Section 1.1

February 18, 2025

1 Exercise

(a) Is not associative since: $(a-a)-a=-a$ and $a-(a-a)=a$ i.e. $a \neq -a$.

(b) Is associative since:

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

(c) Is not associative since:

$$\begin{aligned} a \star (b \star c) &= \frac{a + \frac{b+c}{5}}{5} \\ &= \frac{\frac{5a}{5} + \frac{b+c}{5}}{5} \\ &= \frac{5a + b + c}{10} \\ &\neq \frac{a + b + 5c}{10} \\ &= \frac{\frac{a+b}{5} + \frac{5c}{5}}{5} \\ &= \frac{\frac{a+b}{5} + c}{5} \\ &= (a \star b) \star c \end{aligned}$$

(d) Is not associative since:

$$\begin{aligned}(a,b)\star((c,d)\star(e,f)) &= (a,b)\star(cf+de,df)\\ &= (a(cf+de)+bdf,bdf)\\ &= (acf+ade+bdf,bdf)\\ &= (acf+ade+bdf,bdf)\\ &\neq (adf+bcf+bde,bdf)\\ &= ((ad+bc)f+bde,bdf)\\ &= (ad+bc,bd)\star(e,f)\\ &= ((a,b)\star(c,d))\star(e,f)\end{aligned}$$

(e) Is not associative since:

$$\begin{aligned}a\star(b\star c) &= \frac{a}{\frac{b}{c}}\\ &= a\left(\frac{b}{c}\right)^{-1}\\ &= a\left(\frac{c}{b}\right)\\ &= \frac{ac}{b}\\ &\neq \frac{a}{bc}\\ &= \left(\frac{a}{b}\right)c^{-1}\\ &= \frac{\frac{a}{b}}{c}\\ &= a\star(b\star c)\end{aligned}$$

2 Exercise

(a) Is not commutative since $a-2a=-a\neq a=2a-a$.

(b) Is commutative since:

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

(c) Is commutative since:

$$\begin{aligned}a\star b &= \frac{a+b}{5}\\ &= \frac{b+a}{5}\\ &= b\star a\end{aligned}$$

(d) Is commutative since:

$$\begin{aligned}(a,b)\star(c,d) &= (ad+bc,bd)\\ &= (cb+ad,db)\\ &= (c,d)\star(a,b)\end{aligned}$$

(e) Is not commutative since $\frac{1}{2} \neq \frac{2}{1}$

3 Exercise

Proof. Let $\overline{a},\overline{b},\overline{c} \in \mathbb{Z}/n\mathbb{Z}$. Using $\overline{a}+\overline{b} = \overline{a+b}$ we can show that:

$$\begin{aligned}(\overline{a}+\overline{b})+\overline{c} &= \overline{a+b}+\overline{c}\\ &= \overline{a+b+c}\\ &= \overline{a}+\overline{b+c}\\ &= \overline{a}+(\overline{b}+\overline{c})\end{aligned}$$

□

4 Exercise

Proof. Let $\overline{a},\overline{b},\overline{c} \in \mathbb{Z}/n\mathbb{Z}$. Using $\overline{a}\cdot\overline{b} = \overline{a\cdot b}$ we can show that:

$$\begin{aligned}(\overline{a}\cdot\overline{b})\cdot\overline{c} &= \overline{a\cdot b}\cdot\overline{c}\\ &= \overline{a\cdot b\cdot c}\\ &= \overline{a}\cdot\overline{b\cdot c}\\ &= \overline{a}\cdot(\overline{b}\cdot\overline{c})\end{aligned}$$

□

5 Exercise

Proof. We wish to show that $(\mathbb{Z}/n\mathbb{Z},\cdot)$ for any $n > 1$ is not a group. For $(\mathbb{Z}/n\mathbb{Z},\cdot)$ to be a group then there must exists an inverse $\overline{a}$ such that $\overline{a}\cdot\overline{0} = \overline{1}$. If we take the representative of $\overline{a}$ to be a and the representative of $\overline{0}$ to be 0 then we get $a\cdot 0 = 0$ for any a so $\overline{a}\cdot\overline{0} = \overline{0}$. Hence no inverse exists of $\overline{0}$ and therefore $(\mathbb{Z}/n\mathbb{Z},\cdot)$ is not a group. □

6 Exercise

(a) It is easy to see that the inverse $\frac{-a}{2b+1}$ and identity 0 exisist. Addition is also associative so remaining concern is if + always results in an element with an uneven denominator.

$$\begin{aligned}\frac{a}{2b+1}+\frac{c}{2d+1} &= \frac{a(2d+1)+c(2b+1)}{(2b+1)(2d+1)}\\ &= \frac{a(2d+1)+c(2b+1)}{4bd+2b+2d+1}\\ &= \frac{a(2d+1)+c(2b+1)}{2(2bd+b+d)+1}\end{aligned}$$

The denominator is always uneven so the set is closed under addition.

(b) Once again we only need to show the denominator is even.

$$\frac{a}{2b}+\frac{c}{2d}=\frac{a2d+c2b}{2(b2d)}$$

The denominator is always even so the set is closed under addition.

(c) This is not a valid group since $\frac{1}{2}$ is an element in the set but $\frac{1}{2}+\frac{1}{2}=\frac{1}{1}$ is too large to be in set, hence the set is not closed under addition.

(d) This is not a valid group since both 2 and $\frac{-2}{3}$ are members but $2+\frac{-2}{3}=\frac{1}{2}$ is too small to be an element in the set, hence the set is not closed under addition.

(e) Clearly an inverse always exists $\frac{-a}{1}$ or $\frac{-a}{2}$ and we have the identity 0 and an associative operation. It remains to show that the set is closed under addition.

$$\begin{aligned}\frac{a}{1}+\frac{b}{1}&=\frac{a+b}{1}\\ \frac{a}{2}+\frac{b}{2}&=\frac{a+b}{2}\\ \frac{a}{2}+\frac{b}{1}&=\frac{a+2b}{2}\end{aligned}$$

As one can see it is closed under addition.

(f) First we observe that $\frac{1}{2}+\frac{1}{3}=\frac{5}{6}$, since there does no exist a number which both divide 5 and 6 then the fraction can not be simplied and we have an element which can does not belong to the original set. Meaning this set is not closed under addition and therefore not an group.

7 Exercise

Proof. By definition we have that G must be closed under $\star$ since we always remove the integral part leading to $0 \leq x \star y < 1$.

Now we wish to show that the operation is associative, first we realize:

$$[x - [y]] = [x] - [y]$$

This holds since $[y]$ is already an integer so we can subtract it later. Now we can derive the following and show it is associative:

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

We have an identity 0 since:

$$x \star 0 = x + 0 - [x + 0] = x - [x] = 0 + x - [0 + x] = 0 \star x$$

And we have an inverse $-x$ since:

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

Hence $(G, \star)$ must be a group. □

8 Exercise

(a) *Proof.* First it must be shown that $(G, \cdot)$ is closed under multiplciation. Given $z, w \in G$ then it must hold for some $n, m \in \mathbb{Z}^+$ that $(z^n)^x \cdot (w^m)^y =$

1 for all $x, y \in \mathbb{R}$. Since $z^n = w^m = 1$ and $1^x = 1$ for all $x \in \mathbb{R}$ we can derive:

$$\begin{aligned} 1 &= (z^n)^m \cdot (w^m)^n \\ &= z^{mn} \cdot w^{mn} \\ &= (zw)^{nm} \end{aligned}$$

Hence G is closed under multiplciation since $(zw)^{nm} = 1$, therefore $zw \in G$. Lastly $(G, \cdot)$ is a group since $1 \in G$ is the identity. The inverse to z is z^{n-1} since $z \cdot z^{n-1} = z^n = 1$ for some $n \in \mathbb{Z}^+$ and $z^{n-1} \in G$ because $(z^{n-1})^n = z^{n \cdot n - n} = \frac{z^{n \cdot n}}{z^n} = z^{n \cdot n} = (z^n)^n = 1$. And multiplication is associative. □

(b) *Proof.* $(G, +)$ is not a group since $1 \in G$ but $1 + 1 = 2 \notin G$ since there exists no $n \in \mathbb{Z}^+$ such that $2^n = 1$ hence G is not closed under addition and therefore not a group. □

9 Exercise

(a) *Proof.* $(G, +)$ is closed under addition since given $a + b\sqrt{2}, c + d\sqrt{2} \in G$ then:

$$a + b\sqrt{2} + c + d\sqrt{2} = (a + c) + (b + d)\sqrt{2} \in G$$

$(G, +)$ is also a group since since 0 is the identity, the inverse to $a + b\sqrt{2}$ is $(-a) + (-b\sqrt{2})$, and addition is associative. □

(b) *Proof.* $(G, \cdot)$ is closed under addition since given $a + b\sqrt{2}, c + d\sqrt{2} \in G$ then:

$$\begin{aligned} (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= c(a + b\sqrt{2}) + d\sqrt{2}(a + b\sqrt{2}) \\ &= ca + cb\sqrt{2} + ad\sqrt{2} + db(\sqrt{2})^2 \\ &= (ca + db2) + (cb + ad)\sqrt{2} \in G \end{aligned}$$

$(G, \cdot)$ is also a group since since 1 is the identity, the inverse to $a + b\sqrt{2}$ is

$\frac{1}{a+b\sqrt{2}}$ which is in G since:

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

And addition is associative. □

10 Exercise

Proof. Let $(G,+)$ be an abelian group then for elements $g_i, g_j \in G$ where $i,j \in \mathbb{Z}^+$ are the indices in the group table M. Since $(G,+)$ is an abelian group then:

$$g_i + g_j = g_j + g_i$$

So it must hold that $M_{ij} = M_{ji}$ henece M is symmetric.

Let the group table M be an symmetric matrix i.e. $M_{ij} = M_{ji}$ then it must hold that $g_i + g_j = g_j + g_i$, hence $(G,+)$ is an abelian group. □

11 Exercise

$$\overline{0}^{1} = 0; |\overline{0}| = 1$$
$$\overline{1}^{1}2 = 0; |\overline{1}| = 12$$
$$\overline{2}^{6} = 0; |\overline{2}| = 6$$
$$\overline{3}^{4} = 0; |\overline{3}| = 4$$
$$\overline{4}^{3} = 0; |\overline{4}| = 3$$
$$\overline{5}^{12} = 0; |\overline{5}| = 12$$
$$\overline{6}^{2} = 0; |\overline{6}| = 2$$
$$\overline{7}^{12} = 0; |\overline{7}| = 12$$
$$\overline{8}^{3} = 0; |\overline{8}| = 3$$
$$\overline{9}^{4} = 0; |\overline{9}| = 4$$
$$\overline{10}^{6} = 0; |\overline{10}| = 6$$
$$\overline{11}^{12} = 0; |\overline{11}| = 12$$

12 Exercise

$$\overline{1}^{1} = 1; |\overline{1}| = 1$$
$$\overline{-1}^{2} = \overline{11}^{2} = 1; |\overline{-1}| = 2$$
$$\overline{5}^{2} = 1; |\overline{5}| = 2$$
$$\overline{-7}^{2} = \overline{5}^{2} = 1; |\overline{-7}| = 2$$
$$\overline{13}^{1} = \overline{1}^{1} = 1; |\overline{13}| = 2$$

13 Exercise

$$\overline{1}^{36} = 0; |\overline{1}| = 36$$
$$\overline{2}^{18} = 0; |\overline{2}| = 18$$
$$\overline{6}^{6} = 0; |\overline{6}| = 6$$
$$\overline{9}^{4} = 0; |\overline{9}| = 4$$
$$\overline{10}^{18} = 0; |\overline{10}| = 18$$
$$\overline{12}^{3} = 0; |\overline{12}| = 3$$
$$\overline{-1}^{36} = 0; |\overline{-1}| = 36$$
$$\overline{-10}^{18} = 0; |\overline{-10}| = 18$$
$$\overline{-18}^{2} = 0; |\overline{-18}| = 2$$

14 Exercise

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

15 Exercise

Proof. Let $P(n) : (a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$, we wish to show this predicate holds for $2 \leq n$ by induction. By Proposition 1. we have the base case $P(2) : (a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$. Now assume $P(n)$ holds, we can then show taht $P(n+1)$ holds by Proposition 1:

$$\begin{gathered}(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1} \\ \iff \\ a_{n+1}^{-1}(a_1 a_2 \cdots a_n)^{-1} = a_{n+1}^{-1} a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1} \\ \iff \\ (a_1 a_2 \cdots a_n a_{n+1})^{-1} = a_{n+1}^{-1} a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}\end{gathered}$$

□

16 Exercise

Proof. First we wish to show given $x^2 = 1$ then $|x| = 1$ or $|x| = 2$ exists, by $x^2 = 1$ we have:

$$x^2 = 1 \iff x = x^{-1}$$

So x is its own inverse and either $x = 1$ or $x \neq 1$. The first case exists for any group $1 \cdot 1 = 1$ and we have $|x| = 1$. The second case exists since there exists a group $(\mathbb{Z}/4\mathbb{Z}, +)$ where $\overline{2} + \overline{2} = \overline{0}$ so we have $|x| = 2$.

Let $x^2 = 1$ then it must hold that $|x| \leq 2$ and if $x^n = 1$ for $n > 2$ then $|x| \leq 2$ since 1 or 2 is smaller than n.

Let $|x| \leq 2$ then $x^n = 1$ for $1 \leq n \leq 2$, if $x^1 = 1$ then $x = 1$ and $x^2 = 1$ holds, so $x^2 = 1$ holds for any $|x| \leq 2$. So the biimplication holds in both directions. □

17 Exercise

Proof. Let $|x| = n$ for some $n > 1$ then:

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

□

18 Exercise

Proof. Let $xy = yx$ then:

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

□

19 Exercise

(a) *Proof.* Let P be the predicate $P(b) : x^a x^b = x^{a+b}$ where $a, b \in \mathbb{Z}^+$. We wish to show this holds forall $b \in \mathbb{Z}^+$. The base case holds since for $b = 1$ then $x^a x = x^{a+1}$. Given $P(b)$ we can now show $P(b+1)$ holds.

$$\begin{aligned} x^a x^b = x^{a+b} &\iff x^a x^b x = x^{a+b} x \\ &\iff x^a x^{b+1} = x^{a+(b+1)} \end{aligned}$$

□

Proof. Let P be the predicate $P(b) : (x^a)^b = x^{ab}$ where $a, b \in \mathbb{Z}^+$. We wish to show this holds forall $b \in \mathbb{Z}^+$. The base case holds since for $b = 1$ then $(x^a)^1 = x^a$. Given $P(b)$ we can now show $P(b+1)$ holds.

$$\begin{aligned}(x^a)^b = x^{ab} &\iff (x^a)^b x^a = x^{ab} x^a \\ &\iff (x^a)^{b+1} = x^{a(b+1)} \quad \text{(Holds by previous proof)}\end{aligned}$$

□

(b) *Proof.* Let P be the predicate $P(a) : (x^a)^{-1} = x^{-a}$ where $a \in \mathbb{Z}^+$. We wish to show this holds forall $a \in \mathbb{Z}^+$. The base case holds since for $a = 1$ then $(x^1)^{-1} = x^{-1}$. Given $P(a)$ we can now show $P(a+1)$ holds.

$$\begin{aligned}(x^a)^{-1} = x^{-a} &\iff (x^a)^{-1} x^{-1} = x^{-a} x^{-1} \\ &\iff (xx^a)^{-1} = x^{-(a+1)} \quad \text{(By Prop 2. and def. of } x^{-a}\text{)} \\ &\iff (x^{a+1})^{-1} = x^{-(a+1)}\end{aligned}$$

□

(c) *Proof.* Let $a, b \in \mathbb{Z}^+$. □