

(15) Let $\mathcal{F}(\mathbb{R})$ denote the set of all functions from \mathbb{R} to \mathbb{R} . Define addition and multiplication on $\mathcal{F}(\mathbb{R})$ as follows:

- For all $f, g \in \mathcal{F}(\mathbb{R})$, $(f + g) : \mathbb{R} \rightarrow \mathbb{R}$ is the function defined by

$$(f + g)(x) = f(x) + g(x)$$

for all $x \in \mathbb{R}$.

- $f, g \in \mathcal{F}(\mathbb{R})$, $(fg) : \mathbb{R} \rightarrow \mathbb{R}$ is the function defined by

$$(fg)(x) = f(x)g(x)$$

for all $x \in \mathbb{R}$.

(a) Prove that $\mathcal{F}(\mathbb{R})$ is an Abelian group under addition.

For this proof we will first show that $\mathcal{F}(\mathbb{R})$ is closed under addition, that addition is associative in $\mathcal{F}(\mathbb{R})$, that $\mathcal{F}(\mathbb{R})$ contains an identity element, and that each element in $\mathcal{F}(\mathbb{R})$ has an inverse. Finally, we will show that addition is commutative in $\mathcal{F}(\mathbb{R})$.

First of all, from the definition of addition in $\mathcal{F}(\mathbb{R})$ we see that this operation will always give us another function from the reals to the reals which is also an element in $\mathcal{F}(\mathbb{R})$. Therefore, $\mathcal{F}(\mathbb{R})$ is closed under addition. Next, we will prove that addition is associative in $\mathcal{F}(\mathbb{R})$.

Proof. Let $f, g, h \in \mathcal{F}(\mathbb{R})$ and let $x \in \mathbb{R}$. From the definition of addition in $\mathcal{F}(\mathbb{R})$ we know that

$$((f + g) + h)(x) = (f(x) + g(x)) + h(x) \quad (1)$$

and

$$(f + (g + h))(x) = f(x) + (g(x) + h(x)) \quad (2)$$

We also know that

$$f(x) \in \mathbb{R}, \quad (3)$$

$$g(x) \in \mathbb{R}, \quad (4)$$

and

$$h(x) \in \mathbb{R} \quad (5)$$

from the fact that the codomain of f, g , and h is \mathbb{R} . We already know that addition is associative in \mathbb{R} . From this fact and the equations (3), (4), and (5) we also know that

$$(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x)). \quad (6)$$

Applying the transitive property of equality to (6) and (1), we obtain

$$((f + g) + h)(x) = f(x) + (g(x) + h(x)). \quad (7)$$

Applying this same property again to (7) and (2), we obtain

$$((f + g) + h)(x) = (f + (g + h))(x). \quad (8)$$

Finally, from (8) we see that addition is associative in $\mathcal{F}(\mathbb{R})$. \square

Next we will prove that $\mathcal{F}(\mathbb{R})$ contains an identity element.

Proof. Let $e \in \mathcal{F}(\mathbb{R})$ such that

$$e(x) = 0 \quad (9)$$

for all $x \in \mathbb{R}$. Let $f \in \mathcal{F}(\mathbb{R})$ and let $a \in \mathbb{R}$. We see that

$$(f + e)(a) = f(a) + e(a) = f(a) + 0 = f(a)$$

and

$$(e + f)(a) = e(a) + f(a) = 0 + f(a) = f(a).$$

In conclusion, we have shown that $(f + e)(a) = (e + f)(a) = f(a)$ for some $a \in \mathbb{R}$ and therefore the function e defined $e(x) = 0$ for all $x \in \mathbb{R}$ is the identity element in $\mathcal{F}(\mathbb{R})$. \square

Next will show that each function in $\mathcal{F}(\mathbb{R})$ has an inverse under addition.

Proof. Let $f \in \mathcal{F}(\mathbb{R})$ and let $x \in \mathbb{R}$. First we note that $f(x) \in \mathbb{R}$. Because the reals are a group under addition we know that there exists some $g \in \mathcal{F}(\mathbb{R})$ such that $f(x) + g(x) = 0$ and $g(x) + f(x) = 0$. Therefore, the arbitrary element $f \in \mathcal{F}(\mathbb{R})$ has an inverse.

In conclusion we have shown that every element in $\mathcal{F}(\mathbb{R})$ has an inverse. \square

Finally, we will show that every element in $\mathcal{F}(\mathbb{R})$ commutes under addition.

Proof. Let $f, g \in \mathcal{F}(\mathbb{R})$ and let $x \in \mathbb{R}$. We know that

$$(f + g)(x) = f(x) + g(x) \quad (10)$$

and

$$(g + f)(x) = g(x) + f(x) \quad (11)$$

from the definition of a function in $\mathcal{F}(\mathbb{R})$. We also know that

$$f(x) \in \mathbb{R} \quad (12)$$

and

$$g(x) \in \mathbb{R} \quad (13)$$

from the fact that a function in $\mathcal{F}(\mathbb{R})$ has the codomain \mathbb{R} . Because addition is commutative in \mathbb{R} , from (12) and (13) we can conclude that

$$f(x) + g(x) = g(x) + f(x). \quad (14)$$

Applying the transitive property of equality to (10) and (14) we obtain

$$(f + g)(x) = g(x) + f(x). \quad (15)$$

Applying this same property to (15) and (11) we obtain

$$(g + f)(x) = (f + g)(x).$$

In conclusion, we have shown that $(g + f)(x) = (f + g)(x)$ for all $x \in \mathbb{R}$ and therefore addition is commutative in $\mathcal{F}(\mathbb{R})$. \square

In conclusion, we have shown that $\mathcal{F}(\mathbb{R})$ is closed under addition, addition is associative in $\mathcal{F}(\mathbb{R})$, $\mathcal{F}(\mathbb{R})$ contains an identity element, each element in $\mathcal{F}(\mathbb{R})$ has an inverse, and addition is commutative in $\mathcal{F}(\mathbb{R})$. From this we know that $\mathcal{F}(\mathbb{R})$ is an Abelian group under addition.

(b) Does $\mathcal{F}(\mathbb{R})$ have an identity element for multiplication?

Yes, let $e \in \mathcal{F}(\mathbb{R})$ such that

$$e(x) = 1$$

for all $x \in \mathbb{R}$. Let $f \in \mathcal{F}(\mathbb{R})$ and let $a \in \mathbb{R}$. We see that

$$(fe)(a) = f(a)e(a) = f(a) \cdot 1 = f(a)$$

and

$$(ef)(a) = e(a)f(a) = 1 \cdot f(a) = f(a).$$

Therefore, e is the identity in $\mathcal{F}(\mathbb{R})$ under multiplication.

(c) Find an element in $\mathcal{F}(\mathbb{R})$ that does not have a multiplicative inverse in $\mathcal{F}(\mathbb{R})$. Explain how this shows $\mathcal{F}(\mathbb{R})$ is not a group under multiplication.

Let $f \in \mathcal{F}(\mathbb{R})$ such that

$$f(x) = 0$$

for all $x \in \mathbb{R}$. Let $g \in \mathcal{F}(\mathbb{R})$ and let $a \in \mathbb{R}$. We see that

$$(fg)(a) = 0 \cdot g(a) = 0 \neq 1.$$

And from this we can conclude that the function f defined as $f(x) = 0$ for all $x \in \mathbb{R}$ has no inverse. Because a group must have an inverse for every element and f is an element in $\mathcal{F}(\mathbb{R})$, $\mathcal{F}(\mathbb{R})$ is not a group under multiplication.

(d) Find necessary and sufficient conditions for an element in $\mathcal{F}(\mathbb{R})$ to be a unit in $\mathcal{F}(\mathbb{R})$. State your result in a lemma of the form “The function $f \in \mathcal{F}(\mathbb{R})$ is a unit in $\mathcal{F}(\mathbb{R})$ if and only if ...”. Your lemma must say something more than just a rehash of the definition of a unit; rather, it must actually characterize the functions that are invertible under multiplication in $\mathcal{F}(\mathbb{R})$.

Conjecture. An element in $\mathcal{F}(\mathbb{R})$ is a unit if and only if $f(x) \neq 0$ for all $x \in \mathbb{R}$.

First we will show that if f is a function in $\mathcal{F}(\mathbb{R})$ such that $f(x) \neq 0$ for all $x \in \mathbb{R}$, then f is a unit.

Proof. Let f be a function in $\mathcal{F}(\mathbb{R})$ such that $f(x) \neq 0$ for all $x \in \mathbb{R}$ and let $a \in \mathbb{R}$. Because the set $\mathbb{R} - \{0\}$ is a group under multiplication and $f(x)$ is in this group we know that there exists some g in $\mathcal{F}(\mathbb{R})$ such that $f(x)g(x) = 1$ and $g(x)f(x) = 1$. From this we see that f has an inverse in $\mathcal{F}(\mathbb{R})$. \square

Next we will show that if f is a unit, then it must be true that $f(x) \neq 0$ for all $x \in \mathbb{R}$.

Proof. We assume to the contrary that f is a unit in $\mathcal{F}(\mathbb{R})$ such that there exists some $a \in \mathbb{R}$ such that $f(a) = 0$. Because f is a unit, there must exist some g in $\mathcal{F}(\mathbb{R})$ such that $g(x)f(x) = 1$ for all $x \in \mathbb{R}$. This implies that there exists a real number $g(a)$ such that $g(a) \cdot 0 = 1$. This is a contradiction and so it must be necessary for $f(x) \neq 0$ for all $x \in \mathbb{R}$ in order for f to be a unit. \square

Activity 20.12. In this activity, we will explore a simple relationship between the order of a group element and the order of its inverse.

(a) Determine the order of $[2]$ in \mathbb{Z}_6 . What is the inverse of $[2]$ in \mathbb{Z}_6 ? Directly compute the order of the inverse of $[2]$ in \mathbb{Z}_6 . What do you notice?

First of all, we note that $\langle [2] \rangle = \{[0], [2], [4]\}$. The magnitude of this set is 3 and therefore the order of $[2]$ in \mathbb{Z}_6 is 3. The inverse of $[2]$ is $[4]$ ($[2] + [4] = [0]$).

The order of $[4]$ in \mathbb{Z}_6 is equal to the magnitude of $\langle [4] \rangle = \{[0], [2], [4]\}$, and so the order of $[4]$ is 3. The sets $\langle [2] \rangle$ and $\langle [4] \rangle$ are equal and therefore the orders $[2]$ and $[4]$ must be equal as well.

(b) Determine the order of $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ in the group D_4 of symmetries of a square. What is the inverse of α in D_4 ? Directly compute the order of the inverse of α in D_4 . What do you notice?

First of all, we note that

$$\langle \alpha \rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}.$$

From this we see that the magnitude of α is 4. The inverse of α is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

The cyclic group generated by α^{-1} is

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}.$$

Therefore the order of α^{-1} is 4. Again, this is equal to α .

(c) Based on your observations in parts (a) and (b), what relationship do you think exists between $|a|$ and $|a^{-1}|$ in a group G ?

The order of a is equal to the order of a^{-1} .

(d) Let G be a group with identity e , and let $a \in G$. Show that if $a^n = e$ for some positive integer n , then $(a^{-1})^n = e$.

Proof. Let G be a group with identity e and let $a \in G$ such that

$$a^n = e \tag{16}$$

for some positive integer n . Applying the definitions of an integer power of an element in a group we see that

$$(a^{-1})^n = a^{-1 \cdot n} = a^{-n} = (a^n)^{-1} \tag{17}$$

Now applying the transitive property of equality to (16) and (17) we obtain

$$(a^{-1})^n = e^{-1} = e.$$

In conclusion, we have shown that if G be a group with identity e and $a \in G$ such that $a^n = e$ for some positive integer n , then $(a^{-1})^n = e$. \square

(e) Let G be a group with identity e , and let a be an element of G with finite order. For this case, prove the relationship you conjectured between $|a|$ and $|a^{-1}|$ in part (c).

Conjecture. Let G be a group with identity e with element a of finite order. The order of a is equal to the order of a^{-1} .

Proof. We know that $\langle a \rangle$ contains e and so there must exist some positive integer n such that

$$a^n = e. \quad (18)$$

Let $S = \{x \in \mathbb{Z}^+ : a^x = e\}$. From (18) we know that S is not empty. Therefore, from the Axiom of Choice we are able to choose the a smallest element $k \in S$. The set $\{a, a^2, \dots, a^k\}$ is equal to the set $\langle a \rangle$ (it contains a and all of the elements up to e) and so the order of a is k . From part (d) we know that $(a^{-1})^k = e$ and so $|a^{-1}| \leq |a|$.

We also know that $\langle a^{-1} \rangle$ contains e and so there must exist some positive integer m such that

$$(a^{-1})^m = e. \quad (19)$$

Let $T = \{x \in \mathbb{Z}^+ : ((a)^{-1})^x = e\}$. From (19) we know that T is not empty. Therefore, from the Axiom of Choice we are able to choose the a smallest element $p \in T$. The set $\{a^{-1}, (a^{-1})^2, \dots, (a^{-1})^p\}$ is equal to the set $\langle a^{-1} \rangle$ (it contains a^{-1} and all of the elements up to e) and so the order of a^{-1} is p . From part (d) we know that $a^p = e$ and so $|a| \leq |a^{-1}|$.

In conclusion we have shown that the order of a is less than or equal to the order of a^{-1} and the order of a^{-1} is less than or equal to the order of a . Therefore, the order of a and the order of a^{-1} is equal. \square

(f) Let G be a group with identity e , and let $a \in G$. Prove that if a has infinite order, then a^{-1} has infinite order.

Proof. Assume to the contrary that a has infinite order, but a^{-1} does not. Because the order of a^{-1} is finite, there must exist some $n \in \mathbb{Z}^+$ such that

$$|a^{-1}| < n \quad (20)$$

The inverse of a^n is a^{-n} , but because the order of a^{-1} is less than n there must exist some $k < n$ such that $(a^{-1})^n = (a^{-1})^k$. But this would mean that $(a^{-1})^k$ has two unique inverses, a^k and a^n . This is a contradiction and so a^{-1} has infinite order. \square

(3) Let H denote the set of all 2×2 matrices of the form

$$\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}$$

where $x, y \in \mathbb{R}$. Is H a subgroup of $\mathcal{M}_{2 \times 2}(\mathbb{R})$?

Conjecture. The set H is a subgroup of $\mathcal{M}_{2 \times 2}(\mathbb{R})$.

Proof. First of all, the identity of $\mathcal{M}_{2 \times 2}(\mathbb{R})$ under addition is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and this is in H ($x = 0, y = 0$). Next, let $a, b, c, d \in \mathbb{R}$. Then $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ and $\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$ are both in H . When we add these two matrices together we get

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} + \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} a + c & 0 \\ b + d & 0 \end{bmatrix}.$$

Because the reals are closed under addition, we know that both $a + c$ and $b + d$ are in \mathbb{R} . Therefore, $\begin{bmatrix} a + c & 0 \\ b + d & 0 \end{bmatrix}$ is in H and from this we can conclude that H is closed under addition. Finally let $x, y \in \mathbb{R}$. The inverses of x and y are also in \mathbb{R} and so both $\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}$ and $\begin{bmatrix} -x & 0 \\ -y & 0 \end{bmatrix}$ are in H . We also see that

$$\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} + \begin{bmatrix} -x & 0 \\ -y & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

From this, we can conclude that every element in H has an inverse. In conclusion, we have shown that the subset H of $\mathcal{M}_{2 \times 2}(\mathbb{R})$ is closed under addition, the identity of $\mathcal{M}_{2 \times 2}(\mathbb{R})$ under addition is in H , and every element of H has an inverse. From this we have shown that H is a subgroup of $\mathcal{M}_{2 \times 2}(\mathbb{R})$ under addition. \square

(4) Let G be a group and H a subgroup of G . Which of the following conjectures do you think are true, and which do you think are false? Provide brief arguments or examples to justify your answers.

(a) If G is finite, then H is finite.

This statement is true due to the fact that H is a subset of G and therefore cannot have a magnitude greater than its superset G .

(b) If H is finite, then G is finite.

This is not necessarily true. For example, $\{0\}$ is a subgroup of \mathbb{Z} under addition. In this case H is finite, but G is infinite.

(c) If G is Abelian, then H is Abelian.

This is a property of the operator of G and therefore it will also be true for H whose elements are all in G .

(d) If H is Abelian, then G is Abelian.

This is not always true. For example, we have the group G containing the symmetries of a square with the subgroup H containing only its identity. In this case H is Abelian, but G is not.

(8) Intersections of subgroups. Let G be a group with subgroups H and K .

(a) Is $H \cap K$ a subgroup of G ? Prove your answer.

Conjecture. Let G be a group with subgroups H and K . Then $H \cap K$ is a subgroup of G .

Proof. Let G be a group with identity e and let H and K be subgroups of G . We know from the fact that H and K are subgroups of G that $e \in H$ and $e \in K$, and so $e \in H \cap K$. Next, let $a, b \in H \cap K$. From the definition of intersection of sets we know that $a, b \in H$ and $a, b \in K$. Because H and K are groups, $ab \in H$ and $ab \in K$. Therefore $ab \in H \cap K$, coming from the definition of intersection. From this we have shown that $H \cap K$ are closed under the operation of G . Finally, let $x \in H \cap K$. From the definition of intersection of sets we know that $x \in H$ and $x \in K$. Because H and K are groups, $x^{-1} \in H$ and $x^{-1} \in K$. Therefore $x^{-1} \in H \cap K$, coming from the definition of intersection of sets.

In conclusion, we have shown that the identity of G is in $H \cap K$, the set $H \cap K$ is closed under the operation of G , and each element in $H \cap K$ has an inverse in $H \cap K$. Therefore, $H \cap K$ is a subgroup of G . \square

(b) Can we generalize? That is, if H_α is a collection of subgroups of G indexed by α in an indexing set I , is it the case that $\cap_{\alpha \in I} H_\alpha$ is a subgroup of G ? Prove your answer.

Conjecture. Let H_α be a collection of subgroups of G indexed by α in an indexing set I . Then $\cap_{\alpha \in I} H_\alpha$ is a subgroup of G .

Proof. Let H be a subgroup of G in the collection H_α . We know that $e \in H$ from the fact that H is a subgroup of G . Because H is an arbitrary element in H_α we have shown that e is in every element of H_α . Therefore, from the definition of intersection of sets $e \in \cap_{\alpha \in I} H_\alpha$. Next let $a, b \in \cap_{\alpha \in I} H_\alpha$. From the definition of intersection we know that $a, b \in H$. Because H is a group, $ab \in H$. Again, H is an arbitrary element in H_α and so $ab \in \cap_{\alpha \in I} H_\alpha$. From this, we see that $\cap_{\alpha \in I} H_\alpha$ is closed under the operation of the group G . Finally, let $x \in \cap_{\alpha \in I} H_\alpha$. From the definition of intersection we know that $x \in H$. Because H is a group, $x^{-1} \in H$. And because H is an arbitrary element in H_α , $x^{-1} \in \cap_{\alpha \in I} H_\alpha$.

In conclusion, we have shown that $\cap_{\alpha \in I} H_\alpha$ contains the identity $e \in G$, it is closed under the operation of G , and each element in $\cap_{\alpha \in I} H_\alpha$ has an inverse. Therefore, $\cap_{\alpha \in I} H_\alpha$ is a subgroup of G . \square

(12) Determine whether H is a subgroup of G .

(a) $G = \mathbb{Z}_{20}$ under addition, $H = \{[0], [3], [6], [9], [12], [15], [18]\}$.

The inverse of $[3]$ is $[17]$ which is not in H . Therefore H is not a subgroup of G .

(b) $G = U_7$ under multiplication, $H = \{[1], [2], [4]\}$.

First of all, the identity $[1]$ is in H . Now we will construct an operation table to see if H is closed under multiplication and each element of H has an inverse.

\cdot	$[1]$	$[2]$	$[4]$
$[1]$	$[1]$	$[2]$	$[4]$
$[2]$	$[2]$	$[4]$	$[1]$
$[4]$	$[4]$	$[1]$	$[2]$

From this operation table we see that H is closed under multiplication and each element of H has an inverse. And so, we can conclude that H is a subgroup of G .

(c) $G = U_{16}$ and $H = \{[1], [7], [9], [15]\}$.

First of all, the identity $[1]$ is in H . Now we will construct an operation table to see if H is closed under multiplication and each element of H has

an inverse.

\cdot	$[1]$	$[7]$	$[9]$	$[15]$
$[1]$	$[1]$	$[7]$	$[9]$	$[15]$
$[7]$	$[7]$	$[1]$	$[15]$	$[9]$
$[9]$	$[9]$	$[15]$	$[1]$	$[7]$
$[15]$	$[15]$	$[9]$	$[7]$	$[1]$

From this operation table we see that H is closed under multiplication and each element of H has an inverse. And so, we can conclude that H is a subgroup of G .