation on $\mathbb{Q}$.

We prove $*$ is associative.

Let $a, b, c \in \mathbb{Q}$.

Then

$$\begin{aligned}(a*b)*c &= (a+b+3)*c \\ &= [(a+b+3)+c]+3 \\ &= [a+(b+3+c)]+3 \\ &= [a+(b+c+3)]+3 \\ &= [a+(b*c)]+3 \\ &= a*(b*c).\end{aligned}$$

Therefore, $(a*b)*c = a*(b*c)$, so $*$ is associative.

We prove -3 is identity for G.
Observe that $-3 = \frac{-3}{1} \in \mathbb{Q}$.
Let $a \in \mathbb{Q}$.
Then $a*(-3) = a+(-3)+3 = a+0 = a = 0+a = (-3)+3+a = -3+a+3 = (-3)*a$.
Since $-3 \in \mathbb{Q}$ and $a*(-3) = a = (-3)*a$, then -3 is identity for $*$ in $\mathbb{Q}$.

We prove every $a \in \mathbb{Q}$ has inverse $-a-6 \in \mathbb{Q}$.
Let $a \in \mathbb{Q}$.
Since $\mathbb{Q}$ is closed under subtraction, then $-a-6 \in \mathbb{Q}$.
Observe that

$$\begin{aligned}a*(-a-6) &= a+(-a-6)+3 \\ &= [(a+(-a)]-6+3 \\ &= 0-6+3 \\ &= -3 \\ &= -6+3 \\ &= (0-6)+3 \\ &= [(-a+a)-6]+3 \\ &= [(-a-6)+a]+3 \\ &= (-a-6)*a.\end{aligned}$$

Since $-a-6 \in \mathbb{Q}$ and $a*(-a-6) = -3 = (-a-6)*a$, then every $a \in \mathbb{Q}$ has an inverse $-a-6 \in \mathbb{Q}$.

Since $*$ is a binary operation on $\mathbb{Q}$ and $*$ is associative and $-3 \in \mathbb{Q}$ is an identity for $*$ and every $a \in \mathbb{Q}$ has an inverse $-a-6 \in \mathbb{Q}$, then $(\mathbb{Q}, *)$ is a group.

We prove $*$ is commutative.
Let $a, b \in \mathbb{Q}$.
Then $a*b = a+b+3 = b+a+3 = b*a$, so $*$ is commutative.

Since $(\mathbb{Q}, *)$ is a group and $*$ is commutative, then $(\mathbb{Q}, *)$ is an abelian group. □

Exercise 40. Let $S = \{r \in \mathbb{R}^* : r \neq 1\}$.

Let $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ where
$f_1 : S \to S$ is the function defined by $f_1(x) = x$ and
$f_2 : S \to S$ is the function defined by $f_2(x) = 1 - x$ and
$f_3 : S \to S$ is the function defined by $f_3(x) = \frac{1}{x}$ and
$f_4 : S \to S$ is the function defined by $f_4(x) = \frac{1}{1-x}$ and
$f_5 : S \to S$ is the function defined by $f_5(x) = \frac{x-1}{x}$ and
$f_6 : S \to S$ is the function defined by $f_6(x) = \frac{x}{x-1}$.
Then G is a group under function composition.

Solution. We compute the composition of every pair of functions of G to construct the Cayley multiplication table.

The Cayley table for G is shown below.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

The Cayley table shows that the composition of every pair of functions in G is a unique function in G, so function composition is a binary operation on G.

Function composition is associative.

The Cayley table shows that $f_1 \circ f = f = f \circ f_1$ for all $f \in G$, so f_1 is the identity function for $\circ$.

Since $f_1 \circ f_1 = f_1$, then f_1 is its own inverse.
Since $f_2 \circ f_2 = f_1$, then f_2 is its own inverse.
Since $f_3 \circ f_3 = f_1$, then f_3 is its own inverse.
Since $f_4 \circ f_5 = f_1 = f_5 \circ f_4$, then f_4 and f_5 are inverses of each other.
Since $f_6 \circ f_6 = f_1$, then f_6 is its own inverse.
Therefore, every function in G has an inverse in G.

Since function composition is a binary operation on G and function composition is associative and the identity function f_1 is an identity for function composition and every function in G has an inverse in G, then $(G, \circ)$ is a group.

Since $f_2 \circ f_3 = f_5 \neq f_4 = f_3 \circ f_2$, then function composition is not commutative.

Since $(G, \circ)$ is a group and $\circ$ is not commutative, then $(G, \circ)$ is a non-abelian group. □

Exercise 41. Define $a * b = |a|b$ for all $a, , b \in \mathbb{R}^*$.

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

Solution. There is no identity for $*$, so $\mathbb{R}^*$ is not a group. □

Proof. Suppose there exists $e \in \mathbb{R}^*$ such that e is an identity for $*$.

Then $a * e = e * a = a$ for all $a \in \mathbb{R}^*$.

Let $a \in \mathbb{R}^*$.

Then $a \in \mathbb{R}$ and $a \neq 0$, so either $a > 0$ or $a < 0$.

We consider these cases separately.

Case 1: Suppose $a > 0$.

Then $a = a * e = |a|e = ae$, so $a = ae$.

Since $a \neq 0$, then we divide by a to obtain $e = 1$.

Case 2: Suppose $a < 0$.

Then $a = a * e = |a|e = -ae$, so $a = -ae$.

Since $a \neq 0$, then we divide by a to obtain $e = -1$.

Therefore, an identity is either 1 or -1.

But, the identity in any group must be unique.

Since the identity of $\mathbb{R}^*$ is not unique, then $(\mathbb{R}^*, *)$ cannot be a group. □

Exercise 42. Let $(G, *)$ be a group.

Define $a \triangle b = b * a$ for all $a, b \in G$.

Then $(G, \triangle)$ is a group.

Proof. Let $a, b \in G$.

Since $(G, *)$ is a group, then by closure of G under $*$, $b * a \in G$, so $a \triangle b \in G$.

Therefore, G is closed under $\triangle$.

Since $*$ is a binary operation on G, then $b * a$ is unique, so $a \triangle b$ is unique.

Since G is closed under $\triangle$ and $a \triangle b$ is unique, then $\triangle$ is a binary operation on G.

We prove $\triangle$ is associative.

Let $a, b, c \in G$.

Then

$$\begin{aligned}
(a \triangle b) \triangle c &= (b * a) \triangle c \\
&= c * (b * a) \\
&= (c * b) * a \\
&= (b \triangle c) * a \\
&= a \triangle (b \triangle c).
\end{aligned}$$

Therefore, $(a \triangle b) \triangle c = a \triangle (b \triangle c)$, so $\triangle$ is associative.

Let $e \in G$ be identity for $*$.

Then $e * a = a * e = a$ for all $a \in G$.

Let $a \in G$.

Then

$$\begin{aligned} a \triangle e &= e * a \\ &= a \\ &= a * e \\ &= e \triangle a. \end{aligned}$$

Since $a \triangle e = a = e \triangle a$ and $e \in G$, then e is an identity for $\triangle$.

We prove every element of G has an inverse.

Let $a \in G$.

Since $(G*)$ is a group, then $a^{-1} \in G$ and $a * a^{-1} = e = a^{-1} * a$.

Observe that

$$\begin{aligned} a \triangle a^{-1} &= a^{-1} * a \\ &= e \\ &= a * a^{-1} \\ &= a^{-1} \triangle a. \end{aligned}$$

Since $a^{-1} \in G$ and $a \triangle a^{-1} = e = a^{-1} \triangle a$, then a^{-1} is an inverse of a for $\triangle$.

Therefore, every element of G has an inverse for $\triangle$.

Since $\triangle$ is a binary operation on G and $\triangle$ is associative and $e \in G$ is an identity for $\triangle$ and every element of G has an inverse for $\triangle$, then $(G, \triangle)$ is a group. □

Exercise 43. Define $*$ for all $a, b \in \mathbb{R}^*$ by

$$a * b = \begin{cases} ab & \text{if } a > 0 \\ \frac{a}{b} & \text{if } a < 0 \end{cases}$$

Then $(\mathbb{R}^*, *)$ is a group.

Proof. We prove $*$ is a binary operation on $\mathbb{R}^*$.

Let $a, b \in \mathbb{R}^*$.

Since $a \in \mathbb{R}^*$, then $a \in \mathbb{R}$ and $a \neq 0$.

Since $b \in \mathbb{R}^*$, then $b \in \mathbb{R}$ and $b \neq 0$.

Since $a \neq 0$, then either $a > 0$ or $a < 0$.

We consider these cases separately.

Case 1: Suppose $a > 0$.

Then $a * b = ab$.

Since $\mathbb{R}$ is closed under multiplication and $a, b \in \mathbb{R}$, then $ab \in \mathbb{R}$.

The product of two non-zero real numbers is non-zero.
Since $a, b \in \mathbb{R}$ and $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.
Since $ab \in \mathbb{R}$ and $ab \neq 0$, then $ab \in \mathbb{R}^*$.
Case 2: Suppose $a < 0$.
Then $a * b = \frac{a}{b}$.
Since $a, b \in \mathbb{R}$ and $b \neq 0$, then $\frac{a}{b} \in \mathbb{R}$.
Since $a \neq 0$, then $\frac{a}{b} \neq 0$.
Since $\frac{a}{b} \in \mathbb{R}$ and $\frac{a}{b} \neq 0$, then $\frac{a}{b} \in \mathbb{R}^*$, so $a * b \in \mathbb{R}^*$.

Hence, in all cases, $a * b \in \mathbb{R}^*$, so $\mathbb{R}^*$ is closed under $*$.
Therefore, $*$ is a binary operation on $\mathbb{R}^*$. □

Proof. We prove $*$ is associative.
Let $a, b, c \in \mathbb{R}^*$.
Then $a, b, c \in \mathbb{R}$ and $a \neq 0$ and $b \neq 0$ and $c \neq 0$.
Since $a \neq 0$, then either $a > 0$ or $a < 0$.
Since $b \neq 0$, then either $b > 0$ or $b < 0$.
Since $c \neq 0$, then either $c > 0$ or $c < 0$.
Hence, either
$a > 0$ and $b > 0$ and $c > 0$, or
$a > 0$ and $b > 0$ and $c < 0$, or
$a > 0$ and $b < 0$ and $c > 0$, or
$a > 0$ and $b < 0$ and $c < 0$, or
$a < 0$ and $b > 0$ and $c > 0$, or
$a < 0$ and $b > 0$ and $c < 0$, or
$a < 0$ and $b < 0$ and $c > 0$, or
$a < 0$ and $b < 0$ and $c < 0$.
We consider these $2^3 = 8$ cases separately.
Case 1: Suppose $a > 0$ and $b > 0$ and $c > 0$.
Since $a > 0$ and $b > 0$, then $ab > 0$.
Observe that

$$\begin{aligned} (a * b) * c &= ab * c \\ &= (ab)c \\ &= a(bc) \\ &= a * (bc) \\ &= a * (b * c). \end{aligned}$$

Therefore, $(a * b) * c = a * (b * c)$.
Case 2: Suppose $a > 0$ and $b > 0$ and $c < 0$.
Since $a > 0$ and $b > 0$, then $ab > 0$.

Observe that

$$\begin{aligned}(a*b)*c &= ab*c \\ &= (ab)c \\ &= a(bc) \\ &= a*(bc) \\ &= a*(b*c).\end{aligned}$$

Therefore, $(a*b)*c = a*(b*c)$.
Case 3: Suppose $a > 0$ and $b < 0$ and $c > 0$.
Since $a > 0$ and $b < 0$, then $ab < 0$.
Observe that

$$\begin{aligned}(a*b)*c &= ab*c \\ &= \frac{ab}{c} \\ &= a(\frac{b}{c}) \\ &= a(b*c) \\ &= a*(b*c).\end{aligned}$$

Therefore, $(a*b)*c = a*(b*c)$.
Case 4: Suppose $a > 0$ and $b < 0$ and $c < 0$.
Since $a > 0$ and $b < 0$, then $ab < 0$.
Observe that

$$\begin{aligned}(a*b)*c &= ab*c \\ &= \frac{ab}{c} \\ &= a(\frac{b}{c}) \\ &= a(b*c) \\ &= a*(b*c).\end{aligned}$$

Therefore, $(a*b)*c = a*(b*c)$.
Case 5: Suppose $a < 0$ and $b > 0$ and $c > 0$.
Since $a < 0$ and $b > 0$, then $\frac{a}{b} < 0$.
Observe that

$$\begin{aligned}(a*b)*c &= (\frac{a}{b})*c \\ &= \frac{a}{b}/c \\ &= \frac{a}{bc} \\ &= a*(bc) \\ &= a*(b*c).\end{aligned}$$

Therefore, $(a*b)*c = a*(b*c)$.
Case 6: Suppose $a < 0$ and $b > 0$ and $c < 0$.
Since $a < 0$ and $b > 0$, then $\frac{a}{b} < 0$.
Observe that

$$\begin{aligned}(a*b)*c &= (\frac{a}{b})*c \\ &= \frac{a}{b}/c \\ &= \frac{a}{bc} \\ &= a*(bc) \\ &= a*(b*c).\end{aligned}$$

Therefore, $(a*b)*c = a*(b*c)$.
Case 7: Suppose $a < 0$ and $b < 0$ and $c > 0$.
Since $a < 0$ and $b < 0$, then $\frac{a}{b} > 0$.
Observe that

$$\begin{aligned}(a*b)*c &= (\frac{a}{b})*c \\ &= (\frac{a}{b})c \\ &= \frac{ac}{b} \\ &= a/\frac{b}{c} \\ &= a/(b*c) \\ &= a*(b*c).\end{aligned}$$

Therefore, $(a*b)*c = a*(b*c)$.
Case 8: Suppose $a < 0$ and $b < 0$ and $c < 0$.
Since $a < 0$ and $b < 0$, then $\frac{a}{b} > 0$.
Observe that

$$\begin{aligned}(a*b)*c &= (\frac{a}{b})*c \\ &= (\frac{a}{b})c \\ &= \frac{ac}{b} \\ &= a/\frac{b}{c} \\ &= a/(b*c) \\ &= a*(b*c).\end{aligned}$$

Therefore, $(a*b)*c = a*(b*c)$.

In all cases, $(a * b) * c = a * (b * c)$, so $*$ is associative. □

Proof. We prove $1 \in \mathbb{R}^*$ is identity for $*$.
Since $1 \in \mathbb{R}$ and $1 \neq 0$, then $1 \in \mathbb{R}^*$.
Let $a \in \mathbb{R}^*$.
Then $a \in \mathbb{R}$ and $a \neq 0$, so either $a > 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$.
Then $a * 1 = a(1) = a = 1(a) = 1 * a$.
Case 2: Suppose $a < 0$.
Then $a * 1 = \frac{a}{1} = a = 1(a) = 1 * a$.

In all cases, $a * 1 = a = 1 * a$.
Since $1 \in \mathbb{R}^*$ and $a * 1 = a = 1 * a$, then $1 \in \mathbb{R}^*$ is an identity for $*$. □

Proof. We prove every $a \in \mathbb{R}^*$ has an inverse.
Let $a \in \mathbb{R}^*$.
Then $a \in \mathbb{R}$ and $a \neq 0$, so either $a > 0$ or $a < 0$.
We consider these cases separately.
Case 1: Suppose $a > 0$.
Let $a^{-1} = \frac{1}{a}$.
Since $a \neq 0$, then $\frac{1}{a} \in \mathbb{R}$.
Since $1 > 0$ and $a > 0$, then $\frac{1}{a} > 0$, so $\frac{1}{a} \neq 0$.
Since $\frac{1}{a} \in \mathbb{R}$ and $\frac{1}{a} \neq 0$, then $\frac{1}{a} \in \mathbb{R}^*$.
Observe that

$$\begin{aligned} a * \frac{1}{a} &= a(\frac{1}{a}) \\ &= 1 \\ &= \frac{1}{a}(a) \\ &= \frac{1}{a} * a. \end{aligned}$$

Since $\frac{1}{a} \in \mathbb{R}^*$ and $a * \frac{1}{a} = 1 = \frac{1}{a} * a$, then $\frac{1}{a} \in \mathbb{R}^*$ is an inverse of a.
Case 2: Suppose $a < 0$.
Observe that

$$\begin{aligned} a * a &= \frac{a}{a} \\ &= 1. \end{aligned}$$

Since $a \in \mathbb{R}^*$ and $a * a = 1$, then a is an inverse of a.

Therefore, if $a > 0$, then $\frac{1}{a} \in \mathbb{R}^*$ is an inverse and if $a < 0$, then $a \in \mathbb{R}^*$ is its own inverse.
Hence, every $a \in \mathbb{R}^*$ has an inverse in $\mathbb{R}^*$. □

Proof. Since $*$ is a binary operation on $\mathbb{R}^*$ and $*$ is associative and $1 \in \mathbb{R}^*$ is an identity for $*$ and every $a \in \mathbb{R}^*$ has an inverse, then $(\mathbb{R}^*, *)$ is a group.

Since $2 * (-3) = 2(-3) = -6 \neq -\frac{3}{2} = (-3) * 2$, then $*$ is not commutative.

Since $(\mathbb{R}^*, *)$ is a group and $*$ is not commutative, then $(\mathbb{R}^*, *)$ is a non-abelian group. □

Exercise 44. Let G be a group and $a, b, c \in G$.

If $ab = ac$, then $b = c$.

Proof. Suppose $ab = ac$.

Then

$$\begin{aligned} b &= eb \\ &= (a^{-1}a)b \\ &= a^{-1}(ab) \\ &= a^{-1}(ac) \\ &= (a^{-1}a)c \\ &= ec \\ &= c. \end{aligned}$$

Therefore, $b = c$. □

Exercise 45. Each element of a finite group appears exactly once in each row and exactly once in each column of the group's operation table.

Proof. Let G be a finite group.

Let $a \in G$ such that $a = rc$ for some $r \in G$ and $c \in G$.

Then a appears at least once in the row with row header r and a appears at least once in the column with column header c.

Suppose a appears more than once in the row with row header r.

Then there exists $b \neq c$ such that $rb = a$.

Thus, $rb = a = rc$, so $rb = rc$.

By the left cancellation law for groups, we obtain $b = c$.

But, this contradicts that $b \neq c$.

Therefore, a cannot appear more than once in the row with row header r.

Since a appears at least once in the row with row header r and a cannot appear more than once in the row with row header r, then a appears exactly once in the row with row header r.

Suppose a appears more than once in the column with column header c.

Then there exists $d \neq r$ such that $dc = a$.

Thus, $dc = a = rc$, so $dc = rc$.

By the right cancellation law for groups, we obtain $d = r$.

But, this contradicts that $d \neq r$.

Therefore, a cannot appear more than once in the column with column header c.

Since a appears at least once in the column with column header c and a cannot appear more than once in the column with column header c, then a appears exactly once in the column with column header c.

Since a appears exactly once in the row with row header r and r is arbitrary, then a appears exactly once in any row of the operation table of G.

Since a appears exactly once in the column with column header c and c is arbitrary, then a appears exactly once in any column of the operation table of G.

Since a is an arbitrary element of G, then this implies any element of G appears exactly once in any row of the operation table of G and any element of G appears exactly once in any column of the operation table of G. □

Exercise 46. Let T be an infinite set.

Let $(S_T, \circ)$ be the symmetric group on T under function composition.

Let $G = \{f \in S_T : f(t) \neq t \text{ for only a finite number of } t \in T\}$.

Then $(G, \circ)$ is a group.

Proof. We prove $\circ$ is a binary operation on G.

Let $f, g \in G$.

Since $f \in G$, then $f \in S_T$ and $f(t) \neq t$ for only a finite number of $t \in T$.

Since $g \in G$, then $g \in S_T$ and $g(t) \neq t$ for only a finite number of $t \in T$.

Since $f \in S_T$, then $f : T \to T$ is a permutation, so f is a bijection.

Since $g \in S_T$, then $g : T \to T$ is a permutation, so g is a bijection.

Let $f \circ g : T \to T$ be defined by $(f \circ g)(t) = f(g(t))$ for all $t \in T$.

Since composition of bijections is a bijection and f is a bijection and g is a bijection, then $f \circ g$ is a bijection, so $f \circ g : T \to T$ is a permutation.

Hence, $f \circ g \in S_T$.

Since $f(t) \neq t$ for only a finite number of $t \in T$, then there exists $m \in \mathbb{Z}$ with $m \geq 0$ such that $f(x_1) \neq x_1$ and $f(x_2) \neq x_2$ and ... and $f(x_m) \neq x_m$ for some $x_1, x_2, ..., x_m \in T$.

Since $g(t) \neq t$ for only a finite number of $t \in T$, then there exists $n \in \mathbb{Z}$ with $n \geq 0$ such that $f(y_1) \neq y_1$ and $f(y_2) \neq y_2$ and ... and $f(y_n) \neq y_n$ for some $y_1, y_2, ..., y_n \in T$.

Let $f(x_1) = s_1$ and $f(x_2) = s_2$ and ... and $f(x_m) = s_m$.

Then $x_1 \neq s_1$ and $x_2 \neq s_2$ and ... and $x_m \neq s_m$ for $s_1, s_2, ..., s_m \in T$.

Let $g(y_1) = t_1$ and $f(y_2) = t_2$ and ... and $f(y_n) = t_n$.

Then $y_1 \neq t_1$ and $y_2 \neq t_2$ and ... and $y_n \neq t_n$ for $t_1, t_2, ..., t_n \in T$.

TODO We're stuck.

□

Exercise 47. Real linear functions under function composition is a group.

Let $T_{a,b} : \mathbb{R} \to \mathbb{R}$ be the function defined by $T_{a,b}(x) = ax + b$ for $a, b \in \mathbb{R}$ and $a \neq 0$.

Then $G = \{T_{a,b} : a, b \in \mathbb{R} \text{ and } a \neq 0\ \}$ is a non-abelian group under function composition.

Proof. We prove $\circ$ is a binary operation on G.

Let $S_{a,b}$ and $T_{c,d}$ be elements of G.

Since $S_{a,b} \in G$, then $S_{a,b} : \mathbb{R} \to \mathbb{R}$ is the function defined by $S_{a,b}(x) = ax + b$ for $a, b \in \mathbb{R}$ and $a \neq 0$.

Since $T_{c,d} \in G$, then $T_{c,d} : \mathbb{R} \to \mathbb{R}$ is the function defined by $T_{c,d}(x) = cx + d$ for $c, d \in \mathbb{R}$ and $c \neq 0$.

Let $S \circ T : \mathbb{R} \to \mathbb{R}$ be the function defined by $(S \circ T)(x) = S(T(x))$ for all $x \in \mathbb{R}$.

Let $x \in \mathbb{R}$.

Then $(S \circ T)(x) = S(T(x)) = S(cx + d) = a(cx + d) + b = acx + ad + b = (ac)x + (ad + b)$.

Thus, $(S \circ T) = (S \circ T)_{ac,ad+b}$.

Since $a, c \in \mathbb{R}$ and $\mathbb{R}$ is closed under multiplication, then $ac \in \mathbb{R}$.

Since $\mathbb{R}$ is closed under multiplication and addition and $a, b, d \in \mathbb{R}$, then $ad + b \in \mathbb{R}$.

Since $a \neq 0$ and $c \neq 0$, then $ac \neq 0$.

Since $ac \in \mathbb{R}$ and $ad + b \in \mathbb{R}$ and $ac \neq 0$, then $(S \circ T)_{ac,ad+b} \in G$, so $(S \circ T) \in G$.

Therefore, G is closed under $\circ$, so $\circ$ is a binary operation on G. □

Proof. Function composition is associative, so $\circ$ is associative in G. □

Proof. We prove the identity function I is identity for G.

Let $I : \mathbb{R} \to \mathbb{R}$ be the function defined by $I(x) = x$ for all $x \in \mathbb{R}$.

Then $I(x) = x = 1x + 0$, so $I = I_{1,0}$.

Since $1, 0 \in \mathbb{R}$ and $1 \neq 0$, then $I_{1,0} \in G$, so $I \in G$.

Let $T_{a,b} \in G$.

Then $T_{a,b} : \mathbb{R} \to \mathbb{R}$ is the function defined by $T_{a,b}(x) = ax + b$ for $a, b \in \mathbb{R}$ and $a \neq 0$.

Let $x \in \mathbb{R}$.

Observe that

$$\begin{aligned}
(T \circ I)(x) &= T(I(x)) \\
&= T(x) \\
&= ax + b \\
&= I(ax + b) \\
&= I(T(x)) \\
&= (I \circ T)(x).
\end{aligned}$$

Thus, $(T \circ I)(x) = T(x) = (I \circ T)(x)$, so $T \circ I = T = I \circ T$.

Since $I \in G$ and $T \circ I = T = I \circ T$, then I is an identity of G. □

Proof. We prove every element of G has an inverse.

Let $T_{a,b} \in G$.

Then $T_{a,b} : \mathbb{R} \to \mathbb{R}$ is the function defined by $T_{a,b}(x) = ax + b$ for $a, b \in \mathbb{R}$ and $a \neq 0$.

Since $a \in \mathbb{R}$ and $a \neq 0$, then $\frac{1}{a} \in \mathbb{R}$ and $\frac{1}{a} \neq 0$.

Since $a, b \in \mathbb{R}$ and $a \neq 0$, then $\frac{-b}{a} \in \mathbb{R}$.

Let $T^{-1} : \mathbb{R} \to \mathbb{R}$ be the function defined by $T^{-1}(x) = (\frac{1}{a})x - \frac{b}{a}$ for all $x \in \mathbb{R}$.

Since $\frac{1}{a} \in \mathbb{R}$ and $\frac{-b}{a} \in \mathbb{R}$ and $\frac{1}{a} \neq 0$, then $T^{-1} \in G$.

Let $x \in \mathbb{R}$.

Observe that

$$\begin{aligned}
(T \circ T^{-1})(x) &= T(T^{-1}(x)) \\
&= T((\frac{1}{a})x - \frac{b}{a}) \\
&= a((\frac{1}{a})x - \frac{b}{a}) + b \\
&= x - b + b \\
&= x \\
&= I(x) \\
&= x \\
&= x + \frac{b}{a} - \frac{b}{a} \\
&= \frac{1}{a}(ax + b) - \frac{b}{a} \\
&= \frac{1}{a}(T(x)) - \frac{b}{a} \\
&= T^{-1}(T(x)) \\
&= I(T(x)) \\
&= (T^{-1} \circ T)(x).
\end{aligned}$$

Thus, $(T \circ T^{-1})(x) = I(x) = (T^{-1} \circ T)(x)$, so $T \circ T^{-1} = I = T^{-1} \circ T$.

Since $T^{-1} \in G$ and $T \circ T^{-1} = I = T^{-1} \circ T$, then T^{-1} is an inverse of T.

Therefore, for every $T_{a,b} \in G$ defined by $T(x) = ax + b$, there exists $T^{-1} \in G$ defined by $T^{-1}(x) = (\frac{1}{a})x - \frac{b}{a}$ such that T^{-1} is an inverse of T. □

Proof. Since $\circ$ is a binary operation on G and $\circ$ is associative and the identity function $I : \mathbb{R} \to \mathbb{R}$ defined by $I(x) = x$ for all $x \in \mathbb{R}$ is an identity of G and for every $T_{a,b} \in G$ defined by $T_{a,b}(x) = ax + b$, there exists $T^{-1} \in G$ defined by $T^{-1}(x) = (\frac{1}{a})x - \frac{b}{a}$ such that T^{-1} is an inverse of T, then G is a group. □

Proof. We prove $\circ$ is not commutative.

Let $f_{2,3} \in G$ and let $g_{4,-5} \in G$.

Then $f : \mathbb{R} \to \mathbb{R}$ is the function defined by $f(x) = 2x + 3$ and $g : \mathbb{R} \to \mathbb{R}$ is the function defined by $g(x) = 4x - 5$.

Let $x \in \mathbb{R}$.

Observe that

$$\begin{aligned}(f \circ g)(x) &= f(g(x))\\ &= f(4x-5)\\ &= 2(4x-5)+3\\ &= 8x-10+3\\ &= 8x-7.\end{aligned}$$

and

$$\begin{aligned}(g \circ f)(x) &= g(f(x))\\ &= g(2x+3)\\ &= 4(2x+3)-5\\ &= 8x+12-5\\ &= 8x+7.\end{aligned}$$

Since $8x-7 \neq 8x+7$ for all $x \in \mathbb{R}$, then $(f \circ g)(x) \neq (g \circ f)(x)$, so $f \circ g \neq g \circ f$.
Hence, $\circ$ is not commutative.
Since G is a group and $\circ$ is not commutative, then G is a non-abelian group. □

Exercise 48. Let $T_{a,b} : \mathbb{R} \to \mathbb{R}$ be the function defined by $T_{a,b}(x) = ax + b$ for $a, b \in \mathbb{R}$ and $a \neq 0$.
Let $H = \{T_{1,b} : b \in \mathbb{R}\}$.
Then H is an abelian group under function composition.

Proof. We prove function composition $\circ$ is a binary operation on H.
Let $S_{1,a}$ and $T_{1,b}$ be arbitrary elements of H.
Since $S_{1,a} \in H$, then $S : \mathbb{R} \to \mathbb{R}$ is the function defined by $S(x) = x + a$ for $a \in \mathbb{R}$.
Since $T_{1,B} \in H$, then $T : \mathbb{R} \to \mathbb{R}$ is the function defined by $T(x) = x + b$ for $b \in \mathbb{R}$.
Let $S \circ T : \mathbb{R} \to \mathbb{R}$ be the function defined by $(S \circ T)(x) = S(T(x))$ for all $x \in \mathbb{R}$.
Let $x \in \mathbb{R}$.
Then $(S \circ T)(x) = S(T(x)) = S(x+b) = (x+b)+a = x+(b+a) = x+(a+b)$.
Thus, $(S \circ T) = (S \circ T)_{1,a+b}$.
Since $a, b \in \mathbb{R}$ and $\mathbb{R}$ is closed under addition, then $a + b \in \mathbb{R}$.
Since $a + b \in \mathbb{R}$, then $(S \circ T)_{1,a+b} \in H$, so $(S \circ T) \in H$.
Therefore, H is closed under $\circ$, so $\circ$ is a binary operation on H. □

Proof. Function composition is associative, so $\circ$ is associative in H. □

Proof. We prove the identity function I is identity for H.
Let $I : \mathbb{R} \to \mathbb{R}$ be the function defined by $I(x) = x$ for all $x \in \mathbb{R}$.
Then $I(x) = x = 1x + 0$, so $I = I_{1,0}$.
Since $0 \in \mathbb{R}$, then $I_{1,0} \in H$, so $I \in H$.

Let $T_{1,a} \in H$.

Then $T_{1,a} : \mathbb{R} \to \mathbb{R}$ is the function defined by $T(x) = x + a$ for $a \in \mathbb{R}$.

Let $x \in \mathbb{R}$.

Observe that

$$\begin{aligned} (T \circ I)(x) &= T(I(x)) \\ &= T(x) \\ &= x + a \\ &= I(x + a) \\ &= I(T(x)) \\ &= (I \circ T)(x). \end{aligned}$$

Thus, $(T \circ I)(x) = T(x) = (I \circ T)(x)$, so $T \circ I = T = I \circ T$.

Since $I \in H$ and $T \circ I = T = I \circ T$, then I is an identity of H. □

Proof. We prove every element of H has an inverse.

Let $T_{1,a} \in H$.

Then $T_{1,a} : \mathbb{R} \to \mathbb{R}$ is the function defined by $T(x) = x + a$ for $a \in \mathbb{R}$.

Let $T_{1,-a} : \mathbb{R} \to \mathbb{R}$ be the function defined by $T_{1,-a}(x) = x - a$ for all $x \in \mathbb{R}$.

Since $-a \in \mathbb{R}$, then $T_{1,-a} \in H$.

Let $x \in \mathbb{R}$.

Observe that

$$\begin{aligned} (T \circ T_{1,-a})(x) &= T(T_{1,-a}(x)) \\ &= T(x - a) \\ &= (x - a) + a \\ &= x \\ &= I(x) \\ &= x \\ &= (x + a) - a \\ &= T(x) - a \\ &= T_{1,-a}(T(x)) \\ &= (T_{1,-a} \circ T)(x). \end{aligned}$$

Thus, $(T \circ T_{1,-a})(x) = I(x) = (T_{1,-a} \circ T)(x)$, so $T \circ T_{1,-a} = I = T_{1,-a} \circ T$.

Since $T_{1,-a} \in H$ and $T \circ T_{1,-a} = I = T_{1,-a} \circ T$, then $T_{1,-a}$ is an inverse of T.

Therefore, for every $T_{1,a} \in H$ defined by $T(x) = x+a$, there exists $T_{1,-a} \in H$ defined by $T_{1,-a}(x) = x - a$ such that $T_{1,-a}$ is an inverse of T. □

Proof. Since $\circ$ is a binary operation on H and $\circ$ is associative and the identity function $I : \mathbb{R} \to \mathbb{R}$ defined by $I(x) = x$ for all $x \in \mathbb{R}$ is an identity of H and for every $T_{1,a} \in H$ defined by $T(x) = x + a$, there exists $T_{1,-a} \in H$ defined by $T_{1,-a}(x) = x - a$ such that $T_{1,-a}$ is an inverse of T, then H is a group. □

Proof. We prove H is abelian.

Let $S_{1,a}$ and $T_{1,b}$ be arbitrary elements of H.

Then $S : \mathbb{R} \to \mathbb{R}$ is the function defined by $S(x) = x - a$ and $T : \mathbb{R} \to \mathbb{R}$ is the function defined by $T(x) = x + b$ for $a, b \in \mathbb{R}$.

Let $x \in \mathbb{R}$.

Observe that

$$\begin{array}{rcl} (S \circ T)(x) & = & S(T(x)) \\ & = & S(x + b) \\ & = & (x + b) - a \\ & = & x + b - a \\ & = & x - a + b \\ & = & (x - a) + b \\ & = & T(x - a) \\ & = & T(S(x)) \\ & = & (T \circ S)(x). \end{array}$$

Thus, $(S \circ T)(x) = (T \circ S)(x)$, so $S \circ T = T \circ S$.

Therefore, $\circ$ is commutative.

Since H is a group and $\circ$ is commutative, then H is an abelian group. □

Exercise 49. Let $f \in S_n$.

Let I be the identity permutation of the symmetric group S_n.

Then there exists $k \in \mathbb{Z}^+$ such that $f^k = I$, where $f^k = f \circ f \circ f ... \circ f$ (composition of f with itself k times).

Proof. TODO

Let $X = \{1, 2, ..., n\}$.

Observations.

Let $n =$ the number of elements of set X.

Let x represent the number of elements of X that are in the desired position for the identity permutation.

This means 1 is in the first slot, 2 is in the second slot, 3 is in the third slot, ... and n is in the last slot.

Let m represent the number of moves an element requires to move to the desired slot in the identity permutation.

Then m is 0 if $x = n$ and $m = n - x$ otherwise.

Let k be power of f, so that $k = m + 1$.

Each move corresponds to an element $a \in X$ that moves to a different slot, if the elements are arranged in linear order. □

Exercise 50. Let $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Let $(G, *)$ be a group with the following properties.

1. $a * b \leq a + b$ for all $a, b \in G$.

2. $a * a = 0$ for all $a \in G$.

Compute the operation table for G.

Solution. We must ensure each row and each column contains an element exactly once and satisfies the properties above.

We find that $0 \in G$ is the identity.

The operation table for G is shown below.

$\cdot$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	4	5	6	7	2
2	2	3	0	5	6	7	4	1
3	3	4	5	0	7	1	2	6
4	4	5	6	7	0	2	1	3
5	5	6	7	1	2	0	3	4
6	6	7	4	2	1	3	0	5
7	7	2	1	6	3	4	5	0

□

Exercise 51. Let $(G, *)$ be a group with identity $e \in G$.

Let $a \in G$.

If $a^2 = a$, then $a = e$.

Proof. Suppose $a^2 = a$.

Then

$$\begin{aligned} aa &= a^2 \\ &= a \\ &= ae. \end{aligned}$$

Hence, $aa = ae$.

By the left cancellation law, we obtain $a = e$. □

Exercise 52. Let G be a group.

Let $a, b, c, d \in G$.

Compute $(abcd)^{-1}$.

Solution. We show the inverse of $abcd$ is $d^{-1}c^{-1}b^{-1}a^{-1}$.

Let $e \in G$ be the identity of G.

Observe that

$$\begin{aligned}(abcd)(d^{-1}c^{-1}b^{-1}a^{-1}) &= (abc)(dd^{-1})(c^{-1}b^{-1}a^{-1})\\ &= (abc)(e)(c^{-1}b^{-1}a^{-1})\\ &= (abc)(c^{-1}b^{-1}a^{-1})\\ &= (ab)(cc^{-1})(b^{-1}a^{-1})\\ &= (ab)(e)(b^{-1}a^{-1})\\ &= (ab)(b^{-1}a^{-1})\\ &= a(bb^{-1})a^{-1}\\ &= a(e)a^{-1}\\ &= aa^{-1}\\ &= e.\end{aligned}$$

Observe that

$$\begin{aligned}(d^{-1}c^{-1}b^{-1}a^{-1})(abcd) &= (d^{-1}c^{-1}b^{-1})(a^{-1}a)(bcd)\\ &= (d^{-1}c^{-1}b^{-1})(e)(bcd)\\ &= (d^{-1}c^{-1}b^{-1})(bcd)\\ &= (d^{-1}c^{-1})(b^{-1}b)(cd)\\ &= (d^{-1}c^{-1})(e)(cd)\\ &= (d^{-1}c^{-1})(cd)\\ &= d^{-1}(c^{-1}c)d\\ &= d^{-1}(e)d\\ &= d^{-1}d\\ &= e.\end{aligned}$$

Since $(abcd)(d^{-1}c^{-1}b^{-1}a^{-1}) = e = (d^{-1}c^{-1}b^{-1}a^{-1})(abcd)$, then $d^{-1}c^{-1}b^{-1}a^{-1}$ is the inverse of $abcd$.

Therefore, $(abcd)^{-1} = d^{-1}c^{-1}b^{-1}a^{-1}$. □

Exercise 53. Let G be a group with identity $e \in G$.

Let $a, b \in G$.

If $ab = e$, then $ba = e$.

Proof. Observe that

$$\begin{aligned}ba &= (eb)a\\ &= e(ba)\\ &= (a^{-1}a)(ba)\\ &= a^{-1}(ab)a\\ &= a^{-1}(e)a\\ &= a^{-1}a\\ &= e.\end{aligned}$$

Therefore, $ba = e$. □

Exercise 54. Let G be a group.
Let $f : G \to G$ be a function defined by $f(a) = a^{-1}$ for all $a \in G$.
Then f is bijective.

Proof. We prove f is injective.
Let $a, b \in G$ such that $f(a) = f(b)$.
Then $a^{-1} = f(a) = f(b) = b^{-1}$, so $a^{-1} = b^{-1}$.
Hence, $a = (a^{-1})^{-1} = (b^{-1})^{-1} = b$, so $a = b$.
Therefore, $f(a) = f(b)$ implies $a = b$, so f is injective.

We prove f is surjective.
Let $b \in G$.
Since G is a group and $b \in G$, then $b^{-1} \in G$.
Observe that $f(b^{-1}) = (b^{-1})^{-1} = b$.
Since $b^{-1} \in G$ and $f(b^{-1}) = b$, then f is surjective.

Since f is injective and surjective, then f is bijective. □

Exercise 55. Let $S = \mathbb{R} - \{-1\}$.
Define $*$ on S by $a * b = a + b + ab$ for all $a, b \in S$.
Then $(S, *)$ is an abelian group.

Proof. We first prove $*$ is a binary operation on S.
Let $a, b \in S$.
Then $a, b \in \mathbb{R}$ and $a \neq -1$ and $b \neq -1$ and $a * b = a + b + ab$.
Since $a, b \in \mathbb{R}$ and $a * b = a + b + ab$, then by closure of $\mathbb{R}$ under addition and multiplication, $a * b \in \mathbb{R}$.

We prove S is closed under $*$.
Suppose for the sake of contradiction S is not closed under $*$.
Then there exist $x, y \in S$ such that $x * y \notin S$.
Since $x, y \in S$, then $x, y \in \mathbb{R}$ and $x \neq -1$ and $y \neq -1$.
Since $x * y \notin S$, then either $x * y \notin \mathbb{R}$ or $x * y = -1$.
Since $x, y \in \mathbb{R}$, then we know $x * y \in \mathbb{R}$.
Hence, we conclude $x * y = -1$.
Thus, $x + y + xy = -1$, so $0 = x + y + xy + 1 = x + xy + y + 1 = x(1 + y) + (y + 1) = x(y + 1) + (y + 1) = (x + 1)(y + 1)$.
This implies either $x + 1 = 0$ or $y + 1 = 0$, so either $x = -1$ or $y = -1$.
But, neither x nor y is negative one, since $x \neq -1$ and $y \neq -1$.
Therefore, S is closed under $*$.

We next prove $*$ is well defined.

Let $(a,b),(c,d) \in S \times S$ such that $(a,b) = (c,d)$.

Since $(a,b) = (c,d)$, then by definition of equality of ordered pairs, $a = c$ and $b = d$.

Thus, by substitution, we have $a * b = a + b + ab = c + d + cd = c * d$.

Therefore, $*$ is well defined.

Since S is closed under $*$ and $*$ is well defined, then $*$ is a binary operation on S, so $(S,*)$ is a binary structure. □

Proof. We prove $*$ is associative.

Let $a, b, c \in S$.

Observe that

$$\begin{aligned}
(a*b)*c &= (a+b+ab)*c \\
&= (a+b+ab)+c+(a+b+ab)c \\
&= a+b+ab+c+ac+bc+abc \\
&= a+b+c+bc+ab+ac+abc \\
&= a+(b+c+bc)+a(b+c+bc) \\
&= a*(b+c+bc) \\
&= a*(b*c).
\end{aligned}$$

Therefore, $*$ is associative.

We prove $*$ is commutative.

Let $a, b \in S$.

Observe that

$$\begin{aligned}
a*b &= a+b+ab \\
&= b+a+ab \\
&= b+a+ba \\
&= b*a.
\end{aligned}$$

Therefore, $*$ is commutative.

We next prove 0 is an identity for $*$.

Let $a \in S$.

Then $a \in \mathbb{R}$.

Since $0 \in \mathbb{R}$ and $0 \neq -1$, then $0 \in S$.

Since $a*0 = 0*a = 0+a+0a = a+0a = a+0 = a$, then $a*0 = 0*a = a$, so 0 is an identity for $*$. □

Proof. We next prove the inverse of a is $\frac{-a}{a+1}$.

Let $a \in S$.

Let $b = \frac{-a}{a+1}$.

We prove b is an inverse of a.

Since $a \in S$, then $a \in \mathbb{R}$ and $a \neq -1$.
Since $a \neq -1$, then $a + 1 \neq 0$.
Since $a \in \mathbb{R}$, then $-a \in \mathbb{R}$, so $b \in \mathbb{R}$.

Suppose that $b = -1$.
Then $-1 = b = \frac{-a}{a+1}$, so $1 = \frac{a}{a+1}$.
Since $a + 1 \neq 0$, then we multiply both sides by $a + 1$ to obtain $a + 1 = a$.
We subtract a from both sides to obtain $1 = 0$, a contradiction.
Therefore, $b \neq -1$.
Since $b \in \mathbb{R}$ and $b \neq -1$, then $b \in S$.

Observe that

$$\begin{aligned}
a * b &= b * a \\
&= b + a + ba \\
&= \frac{-a}{a+1} + a + (\frac{-a}{a+1})a \\
&= \frac{-a}{a+1} + \frac{a(a+1)}{a+1} - \frac{a^2}{a+1} \\
&= \frac{-a + a(a+1) - a^2}{a+1} \\
&= \frac{-a + a^2 + a - a^2}{a+1} \\
&= 0.
\end{aligned}$$

Since $b \in S$ and $a * b = b * a = 0$, then b is an inverse of a, so a has an inverse.
Since a is arbitrary, then every element of S has an inverse.

Since $(S, *)$ is an associative binary structure with identity 0 and each element of S has an inverse, then $(S, *)$ is a group.
Since $*$ is commutative, then $(S, *)$ is an abelian group. □

Exercise 56. Let $(\mathbb{Z}_n^*, \cdot)$ be the group of units of $\mathbb{Z}_n$, where $\cdot$ is multiplication modulo n.
If $n > 2$, then there is an element $[a] \in \mathbb{Z}_n^*$ such that $[a]^2 = [1]$ and $[a] \neq [1]$.

Solution. Let $n \in \mathbb{Z}^+$.
The statement to prove is P : if $n \geq 3$, then $(\exists [a] \in \mathbb{Z}_n^*)([a]^2 = [1] \wedge [a] \neq [a])$.
We try different values of n, like $n = 1, 2, 3, 4, 5, 6, ...$
We find that when $n < 3$, then $[1]^2 = [1]$, but $[1] = [1]$.
Now, when $n \geq 3$, we find that $[n-1]^2 = [1]$. □

Proof. Let n be a positive integer.
Suppose $n > 2$.
Since $n \in \mathbb{Z}$, then $n - 1 \in \mathbb{Z}$, so $[n-1] \in \mathbb{Z}_n$.

Since $n|n$, then $n|(n-1+1)$, so $n|(n-1)-(-1)$.
Hence, $n-1 \equiv -1 \pmod{n}$, so $[n-1] = [-1]$.
Observe that $[n-1]^2 = [n-1][n-1] = [-1][-1] = [(-1)(-1)] = [1]$.
Since $[n-1] \in \mathbb{Z}_n$ and $[n-1][n-1] = [1]$, then $[n-1] \in \mathbb{Z}_n^*$.

Since $n > 2$, then $n-2 > 0$.
Since $n > 2$ and $n-2 > 0$, then $n > 0$ and $n-2 > 0$.
Hence, n and $n-2$ are positive integers and $n > n-2$.
Since $n|n-2$ implies $n \leq n-2$, then $n > n-2$ implies $n \not| n-2$.
Thus, since $n > n-2$, then we conclude $n \not| n-2$.
Therefore, $n \not|(n-1)-1$, so $n-1 \not\equiv 1 \pmod{n}$.
Thus, $[n-1] \neq [1]$.
Let $a = n-1$.
Then $[a] = [n-1]$.
Since $[n-1] \in \mathbb{Z}_n^*$ and $[n-1]^2 = [1]$ and $[n-1] \neq [1]$, then there exists $[a] \in \mathbb{Z}_n^*$ such that $[a]^2 = [1]$ and $[a] \neq [1]$. □

Exercise 57. Let $(\mathbb{Z}_n^*, \cdot)$ be the group of units of $\mathbb{Z}_n$ where $\cdot$ is multiplication modulo n.
For $n > 2$, there exists $k \in \mathbb{Z}_n^*$ such that $k^2 = 1$ and $k \neq 1$.

Solution. Let $n \in \mathbb{Z}^+$ such that $n > 2$.
Let $k = n-1$.
Since $\gcd(k,n) = \gcd(n-1,n) = 1$, then k has a multiplicative inverse in $\mathbb{Z}_n$, so $k \in \mathbb{Z}_n^*$.
Since $n > 2$, then $k = n-1 > 1$, so $k > 1$.
Hence, $k \neq 1$.
Observe that

$$\begin{aligned} k^2 &= (n-1)^2 \\ &= n^2 - 2n + 1 \\ &= n(n-2) + 1 \\ &= 0(n-2) + 1 \\ &= 0 + 1 \\ &= 1. \end{aligned}$$

□

Exercise 58. Let G be a group such that $g^2 = e$ for all $g \in G$.
Then G is abelian.

Proof. Let $a, b \in G$.
Since G is closed under $*$, then $ab \in G$.
Since $xx = e$ for all $x \in G$, then $x^{-1} = x$ by definition of inverse element.
Thus, $a^{-1} = a$ and $b^{-1} = b$ and $(ab)^{-1} = ab$.
Observe that $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

Thus, $ab = ba$.

Since a, b are arbitrary then $ab = ba$ for all $a, b \in G$.

Hence, $*$ is commutative, so $(G, *)$ is abelian. □

Proof. Let $a, b \in G$.

Then $ab \in G$.

Since $g^2 = e$ for all $g \in G$, then $a^2 = e$ and $b^2 = e$ and $(ab)^2 = e$.

Observe that

$$\begin{aligned} aabb &= a^2b^2 \\ &= ee \\ &= e \\ &= (ab)^2 \\ &= (ab)(ab) \\ &= abab. \end{aligned}$$

Thus, $aabb = abab$.

We apply the left cancellation law to obtain $abb = bab$.

We apply the right cancellation law to obtain $ab = ba$.

Therefore, $ab = ba$ for all $a, b \in G$, so $*$ is commutative.

Hence, G is abelian. □

Exercise 59. Let G be a finite group of even order with identity $e \in G$.

Then there exists $a \in G$ such that $a \neq e$ and $a^2 = e$.

Proof. Suppose G is a finite group of even order with identity $e \in G$.

Let n be the order of G.

Then $n \in \mathbb{Z}^+$ and $n = 2k$ for some integer k and n is the number of elements in G.

We can represent the elements of G such that $G = \{a_1, a_2, ..., a_{n-1}, a_n\}$ and $a_n = e$.

Since there are $n = 2k$ elements in G, then there are k pairs of elements in G.

The pairs of elements of G are given by (a_j, a_{j+1}) where $j = 2i - 1$ and $i \in \{1, 2, ..., k\}$ and the last pair is (a_{n-1}, a_n).

We pair consecutive elements of G as inverses of each other, starting in order from left to right, beginning with the element a_1.

Thus, we pair a_1 and a_2 as inverses of each other, so we form the pair (a_1, a_2) and $(a_1)^{-1} = a_2$ and $(a_2)^{-1} = a_1$.

We continue this process, taking the next pair of elements of G in order from left to right.

Thus, the first $k - 1$ pairs can be formed such that in the pair (a_j, a_{j+1}), we have $(a_j)^{-1} = a_{j+1}$ and $(a_{j+1})^{-1} = a_j$.

Consider the last pair $(a_{n-1}, a_n) = (a_{n-1}, e) = (a_{2k-1}, e)$.
This pair contains distinct elements a_{n-1} and e, so $a_{n-1} \neq e$.
Let $a = a_{n-1}$.
Then $a \in G$ and $a \neq e$.
Let b be the inverse of a in G.
Then $ab = ba = e$.

Suppose $b = e$.
Then $e = ab = ae = a$, so $a = e$.
But, this contradicts $a \neq e$.
Therefore, $b \neq e$.

Suppose b is one of the elements in the first $k - 1$ pairs.
Choose some pair (a_j, a_{j+1}) where $j = 2i - 1$ and $i \in \{1, 2, ..., k - 1\}$.
Then $(a_j)^{-1} = a_{j+1}$ and $(a_{j+1})^{-1} = a_j$.
Either $b = a_j$ or $b = a_{j+1}$.
We consider each case separately.
Case 1: Suppose $b = a_j$.
Then $e = ba = a_j a$, so $(a_j)^{-1} = a$.
Hence, $a = (a_j)^{-1} = a_{j+1}$.
But, a is in the last pair, and a_{j+1} is in one of the first $k - 1$ pairs, so $a \neq a_{j+1}$.
Therefore, $b \neq a_j$.
Case 2: Suppose $b = a_{j+1}$.
Then $e = ba = a_{j+1}a$, so $(a_{j+1})^{-1} = a$.
Hence, $a = (a_{j+1})^{-1} = a_j$.
But, a is in the last pair and a_j is in one of the first $k - 1$ pairs, so $a \neq a_j$.
Therefore, $b \neq a_{j+1}$.

Consequently, b is not one of the elements in the first $k - 1$ pairs.
Since $b \neq e$ and b is not one of the elements in the first $k - 1$ pairs, then we are forced to conclude b must be a itself, so $b = a$.
Hence, $e = ab = aa = a^2$, so $a^2 = e$.

Therefore, there exists $a = a_{n-1} \in G$ such that $a \neq e$ and $a^2 = e$, as desired. □

Exercise 60. Let $(G, *)$ be a group with the property : if $a, b, c \in G$ and $ab = ca$, then $b = c$.
Then G is abelian.

Proof. Let $e \in G$ be the identity of G.
Let $a, b \in G$.

Observe that

$$\begin{array}{rcl} ab & = & ab(e) \\ & = & ab(a^{-1}a) \\ & = & (aba^{-1})a. \end{array}$$

Thus, $ab = (aba^{-1})a$.

Since $a \in G$ and $b \in G$ and $aba^{-1} \in G$ and $ab = (aba^{-1})a$, then we conclude $b = aba^{-1}$.

Hence, $ab = (aba^{-1})a = ba$.

Therefore, $ab = ba$ for all $a, b \in G$, so G is abelian. □

Exercise 61. Let $(G, *)$ be a group.

If $(ab)^2 = a^2b^2$ for all $a, b \in G$, then G is abelian.

Proof. Let $a, b \in G$.

Suppose $(ab)^2 = a^2b^2$.

Then $aabb = a^2b^2 = (ab)^2 = (ab)(ab) = abab$.

Hence, $aabb = abab$.

By the left cancellation law, we obtain $abb = bab$.

By the right cancellation law, we obtain $ab = ba$.

Therefore, $ab = ba$ for all $a, b \in G$, so G is abelian. □

Exercise 62. Let $(G, *)$ be a group.

Then G is abelian iff $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Proof. Suppose G is abelian.

Let $a, b \in G$.

Then $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$, so $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. □

Proof. Conversely, suppose $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Let $a, b \in G$.

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

Observe that

$$\begin{array}{rcl} ab & = & [(ab)^{-1}]^{-1} \\ & = & [(ba)^{-1}]^{-1} \\ & = & ba. \end{array}$$

Hence, $ab = ba$, so $ab = ba$ for all $a, b \in G$.

Therefore, G is abelian. □

Exercise 63. Let $(G, *)$ be a group.

Let $a, b, c \in G$.

Then there is a unique $x \in G$ such that $axb = c$.

Proof. Let $e \in G$ be the identity of G.

Let $x = a^{-1}cb^{-1}$.

Since $a \in G$, then $a^{-1} \in G$.

Since $b \in G$, then $b^{-1} \in G$.

Since $a^{-1} \in G$ and $b^{-1} \in G$ and $c \in G$, then $x \in G$, by closure of G under $*$.

Observe that

$$\begin{aligned} a(a^{-1}cb^{-1})b &= (aa^{-1})c(b^{-1}b) \\ &= ece \\ &= ce \\ &= c. \end{aligned}$$

Therefore, there is at least one solution to the equation $axb = c$. □

Proof. We prove there is at most one solution to the equation $axb = c$.

Suppose x' and x'' are solutions to the equation $axb = c$.

Then $ax'b = c$ and $ax''b = c$, so $ax'b = c = ax''b$.

By the left cancellation law we obtain $x'b = x''b$.

By the right cancellation law we obtain $x' = x''$.

Therefore, there is at most one solution to the equation $axb = c$. □

Proof. Since there is at least one solution to the equation $axb = c$ and there is at most one solution to the equation $axb = c$, then there is exactly one solution to the equation $axb = c$, so there is a unique solution to the equation $axb = c$. □

Exercise 64. Let a, b be elements of a group $(G, *)$ with identity $e \in G$.

If $a^4b = ba$ and $a^3 = e$, then $ab = ba$.

Proof. Suppose $a^4b = ba$ and $a^3 = e$.

Then

$$\begin{aligned} ab &= e(ab) \\ &= (a^3)(ab) \\ &= (a^3a)b \\ &= a^4b \\ &= ba. \end{aligned}$$

Therefore, $ab = ba$. □

Exercise 65. Let $(G, *)$ be a group.

If $a^4b = ba$ and $a^3 = e$ for all $a, b \in G$, then G is abelian.

Proof. Let $a, b \in G$.

Suppose $a^4b = ba$ and $a^3 = e$.

Then

$$\begin{aligned} ab &= e(ab) \\ &= (a^3)(ab) \\ &= (a^3a)b \\ &= a^4b \\ &= ba. \end{aligned}$$

Hence, $ab = ba$.

Therefore, $ab = ba$ for all $a, b \in G$, so G is abelian. □

Exercise 66. Let G be a group.

If $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all $a, b \in G$, then G is abelian.

Proof. Suppose $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all $a, b \in G$.

Let $a, b \in G$.

Since $(ab)^3 = a^3b^3$, then $(ab)(ab)(ab) = (aaa)(bbb)$, so by cancellation, we obtain $baba = aabb$.

Since $(ab)^5 = a^5b^5$, then $(ab)(ab)(ab)(ab)(ab) = (aaaaa)(bbbbb)$, so by cancellation, we obtain $babababa = aaaabbbb$.

Substituting, we obtain $(aabb)(aabb) = (aaaa)(bbbb)$.

By cancellation, we obtain $bbaa = aabb$.

Thus, $baba = aabb = bbaa$, so $baba = bbaa$.

Hence, by cancellation, we obtain $ab = ba$, so G is abelian. □

Exercise 67. Let G be a group with identity $e \in G$.

If $a, b \in G$ and $b^6 = e$ and $ab = b^4a$, then $b^3 = e$ and $ab = ba$.

Proof. Suppose $a, b \in G$ and $b^6 = e$ and $ab = b^4a$.

Since $ab = b^4a$, then $aba^{-1} = b^4$.

Observe that

$$\begin{aligned} e &= e^2 \\ &= (b^6)^2 \\ &= b^{12} \\ &= (b^4)^3 \\ &= (aba^{-1})^3 \\ &= (aba^{-1})(aba^{-1})(aba^{-1}) \\ &= abbba^{-1}. \end{aligned}$$

Thus, $e = abbba^{-1}$, so $ae = a = ea = abbba^{-1}a = abbbe = abbb$.

Therefore, $ae = abbb$, so $e = bbb = b^3$.

Hence, $b^3 = e$.

Observe that

$$\begin{aligned} ab &= b^4a \\ &= (b^3b)a \\ &= (eb)a \\ &= ba. \end{aligned}$$

Therefore, $b^3 = e$ and $ab = ba$. □

Exercise 68. Let $(G, *)$ be a group such that for all $x, y \in G$, $xy = x^{-1}y^{-1}$.
Then $(G, *)$ is abelian.

Proof. Let e be the identity of G.
Let $x \in G$.
Then $xe = x^{-1}e^{-1}$.
Thus,

$$\begin{aligned} x &= xe \\ &= x^{-1}e^{-1} \\ &= x^{-1}e \\ &= x^{-1}. \end{aligned}$$

Hence, each element in G is its own inverse.

Let $a, b \in G$.
By closure of $G, ab \in G$.
Since each element in G is its own inverse and $a \in G$ and $b \in G$ and $ab \in G$, then a is its own inverse and b is its own inverse, and ab is its own inverse, so $a^{-1} = a$ and $b^{-1} = b$ and $(ab)^{-1} = ab$.
Observe that

$$\begin{aligned} ab &= (ab)^{-1} \\ &= b^{-1}a^{-1} \\ &= ba. \end{aligned}$$

Therefore, G is abelian. □

Exercise 69. Let $(G, *)$ be a group such that for all $x, y \in G$, $(xy)^2 = xy$.
Then $(G, *)$ is abelian.

Proof. Let $x \in G$.
Then $(xx)^2 = xx$.
Thus,

$$\begin{aligned} xxe &= xx \\ &= (xx)^2 \\ &= (xx)(xx). \end{aligned}$$

Hence, $xxe = xxxx$, so by the left cancellation law, $e = xx$.
Thus, $x^{-1} = x$.
Therefore, each element of G is its own inverse.

Let $a, b \in G$.
Then $ab \in G$.
Observe that

$$\begin{aligned} ab &= (ab)^{-1} \\ &= b^{-1}a^{-1} \\ &= ba. \end{aligned}$$

Therefore, $ab = ba$, so G is abelian. □

Exercise 70. Let $G = \{x \in \mathbb{R} : x > 1\}$.
Define $x * y = xy - x - y + 2$ for all $x, y \in G$.
Then $(G, *)$ is an abelian group.

Solution. To prove G is a group, we must prove:
1. $*$ is a binary operation on G.
2. $*$ is associative.
3. There exists an identity element in G.
4. Each element of G has an inverse in G.

To prove $*$ we must prove G is closed under $*$.
Thus, assume $a, b \in G$.
To prove $a * b \in G$, we must prove $a * b \in \mathbb{R}$ and $ab - a - b + 2 > 1$.
Let's work backwards.

Suppose $a, b \in G$. Then $a, b \in \mathbb{R}$ and $a > 1$ and $b > 1$. To prove $a * b > 1$, we must prove $ab - a - b + 2 > 1$. Thus, $ab - a - b + 2 > 1$ iff $ab - a - b + 1 > 0$ iff $a(b-1) - b + 1 > 0$ iff $a(b-1) - (b-1) > 0$ iff $(a-1)(b-1) > 0$. Since $a > 1$, then $a - 1 > 0$ and $b > 1$ implies $b - 1 > 0$. □

Proof. Since $2 \in \mathbb{R}$ and $2 > 1$, then $2 \in G$, so $G \neq \emptyset$.
Therefore, G is a nonempty set.

We prove $*$ is a binary operation on G.
Let $x, y \in G$.
Then $x, y \in \mathbb{R}$ and $x > 1$ and $y > 1$ and $x * y = xy - x - y + 2$ is unique.
Since $x > 1$ and $y > 1$, then $x - 1 > 0$ and $y - 1 > 0$.
We multiply to obtain $(x-1)(y-1) > 0$.
Thus, $xy - x - y + 1 > 0$, so $xy - x - y + 2 > 1$.
Hence, $x * y > 1$.
By closure of $\mathbb{R}$ under addition and multiplication, $x * y \in \mathbb{R}$.
Since $x * y \in \mathbb{R}$ and $x * y > 1$, then $x * y \in G$.
Since $x * y \in G$ and $x * y$ is unique, then $*$ is a binary operation on G.

We prove $*$ is commutative.

Let $x, y \in G$.

Then

$$\begin{aligned}
x * y &= xy - x - y + 2 \\
&= yx - x - y + 2 \\
&= yx - y - x + 2 \\
&= y * x.
\end{aligned}$$

Therefore, $*$ is commutative.

We prove $*$ is associative.

Let $x, y, z \in G$.

Then

$$\begin{aligned}
(x * y) * z &= (xy - x - y + 2) * z \\
&= (xy - x - y + 2)z - (xy - x - y + 2) - z + 2 \\
&= xyz - xz - yz + 2z - xy + x + y - 2 - z + 2 \\
&= xyz - xz - yz + z - xy + x + y \\
&= xyz - xy - xz - yz + z + x + y \\
&= xyz - xy - xz + x - yz + z + y \\
&= xyz - xy - xz + x - yz + y + z \\
&= xyz - xy - xz + 2x - x - yz + y + z - 2 + 2 \\
&= x(yz - y - z + 2) - x - (yz - y - z + 2) + 2 \\
&= x(y * z) - x - (y * z) + 2 \\
&= x * (y * z).
\end{aligned}$$

Therefore, $*$ is associative.

We prove 2 is an identity for $*$.

Observe that $2 \in G$.

Let $a \in G$.

Then $a * 2 = a(2) - a - 2 + 2 = 2a - a = a$ and $2 * a = 2a - 2 - a + 2 = a$.

Since $2 \in G$ and $a * 2 = a = 2 * a$, then 2 is an identity for $*$.

We prove every element of G has an inverse.

Let $a \in G$.

Then $a \in \mathbb{R}$ and $a > 1$.

Let $b = \frac{a}{a-1}$.

Since $a > 1$, then $a - 1 > 0$, so $a - 1 \neq 0$.

Since $a \in \mathbb{R}$ and $a - 1 \neq 0$, then $b \in \mathbb{R}$.

Since $0 > -1$, then $a > a - 1$.

Since $a - 1 > 0$, we divide by $a - 1$ to get $\frac{a}{a-1} > 1$, so $b > 1$.

Since $b \in \mathbb{R}$ and $b > 1$, then $b \in G$.

Observe that

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

and $a * b = b * a$.

Since $b \in G$ and $a * b = b * a = 2$, then b is an inverse of a.

Therefore, for every element $a \in G$, there exists an inverse $\frac{a}{a-1} \in G$.

Since $*$ is a binary operation on G and $*$ is associative and $2 \in G$ is an identity for $*$ and for every element $a \in G$, there exists an inverse $\frac{a}{a-1} \in G$, then $(G, *)$ is a group.

Since $*$ is commutative, then $(G, *)$ is an abelian group. □

Exercise 71. Define $a * b = \frac{ab}{2}$ for all $a, b \in \mathbb{Q}^*$.

Then $(\mathbb{Q}^*, *)$ is an abelian group.

Proof. Let $a, b \in \mathbb{Q}^*$.

Since multiplication is a binary operation over $\mathbb{Q}^*$, then $ab \in \mathbb{Q}^*$ and ab is unique.

Therefore, $\frac{ab}{2} \in \mathbb{Q}^*$ and $\frac{ab}{2}$ is unique, so $*$ is a binary operation over $\mathbb{Q}^*$.

We prove $*$ is associative.

Let $a, b, c \in \mathbb{Q}^*$.

Then

$$\begin{aligned} (a * b) * c &= \frac{ab}{2} * c \\ &= \frac{(\frac{ab}{2})c}{2} \\ &= \frac{a(\frac{bc}{2})}{2} \\ &= a * \frac{bc}{2} \\ &= a * (b * c). \end{aligned}$$

Therefore, $*$ is associative.

We prove $*$ is commutative.

Let $a, b \in \mathbb{Q}^*$.

Then

$$\begin{aligned} a * b &= \frac{ab}{2} \\ &= \frac{ba}{2} \\ &= b * a. \end{aligned}$$

Therefore, $*$ is commutative.

We prove $\mathbb{Q}^*$ has an identity for $*$.

Let $a \in \mathbb{Q}^*$.

Since $2 \in \mathbb{Q}^*$ and $2 * a = \frac{2a}{2} = a = \frac{a2}{2} = a * 2$, then $2 \in \mathbb{Q}^*$ is an identity for $*$.

We prove every element of $\mathbb{Q}^*$ has an inverse for $*$.

Let $a \in \mathbb{Q}^*$.

Then $a \in \mathbb{Q}$ and $a \neq 0$.

Let $b = \frac{4}{a}$.

Since $a \neq 0$, then $b \in \mathbb{Q}^*$.

Observe that

$$\begin{aligned} a * \frac{4}{a} &= \frac{4}{a} * a \\ &= \frac{(\frac{4}{a})a}{2} \\ &= \frac{4}{2} \\ &= 2. \end{aligned}$$

Therefore, for every element $a \in \mathbb{Q}^*$, there exists an inverse $\frac{4}{a} \in \mathbb{Q}^*$.

Since $*$ is a binary operation on $\mathbb{Q}^*$ and $*$ is associative and $2 \in \mathbb{Q}^*$ is an identity for $*$ and for every element $a \in \mathbb{Q}^*$, there exists an inverse $\frac{4}{a} \in \mathbb{Q}^*$, then $(\mathbb{Q}^*, *)$ is a group.

Since $*$ is commutative, then $(\mathbb{Q}^*, *)$ is an abelian group. □

Exercise 72. Let G be a group with identity $e \in G$.

Let $a, b, c \in G$.

Solve the equation $axc = b$.

Solution. Since $axc = b$, then $axcc^{-1} = bc^{-1}$, so $ax = bc^{-1}$.

Thus, $a^{-1}ax = a^{-1}bc^{-1}$, so $x = a^{-1}bc^{-1}$.

Since $a(a^{-1}bc^{-1})c = (aa^{-1})b(c^{-1}c) = ebe = b$, then the solution is $x = a^{-1}bc^{-1}$. □

Exercise 73. Let $C[0,1] = \{f : [0,1] \to \mathbb{R} | f \text{ is continuous on } [0,1]\}$.

Then $C[0,1]$ is an abelian group under function addition defined by $(f+g)(x) = f(x) + g(x)$ for all $x \in [0,1]$ for all $f, g \in C[0,1]$.

Proof. Let $f, g \in C[0,1]$.

Then $f : [0,1] \to \mathbb{R}$ and $g : [0,1] \to \mathbb{R}$ are continuous functions on the interval $[0,1]$.

The sum $f + g : [0,1] \to \mathbb{R}$ is the unique function defined by $(f+g)(x) = f(x) + g(x)$ for all $x \in [0,1]$.

Let $c \in [0,1]$.

Since f is continuous at $x = c$ and g is continuous at $x = c$, then the sum $f + g$ is continuous at $x = c$.

Since c is arbitrary, then $f + g$ is continuous on the interval $[0,1]$.

Thus, $f + g : [0,1] \to \mathbb{R}$ is a continuous function on the interval $[0,1]$, so $f + g \in C[0,1]$.

Since $f + g \in C[0,1]$ and $f + g$ is unique, then function addition is a binary operation on the set $C[0,1]$.

We prove function addition is associative.

Let $f, g, h \in C[0,1]$.

Then $f : [0,1] \to \mathbb{R}$ and $g : [0,1] \to \mathbb{R}$ and $h : [0,1] \to \mathbb{R}$ are continuous functions on $[0,1]$.

Observe that

$$\begin{aligned} [(f+g)+h](x) &= (f+g)(x) + h(x) \\ &= (f(x) + g(x)) + h(x) \\ &= f(x) + (g(x) + h(x)) \\ &= f(x) + (g+h)(x) \\ &= [f + (g+h)](x) \end{aligned}$$

for all $x \in [0,1]$.

Hence, $(f+g)+h = f+(g+h)$ for all $f, g, h \in C[0,1]$

Therefore, function addition is associative.

We prove function addition is commutative.

Let $f, g \in C[0,1]$.

Observe that

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ &= g(x) + f(x) \\ &= (g+f)(x) \end{aligned}$$

for all $x \in [0,1]$.

Hence, $f + g = g + f$ for all $f, g \in C[0,1]$.

Therefore, function addition is commutative.

Let $i : [0,1] \to \mathbb{R}$ be defined by $i(x) = 0$ for all $x \in [0,1]$.

Since any constant function is continuous on its domain, then in particular, i is continuous on $[0,1]$.

Hence, $i \in C[0,1]$.

We prove i is an identity for function addition.

Let $f \in C[0,1]$.

Then $f : [0,1] \to \mathbb{R}$ is a continuous function.

For all $x \in [0,1]$ we have

$$\begin{aligned}
(i+f)(x) &= i(x) + f(x) \\
&= 0 + f(x) \\
&= f(x) \\
&= f(x) + 0 \\
&= f(x) + i(x) \\
&= (f+i)(x).
\end{aligned}$$

Thus, $(i+f)(x) = f(x) = (f+i)(x)$ for all $x \in [0,1]$, so $i + f = f = f + i$ for all $f \in C[0,1]$.

Since $i \in C[0,1]$ and $i+f = f+i = f$ for all $f \in C[0,1]$, then i is an identity for function addition.

We prove every function in $C[0,1]$ has an inverse for function addition.

Let $f \in C[0,1]$.

Then $f : [0,1] \to \mathbb{R}$ is a continuous function.

Let $-f : [0,1] \to \mathbb{R}$ be defined by $(-f)(x) = -f(x)$ for all $x \in [0,1]$.

Let $c \in [0,1]$.

Then $\lim_{x\to c} (-f)(x) = \lim_{x\to c} -f(x) = -\lim_{x\to c} f(x) = -f(c)$.

Hence, $-f$ is continuous at $x = c$.

Since c is arbitrary, then $-f$ is continuous on $[0,1]$.

Hence, $-f \in C[0,1]$.

For all $x \in [0,1]$ we have

$$\begin{aligned}(f+(-f))(x) &= f(x)+(-f)(x)\\ &= f(x)+[-f(x)]\\ &= 0\\ &= i(x)\\ &= 0\\ &= -f(x)+f(x)\\ &= (-f)(x)+f(x)\\ &= (-f+f)(x).\end{aligned}$$

Thus, $(f+(-f))(x) = i(x) = (-f+f)(x)$ for all $x \in [0,1]$, so $f+(-f) = i = -f+f$ for all $f \in C[0,1]$.

Hence, for every continuous function $f : [0,1] \to \mathbb{R}$, there exists an inverse continuous function $-f : [0,1] \to \mathbb{R}$.

Since function addition is a binary operation on the set $C[0,1]$ and function addition is associative and the constant function $i : [0,1] \to \mathbb{R}$ defined by $i(x) = 0$ for all $x \in [0,1]$ is an identity for function addition and for every continuous function $f : [0,1] \to \mathbb{R}$, there exists an inverse continuous function $-f : [0,1] \to \mathbb{R}$ defined by $(-f)(x) = -f(x)$ for all $x \in [0,1]$, then $C[0,1]$ is a group under function addition.

Since function addition is commutative, then $C[0,1]$ is an abelian group. □

Exercise 74. Let $(G, \cdot)$ be a group.

Let $a \in G$.

Define $*$ on G by $x * y = xay$ for all $x, y \in G$.

Then $(G, *)$ is a group.

Proof. We prove $*$ is a binary operation on G.

Let $x, y \in G$.

Then $x * y = xay$.

Since $(G, \cdot)$ is a group, then G is closed under $\cdot$, so $xay \in G$.

Therefore, $x * y \in G$.

Since xay is unique, then $x * y$ is unique.

Since $x * y \in G$ and $x * y$ is unique, then $*$ is a binary operation on G.

We prove $*$ is associative.

Let $x, y, z \in G$.

Then

$$\begin{aligned}(x * y) * z &= (xay) * z \\ &= (xay)az \\ &= xayaz \\ &= xa(yaz) \\ &= xa(y * z) \\ &= x * (y * z).\end{aligned}$$

Since $(x * y) * z = x * (y * z)$, then $*$ is associative.

We prove there is an identity for $*$.
Let $e \in G$ be the identity for $\cdot$.
Since G is a group and $a \in G$, then $a^{-1} \in G$.
Let $x \in G$.
Then

$$\begin{aligned}x * a^{-1} &= xaa^{-1} \\ &= xe \\ &= x \\ &= ex \\ &= a^{-1}ax \\ &= a^{-1} * x.\end{aligned}$$

Hence, $x * a^{-1} = x = a^{-1} * x$ for all $x \in G$.
Therefore, $a^{-1} \in G$ is an identity for $*$.

We prove for every element $x \in G$, there exists an inverse in G.
Let $x \in G$.
Since G is closed under $\cdot$ and $a, x \in G$, then $(axa)^{-1} \in G$.

Observe that

$$\begin{aligned}
x * (axa)^{-1} &= xa(axa)^{-1} \\
&= xaa^{-1}x^{-1}a^{-1} \\
&= xex^{-1}a^{-1} \\
&= xx^{-1}a^{-1} \\
&= ea^{-1} \\
&= a^{-1} \\
&= a^{-1}e \\
&= a^{-1}x^{-1}x \\
&= a^{-1}x^{-1}ex \\
&= a^{-1}x^{-1}a^{-1}ax \\
&= (axa)^{-1}ax \\
&= (axa)^{-1} * x.
\end{aligned}$$

Hence, $x * (axa)^{-1} = a^{-1} = (axa)^{-1} * x$.
Thus, $(axa)^{-1} \in G$ is an inverse of x.
Therefore, for every $x \in G$ there exists an inverse $(axa)^{-1} \in G$.

Since $*$ is a binary operation on G and $*$ is associative and $a^{-1} \in G$ is an identity for $*$ and for every element $x \in G$, there exists an inverse $(axa)^{-1} \in G$, then $(G, *)$ is a group. □

Exercise 75. Let $G = \mathbb{R}^* \times \mathbb{Z}$.
Define $\circ$ on G by $(a, m) \circ (b, n) = (ab, m + n)$ for all $a, b \in \mathbb{R}^*$ and for all $m, n \in \mathbb{Z}$.
Then $(G, \circ)$ is an abelian group.

Proof. We prove $\circ$ is a binary operation on G.
Let $(a, m) \in G$ and $(b, n) \in G$.
Then $a \in \mathbb{R}^*$ and $m \in \mathbb{Z}$ and $b \in \mathbb{R}^*$ and $n \in \mathbb{Z}$.
Since $(\mathbb{R}^*, \cdot)$ is a group, then $\mathbb{R}^*$ is closed under multiplication.
Since $a \in \mathbb{R}^*$ and $b \in \mathbb{R}^*$, then this implies $ab \in \mathbb{R}^*$.
Since $(\mathbb{Z}, +)$ is a group, then $\mathbb{Z}$ is closed under addition.
Since $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$, then this implies $m + n \in \mathbb{Z}$.
Since $ab \in \mathbb{R}^*$ and $m + n \in \mathbb{Z}$, then $(ab, m + n) \in G$.
Since $(a, m) \circ (b, n) = (ab, m + n)$ and $(ab, m + n) \in G$, then G is closed under $\circ$.
Since $(ab, m + n)$ is unique, then $\circ$ is a binary operation on G.

We prove $\circ$ is associative.
Let $(a, m) \in G$ and $(b, n) \in G$ and $(c, p) \in G$.
Then $a \in \mathbb{R}^*$ and $m \in \mathbb{Z}$ and $b \in \mathbb{R}^*$ and $m \in \mathbb{Z}$ and $c \in \mathbb{R}^*$ and $p \in \mathbb{Z}$.

Observe that

$$\begin{aligned}[(a,m)\circ(b,n)]\circ(c,p) &= (ab,m+n)\circ(c,p)\\ &= ((ab)c,(m+n)+p)\\ &= (a(bc),m+(n+p))\\ &= (a,m)\circ(bc,n+p)\\ &= (a,m)\circ[(b,n)\circ(c,p)].\end{aligned}$$

Therefore, $[(a,m)\circ(b,n)]\circ(c,p) = (a,m)\circ[(b,n)\circ(c,p)]$, so $\circ$ is associative.

We prove $\circ$ is commutative.
Let $(a,m)\in G$ and $(b,n)\in G$.
Then $a\in\mathbb{R}^*$ and $m\in\mathbb{Z}$ and $b\in\mathbb{R}^*$ and $n\in\mathbb{Z}$.
Observe that

$$\begin{aligned}(a,m)\circ(b,n) &= (ab,m+n)\\ &= (ba,m+n)\\ &= (ba,n+m)\\ &= (b,n)\circ(a,m).\end{aligned}$$

Therefore, $(a,m)\circ(b,n) = (b,n)\circ(a,m)$, so $\circ$ is commutative.

We prove $(1,0)$ is identity for $\circ$.
Since $1\in\mathbb{R}$ and $1\neq 0$, then $1\in\mathbb{R}^*$.
Since $1\in\mathbb{R}^*$ and $0\in\mathbb{Z}$, then $(1,0)\in G$.
Let $(a,m)\in G$.
Then $a\in\mathbb{R}^*$ and $m\in\mathbb{Z}$.
Observe that

$$\begin{aligned}(a,m)\circ(1,0) &= (a\cdot 1,m+0)\\ &= (a,m)\\ &= (1\cdot a,0+m)\\ &= (1,0)\circ(a,m).\end{aligned}$$

Since $(1,0)\in G$ and $(a,m)\circ(1,0) = (1,0)\circ(a,m) = (a,m)$, then $(1,0)$ is an identity element for $\circ$.

We prove each element of G has an inverse in G.
Let $(a,m)\in G$.
Then $a\in\mathbb{R}^*$ and $m\in\mathbb{Z}$.
Since $(\mathbb{R}^*,\cdot)$ is a group and $a\in\mathbb{R}^*$, then $\frac{1}{a}\in\mathbb{R}^*$.
Since $(\mathbb{Z},+)$ is a group and $m\in\mathbb{Z}$, then $-m\in\mathbb{Z}$.
Since $\frac{1}{a}\in\mathbb{R}^*$ and $-m\in\mathbb{Z}$, then $(\frac{1}{a},-m)\in G$.

Observe that

$$\begin{array}{rcl} (a,m)\circ(\dfrac{1}{a},-m) & = & (a\cdot\dfrac{1}{a},m+(-m)) \\ & = & (1,0) \\ & = & (\dfrac{1}{a}\cdot a,-m+m) \\ & = & (\dfrac{1}{a},-m)\circ(a,m). \end{array}$$

Since $(\frac{1}{a},-m)\in G$ and $(a,m)\circ(\frac{1}{a},-m)=(\frac{1}{a},-m)\circ(a,m)=(1,0)$, then $(\frac{1}{a},-m)$ is an inverse of (a,m).

Therefore, for every $(a,m)\in G$, there is an inverse $(\frac{1}{a},-m)\in G$.

Since $\circ$ is a binary operation on G and $\circ$ is associative and $(1,0)\in G$ is an identity element and for every $(a,m)\in G$, there is an inverse $(\frac{1}{a},-m)\in G$, then $(G,\circ)$ is a group.

Since $\circ$ is commutative, then $(G,\circ)$ is an abelian group. □

Exercise 76. Let $(G,*)$ be a group.

Define a relation $\sim$ on G for all $x,y\in G$ by $x\sim y$ iff there exists some $a\in G$ such that $y=axa^{-1}$.

Then $\sim$ is an equivalence relation on G.

Proof. We prove $\sim$ is reflexive.

Let x be an arbitrary element of G.

Let e be the identity element in G.

Since $e\in G$ and $x=xe=xe^{-1}=exe^{-1}$, then $\sim$ is reflexive. □

Proof. We prove $\sim$ is symmetric.

Let x and y be arbitrary elements of G such that $x\sim y$.

Then there exists some $a\in G$ such that $y=axa^{-1}$.

Hence, $ya=ax$.

Let $b=a^{-1}$.

Since $a\in G$, then $a^{-1}\in G$, so $b\in G$.

Observe that

$$\begin{array}{rcl} byb^{-1} & = & a^{-1}y(a^{-1})^{-1} \\ & = & a^{-1}ya \\ & = & a^{-1}(ya) \\ & = & a^{-1}(ax) \\ & = & (a^{-1}a)x \\ & = & ex \\ & = & x. \end{array}$$

Since $b\in G$ and $x=byb^{-1}$, then $y\sim x$, so $\sim$ is symmetric. □

Proof. We prove $\sim$ is transitive.

Let x, y, and z be arbitrary elements of G such that $x \sim y$ and $y \sim z$.

Since $x \sim y$, then there exists $a \in G$ such that $y = axa^{-1}$.

Since $y \sim z$, then there exists $b \in G$ such that $z = byb^{-1}$.

Let $c = ba$.

Since $a \in G$ and $b \in G$ and G is closed under $*$, then $ba \in G$, so $c \in G$.

Observe that

$$\begin{aligned} cxc^{-1} &= (ba)x(ba)^{-1} \\ &= (ba)x(a^{-1}b^{-1}) \\ &= b(axa^{-1})b^{-1} \\ &= byb^{-1} \\ &= z. \end{aligned}$$

Since $c \in G$ and $z = cxc^{-1}$, then $x \sim z$, so $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric, and transitive, then $\sim$ is an equivalence relation on G. □

Subgroups

Exercise 77. The set of even integers $2\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.

Proof. We prove $2\mathbb{Z} \subset \mathbb{Z}$.

Since $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$, then $2\mathbb{Z}$ is a subset of $\mathbb{Z}$, so $2\mathbb{Z} \subset \mathbb{Z}$.

We prove $2\mathbb{Z}$ is closed under addition.

Let $a, b \in 2\mathbb{Z}$.

Since $a \in 2\mathbb{Z}$, then $a = 2m$ for some integer m.

Since $b \in 2\mathbb{Z}$, then $b = 2n$ for some integer n.

Thus, $a + b = 2m + 2n = 2(m + n)$.

Since $m + n$ is an integer, then $2(m + n) \in 2\mathbb{Z}$, so $a + b \in 2\mathbb{Z}$.

Therefore, $2\mathbb{Z}$ is closed under addition.

We prove the additive identity $0 \in \mathbb{Z}$ is in $2\mathbb{Z}$.

Since $0 = 2 \cdot 0$ and $0 \in \mathbb{Z}$ is the additive identity of $\mathbb{Z}$, then $0 \in 2\mathbb{Z}$.

Therefore, the additive identity $0 \in \mathbb{Z}$ is in $2\mathbb{Z}$.

We prove $2\mathbb{Z}$ is closed under inverses.

Let $2k \in 2\mathbb{Z}$.

Then $k \in \mathbb{Z}$.

Since $2k + (-2k) = [2 + (-2)]k = 0k = 0 = k0 = k(-2 + 2) = k(-2) + 2k = -2k + 2k$, then $2k + (-2k) = 0 = -2k + 2k$, so $-2k$ is additive inverse of $2k$.

Since $-2k = 2(-k)$ and $-k$ is an integer, then $-2k \in 2\mathbb{Z}$.

Therefore, for every $2k \in 2\mathbb{Z}$, there is an additive inverse $-2k$ in $2\mathbb{Z}$, so $2\mathbb{Z}$ is closed under inverses.

Since $2\mathbb{Z} \subset \mathbb{Z}$ and $2\mathbb{Z}$ is closed under addition and the additive identity $0 \in \mathbb{Z}$ is in $2\mathbb{Z}$ and $2\mathbb{Z}$ is closed under inverses, then by the first subgroup test, $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. □

Exercise 78. Let $H = \{2^k : k \in \mathbb{Z}\}$.
Then $(H, \cdot)$ is a subgroup of $(\mathbb{Q}^*, \cdot)$.

Proof. We prove $H \subset \mathbb{Q}^*$.
Let $h \in H$.
Then $h = 2^k$ for some integer k.
Either $k > 0$ or $k = 0$ or $k < 0$.
We consider these cases separately.
Case 1: Suppose $k = 0$.
Then $h = 2^0 = 1 = \frac{1}{1} \neq 0$.
Therefore, $h \in \mathbb{Q}^*$.
Case 2: Suppose $k > 0$.
Then $2^k \in \mathbb{Z}$ and $2^k > 0$, so $2^k \neq 0$.
Therefore, $h = 2^k = \frac{2^k}{1} \in \mathbb{Q}^*$.
Case 3: Suppose $k < 0$.
Since $k \in \mathbb{Z}$, then $-k \in \mathbb{Z}$.
Since $k < 0$, then $-k > 0$.
Thus, $2^{-k} \in \mathbb{Z}$ and $2^{-k} > 0$, so $2^{-k} \neq 0$.
Therefore, $h = 2^k = \frac{1}{2^{-k}} \in \mathbb{Q}^*$.
Hence, in all cases, $h \in \mathbb{Q}^*$.
Since $h \in H$ implies $h \in \mathbb{Q}^*$, then $H \subset \mathbb{Q}^*$.

We prove H is closed under multiplication.
Let $a, b \in H$.
Since $a \in H$, then $a = 2^k$ for some integer k.
Since $b \in H$, then $b = 2^m$ for some integer m.
Thus, $ab = (2^k)(2^m) = 2^{k+m}$.
Since $k + m \in \mathbb{Z}$, then $ab \in H$, so H is closed under multiplication.

We prove the multiplicative identity $1 \in \mathbb{Q}^*$ is in H.
Since $0 \in \mathbb{Z}$ and $1 = 2^0$, then $1 \in H$.
Therefore, the multiplicative identity $1 \in \mathbb{Q}^*$ is in H.

We prove H is closed under inverses.
Let $2^k \in H$.
Then $k \in \mathbb{Z}$.
Since $2^k \cdot 2^{-k} = 2^{k-k} = 2^0 = 1 = 2^0 = 2^{-k+k} = 2^{-k} \cdot 2^k$, then $2^k \cdot 2^{-k} = 1 = 2^{-k} \cdot 2^k$, so 2^{-k} is multiplicative inverse of 2^k.
Since $-k \in \mathbb{Z}$, then $2^{-k} \in H$.

Therefore, for every $2^k \in H$, there is a multiplicative inverse $2^{-k} \in H$, so H is closed under inverses.

Since $H \subset \mathbb{Q}^*$ and H is closed under multiplication and the multiplicative identity $1 \in \mathbb{Q}^*$ is in H and H is closed under inverses, then by the first subgroup test, $H < G$. □

Exercise 79. Let $(G, \cdot)$ be an abelian group.
Let $H = \{a \in G : a^2 = e\}$.
Then H is a subgroup of G.

Proof. Let $e \in G$ be the identity of G.
Let $x \in H$.
Then by definition of H, $x \in G$.
Hence, $x \in H$ implies $x \in G$, so $H \subset G$.

Let $x, y \in H$.
Then $x, y \in G$ and $x^2 = e$ and $y^2 = e$.
Since G is closed under $\cdot$ and $x \in G$ and $y \in G$, then $xy \in G$.
Observe that

$$\begin{aligned}(xy)^2 &= (xy)(xy)\\ &= x(yx)y\\ &= x(xy)y\\ &= (xx)(yy)\\ &= x^2y^2\\ &= ee\\ &= e.\end{aligned}$$

Since $xy \in G$ and $(xy)^2 = e$, then $xy \in H$.
Therefore, H is closed under $*$.
Since $e \in G$ and $e^2 = ee = e$, then by definition of H, $e \in H$.

Let $x \in H$.
Then $x \in G$ and $x^2 = e$.
Since G is a group then $x^{-1} \in G$.
Observe that $(x^{-1})^2 = (x^2)^{-1} = e^{-1} = e$.
Since $x^{-1} \in G$ and $(x^{-1})^2 = e$, then $x^{-1} \in H$.
Therefore, for each $x \in H$ there exists $x^{-1} \in H$.

Since $H \subset G$ and H is closed under $\cdot$ and $e \in H$ and for every $x \in H$ there exists $x^{-1} \in H$, then by the subgroup test, H is a subgroup of G. □

Exercise 80. Let G be an abelian group.
Let $H = \{e\} \cup \{g \in G : |g| = 2\}$.
Then $H < G$.

Proof. Let e be the identity of G.
Let $h \in H$.
Then either $h \in \{e\}$ or $h \in \{g \in G : |g| = 2\}$.
Thus, either $h = e$ or $h \in G$.
Since $e \in G$, then either $h \in G$ or $h \in G$.
Hence, $h \in G$.
Therefore, $h \in H$ implies $h \in G$, so $H \subset G$.
Since $e \in \{e\}$, then $e \in H$.

Let $a, b \in H$.
Since $a \in H$, then either $a = e$ or $|a| = 2$.
Since $b \in H$, then either $b = e$ or $|b| = 2$.
Therefore, there are four cases to consider.
Case 1: Suppose $a = e$ and $b = e$.
Then $ab = ee = e$.
Since $e \in H$, then $ab \in H$.
Case 2: Suppose $a = e$ and $|b| = 2$.
Then $ab = eb = b$.
Since $b \in H$, then $ab \in H$.
Case 3: Suppose $|a| = 2$ and $b = e$.
Then $ab = ae = a$.
Since $a \in H$, then $ab \in H$.
Case 4: Suppose $|a| = 2$ and $|b| = 2$.
Then $a^2 = e = b^2$.
Thus,

$$\begin{aligned}(ab)^2 &= a^2b^2 \\ &= ee \\ &= e.\end{aligned}$$

Let k be the order of ab.
Then $(ab)^2 = e$ iff $k|2$.
Hence, $k|2$.
Thus, either $k = 1$ or $k = 2$.
Suppose $k = 1$.
Then $e = (ab)^1 = ab$, so $ab = e$.
Thus, $ab \in \{e\}$, so $ab \in H$.
Suppose $k = 2$.
Then $|ab| = 2$.
Since $a, b \in H$ and $H \subset G$, then $a, b \in G$.
By closure of G under its binary operation, $ab \in G$.
Since $ab \in G$ and $|ab| = 2$, then $ab \in \{g \in G : |g| = 2\}$.
Thus, $ab \in H$.
Hence, in either case, $ab \in H$.
Therefore, in all cases, $ab \in H$.

Hence, H is closed under $*$ of G.

Let $a \in H$.

Then either $a = e$ or $|a| = 2$.

We consider these cases separately.

Case 1: Suppose $a = e$.

Then $a^{-1} = e^{-1} = e$.

Since $e \in H$, then $a^{-1} \in H$.

Case 2: Suppose $|a| = 2$.

Then 2 is the least positive integer such that $a^2 = e$. Therefore, $a = a^1 \neq e$, so $a \neq e$. Suppose that $a^{-1} = e$. Then $aa^{-1} = ae$, so $e = a$. Thus, we have $a \neq e$ and $a = e$, a contradiction. Hence, $a^{-1} \neq e$. Observe that

$$\begin{aligned} (a^{-1})^2 &= (a^2)^{-1} \\ &= e^{-1} \\ &= e. \end{aligned}$$

Thus, the order of a^{-1} is 2.

Since $a^{-1} \in G$ and $|a^{-1}| = 2$, then $a^{-1} \in H$.

Hence, in all cases, $a^{-1} \in H$.

Therefore, H is closed under taking inverses.

Thus, $H < G$. □

Exercise 81. Let G be an abelian group and let n be a fixed positive integer. Let $H = \{a^n : a \in G\}$. Then $H < G$.

Proof. Let $a^n \in H$.

Then $a \in G$.

Since $a^k \in G$ for every integer k, then in particular, $a^n \in G$.

Hence, $a^n \in H$ implies $a^n \in G$, so $H \subset G$.

Let e be the identity of G.

Since $e \in G$ and $e = e^n$, then $e \in H$.

Let $x, y \in H$.

Then $x = a^n$ for some $a \in G$ and $y = b^n$ for some $b \in G$.

By closure of G, $ab \in G$.

Observe that $xy = a^n b^n = (ab)^n$.

Thus, there exists $ab \in G$ such that $xy = (ab)^n$.

Hence, $xy \in H$, so H is closed.

Let x^{-1} be the inverse of x in G.

Since $a^{-1} \in G$ and $x^{-1} = (a^n)^{-1} = (a^{-1})^n$, then $x^{-1} \in H$.

Thus, H is closed under inverses.

Therefore, by the subgroup test, $H < G$. □

Exercise 82. Let G be an abelian group and let n be a fixed positive integer.

Let $G_n = \{x \in G : x^n = e\}$.

Then $G_n < G$.

Proof. Let e be the identity of G.

Since $e \in G$ and $e^n = e$, then $e \in G_n$.

Observe that G_n is a subset of G.

Let $a, b \in G_n$.

Then $a, b \in G$ and $a^n = e = b^n$.

By closure of $G, ab \in G$.

Observe that $(ab)^n = a^n b^n = ee = e$.

Thus, $ab \in G$ and $(ab)^n = e$, so $ab \in G_n$.

Let $a \in G_n$.

Then $a \in G$ and $a^n = e$.

Let a^{-1} be the inverse of a in G.

Then $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$.

Thus, $a^{-1} \in G4$ and $(a^{-1})^n = e$, so $a^{-1} \in G_n$.

Therefore, $G_n < G$. □

Exercise 83. Let $\langle G, * \rangle$ be an abelian group.

Let $H = \{a \in G : a^n = e, n \in \mathbb{Z}^+\}$.

Then H is a subgroup of G.

Solution. Our hypothesis is: $\langle G, * \rangle$ is an abelian group.

Our conclusion is: H is a subgroup of G.

We must prove: H is a subgroup of G.

To prove this we must show:

1. $H \subset G$.
2. H is closed under $*$.
3. $e \in H$.
4. $\forall x \in H . x^{-1} \in H$.

Note that H is simply a collection of all elements of G which have finite order.

Thus, we're proving the set of all elements of an abelian group G which have finite order is a subgroup of G. □

Proof. Let $e \in G$ be the identity of group G.

Observe that $H \subset G$.

Let $x, y \in H$.

Then $x, y \in G$ and $x^m = e$ and $y^n = e$ for some $m, n \in \mathbb{Z}^+$. Since $x, y \in G$ and G is closed under $*$, then $xy \in G$. Since G is an abelian group we know $(xy)^k = x^k y^k$ for any $k \in \mathbb{Z}$. Observe that $(xy)^{mn} = x^{mn} y^{mn} = (x^m)^n y^{mn} = e^n y^{mn} = e y^{mn} = y^{mn} = y^{nm} = (y^n)^m = e^m = e$. Since $xy \in G$ and $(xy)^{mn} = e$ and $mn \in \mathbb{Z}^+$, then $xy \in H$. Since x, y are arbitrary then $xy \in H$ for all $x, y \in H$. Therefore, H is closed under $*$.

Since $e \in G$ and $e^1 = e$, then $e \in H$.

Let $x \in H$. Then $x \in G$ and $x^k = e$ for some $k \in \mathbb{Z}^+$. Since G is a group and $x \in G$, then $x^{-1} \in G$. Observe that $(x^{-1})^k = (x^k)^{-1} = e^{-1} = e$. Since $x^{-1} \in G$ and $(x^{-1})^k = e$, then $x^{-1} \in H$. Hence, for each $x \in H$, $x^{-1} \in H$.

Therefore, H is a subgroup of G. □

Exercise 84. Let $C[0,1] = \{f : [0,1] \to \mathbb{R} | f \text{ is continuous on } [0,1]\}$ be the abelian group under function addition.

Let P_n be the set of all functions in $C[0,1]$ of the form $a_nx^n + ... + a_1x + a_0$, where each $a_i \in \mathbb{R}$.

Then P_n is subgroup of $C[0,1]$.

Proof. Clearly, $P_n \subset C[0,1]$.

Let $f, g \in P_n$.

Then $f, g \in C[0,1]$ and $f : [0,1] \to \mathbb{R}$ is a function of the form $f(x) = a_nx^n + ... + a_1x + a_0$ and each $a_i \in \mathbb{R}$ and $g : [0,1] \to \mathbb{R}$ is a function of the form $g(x) = b_nx^n + ... + b_1x + b_0$ and each $b_i \in \mathbb{R}$.

By closure of $C[0,1]$, the sum $f + g$ is in $C[0,1]$.

Observe that

$$\begin{aligned}(f+g)(x) &= (a_nx^n + ... + a_1x + a_0) + (b_nx^n + ... + b_1x + b_0) \\ &= (a_n + b_n)x^n + ... + (a_1 + b_1)x + (a_0 + b_0).\end{aligned}$$

Hence, $f + g \in P_n$.

Since function addition is associative in $C[0,1]$ and $P_n \subset C[0,1]$, then function addition is associative in P_n.

Let the additive identity of $C[0,1]$ be the function $i : [0,1] \to \mathbb{R}$ defined by $i(x) = 0$ for all $x \in [0,1]$.

Since $i(x) = 0 = 0x^n + ... + 0x + 0$, then $i \in P_n$.

Let $f \in P_n$.

Then $f : [0,1] \to \mathbb{R}$ is a function and $f(x) = a_nx^n + ... + a_1x + a_0$ and each $a_i \in \mathbb{R}$.

The additive inverse of f is the continuous function $-f : [0,1] \to \mathbb{R}$ defined by $(-f)(x) = -f(x)$ for all $x \in [0,1]$.

Observe that

$$\begin{aligned}(-f)(x) &= -f(x) \\ &= -(a_nx^n + ... + a_1x + a_0) \\ &= -a_nx^n - ... - a_1x - a_0\end{aligned}$$

and each coefficient $-a_i$ is a real number.

Hence, $-f \in P_n$.

Therefore, $P_n < C[0,1]$ □

Exercise 85. Let $C[0,1] = \{f : [0,1] \to \mathbb{R} | f \text{ is continuous on } [0,1]\}$ be the abelian group under function addition.

Let $X \subset [0,1]$.

Let $H = \{f \in C[0,1] : (\forall x \in X)(f(x) = 0)\}$.

Then $H < C[0,1]$.

Proof. TO DO □

Exercise 86. Let G be a group.

If $H < G$ and $K < G$, then $H \cap K < K$.

Proof. Suppose $H < G$ and $K < G$.

Since $H \cap K = K \cap H$ and $K \cap H \subset K$, then $H \cap K \subset K$.

Let e be the identity of G.

Since $H < G$, then $e \in H$.

Since $K < G$, then $e \in K$.

Hence, $e \in H$ and $e \in K$, so $e \in H \cap K$.

Let $a, b \in H \cap K$.

Then $a \in H \cap K$ and $b \in H \cap K$.

Thus, $a \in H$ and $a \in K$ and $b \in H$ and $b \in K$.

By closure of $H, ab \in H$.

By closure of $K, ab \in K$.

Hence, $ab \in H$ and $ab \in K$, so $ab \in H \cap K$.

Let $a \in H \cap K$.

Then $a \in H$ and $a \in K$.

Since H is a group, then $a^{-1} \in H$.

Since K is a group, then $a^{-1} \in K$.

Hence, $a^{-1} \in H$ and $a^{-1} \in K$, so $a^{-1} \in H \cap K$.

Therefore, by the subgroup test, $H \cap K < K$. □

Exercise 87. Let n be an integer greater than 1.

Let $H_n = \{x \in \mathbb{R}^+ : x^n \in \mathbb{Q}\}$.

Then H_n is a subgroup of $\mathbb{R}^+$.

Also, $\mathbb{Q}^+ \subset H_2 \subset H_4 \subset ... \subset H_{2^n} \subset ...$ is an increasing chain of subgroups of $\mathbb{R}^+$.

Proof. Clearly, $H_n \subset \mathbb{R}^+$.

Let $x, y \in H_n$.

Then $x \in \mathbb{R}^+$ and $x^n \in \mathbb{Q}$ and $y \in \mathbb{R}^+$ and $y^n \in \mathbb{Q}$.

Thus, there exist integers a, b with $b \neq 0$ such that $x^n = \frac{a}{b}$ and there exist integers c, d with $d \neq 0$ such that $y^n = \frac{c}{d}$.

By closure of $\mathbb{R}^+$ under multiplication, $xy \in \mathbb{R}^+$.

Observe that

$$\begin{aligned}(xy)^n &= x^n y^n\\ &= \frac{a}{b}\frac{c}{d}\\ &= \frac{ac}{bd}\end{aligned}$$

Since $b \neq 0$ and $d \neq 0$, then $bd \neq 0$.

Since ac and bd are integers and $bd \neq 0$, then $(xy)^n \in \mathbb{Q}$.

Thus, $xy \in \mathbb{R}^+$ and $(xy)^n \in \mathbb{Q}$, so $xy \in H_n$.

Hence, H_n is closed under multiplication.

Since 1 is a positive real number and $1^n = 1 = \frac{1}{1}$, then $1^n \in \mathbb{Q}$.

Thus, $1 \in H_n$.

Let $x \in H_n$.

Then $x \in \mathbb{R}^+$ and $x^n \in \mathbb{Q}$.

Hence, there exist integers a, b with $b \neq 0$ such that $x^n = \frac{a}{b}$.

Since $x \in \mathbb{R}^+$, then $x \in \mathbb{R}$ and $x > 0$.

By closure of $\mathbb{R}^+$ under multiplication, $x^n \in \mathbb{R}^+$, so $\frac{a}{b} \in \mathbb{R}^+$.

Hence, $\frac{a}{b} > 0$, so $\frac{a}{b} \neq 0$.

Since $\frac{a}{b} = 0$ iff $a \neq 0$, then $a \neq 0$.

Since $\mathbb{R}^+$ is a group, then $x^{-1} \in \mathbb{R}^+$.

Observe that

$$\begin{aligned}(x^{-1})^n &= (x^n)^{-1}\\ &= (\frac{a}{b})^{-1}\\ &= \frac{b}{a}.\end{aligned}$$

Since $a, b \in \mathbb{Z}$ and $a \neq 0$, then $(x^{-1})^n \in \mathbb{Q}$.

Thus, $x^{-1} \in \mathbb{R}^+$ and $(x^{-1})^n \in \mathbb{Q}$, so $x^{-1} \in H_n$.

Therefore, $H_n < \mathbb{R}^+$. □

Exercise 88. Let G be a group.

Let $a, b \in G$.

If either $ab \in C(a)$ or $ba \in C(a)$, then $b \in C(a)$.

Proof. Suppose either $ab \in C(a)$ or $ba \in C(a)$.

We consider these cases separately.

Case 1: Suppose $ab \in C(a)$.

Then $ab \in G$ and $(ab)a = a(ab)$.

Thus, $aba = aab$.

By the left cancellation law, we have $ba = ab$.

Hence, $b \in G$ and $ba = ab$, so $b \in C(a)$.

Case 2: Suppose $ba \in C(a)$.

Then $ba \in G$ and $(ba)a = a(ba)$.

Thus, $baa = aba$.
By the right cancellation law, we have $ba = ab$.
Hence, $b \in G$ and $ba = ab$, so $b \in C(a)$.
Therefore, in either case, $b \in C(a)$, as desired. □

Exercise 89. The normalizer $N(H)$ of H in G is a subgroup.
Let $(H, *)$ be a subgroup of a group $(G, *)$.
Define $N(H) = \{g \in G : gh = hg \text{ for all } h \in H\ \}$.
Then $N(H)$ is a subgroup of G.

Proof. Since $N(H) = \{g \in G : gh = hg \text{ for all } h \in H\ \}$, then $N(H) \subset G$.

We prove $N(H)$ is closed under the binary operation $*$ of G.
Let $e \in G$ be the identity of G.
Let $a, b \in N(H)$.
Since $a \in N(H)$, then $a \in G$ and $ah = ha$ for all $h \in H$.
Since $b \in N(H)$, then $b \in G$ and $bh = hb$ for all $h \in H$.
Since $a \in G$ and $b \in G$, then by closure of G, we have $ab \in G$.
Let $h \in H$.
Observe that

$$\begin{aligned} (ab)h &= a(bh) \\ &= a(hb) \\ &= (ah)b \\ &= (ha)b \\ &= h(ab). \end{aligned}$$

Thus, $(ab)h = h(ab)$ for all $h \in H$.
Since $ab \in G$ and $(ab)h = h(ab)$ for all $h \in H$, then $ab \in N(H)$.
Therefore, $N(H)$ is closed under the binary operation of G. □

Proof. We prove $N(H)$ is closed under the identity $e \in G$.
Since $e \in G$ and $H < G$, then $e \in H$.

Let $h \in H$.
Since H is a group and $e \in H$, then $eh = he = h$, so $eh = he$.
Therefore, $eh = he$ for all $h \in H$.
Since $e \in G$ and $eh = he$ for all $h \in H$, then $e \in N(H)$.
Therefore, $N(H)$ is closed under the identity $e \in G$. □

Proof. We prove $N(H)$ is closed under inverses.
Let $a \in N(H)$.
Then $a \in G$ and $ah = ha$ for all $h \in H$.
Since G is a group and $a \in G$, then $a^{-1} \in G$.

Let $h \in H$.

Observe that

$$\begin{aligned} a^{-1}h &= a^{-1}he \\ &= a^{-1}h(aa^{-1}) \\ &= a^{-1}(ha)a^{-1} \\ &= a^{-1}(ah)a^{-1} \\ &= (a^{-1}a)(ha^{-1}) \\ &= eha^{-1} \\ &= ha^{-1}. \end{aligned}$$

Thus, $a^{-1}h = ha^{-1}$ for all $h \in H$.

Since $a^{-1} \in G$ and $a^{-1}h = ha^{-1}$ for all $h \in H$, then $a^{-1} \in N(H)$.

Therefore, $N(H)$ is closed under inverses. □

Proof. Since $N(H) \subset G$ and $N(H)$ is closed under the binary operation of G and $N(H)$ is closed under the identity $e \in G$ and $N(H)$ is closed under inverses, then by the subgroup test, $N(H)$ is a subgroup of G. □