

(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 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

$$((f + g) + h)(x) = (f(x) + g(x)) + h(x) \tag{1}$$

and

$$(f + (g + h))(x) = f(x) + (g(x) + h(x)) \tag{2}$$

We also know that

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

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

and

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

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

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

From 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 $f \in \mathcal{F}(\mathbb{R})$. We see that

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

and

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

In conclusion, we have shown that $(f + e)(x) = (e + f)(x) = f(x)$ for all $x \in \mathbb{R}$ and therefore e 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 $(f - f)(x) = f(x) - f(x) = 0$ coming from the fact that $f(x) \in \mathbb{R}$ and each element in \mathbb{R} has an inverse under addition. We know that for a We know that \mathbb{R} is a group under addition. Therefore each element in \mathbb{R} has an inverse Let $f \in \mathcal{F}(\mathbb{R})$ and let $g \in \mathcal{F}(\mathbb{R})$ such that \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

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

and

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

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 has no inverse.

(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 an 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 $x \in \mathbb{R}$. There exists some g in $\mathcal{F}(\mathbb{R})$ such that $(fg)(x) = (gf)(x) = 1$ for all $x \in \mathbb{R}$. Let $a \in \mathbb{R}$. Let g be a function in $\mathcal{F}(\mathbb{R})$ such that $f(a)g(a) = 1$. \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

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

There 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 (??) and (??) 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. Assume to the contrary that $|a| > |a^{-1}|$. We know that $\langle a \rangle$ contains e and so there must exist some positive integer n such that

$$a^n = e. \tag{18}$$

Let $S = \{x \in \mathbb{Z}^+ : a^x = e\}$. From (??) we now that S is not empty. Therefore from the Axiom of Choice we will choose k to be the From the Axiom of Choice we know that there must exist some least value $k \in S$. \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. □