

Dummit & Foote Ch. 1: Groups

Scott Donaldson

2022

1. (11/14/22)

Let G be a group. Determine which of the following binary operations are associative:

- a) The operation \star on \mathbb{Z} defined by $a \star b = a - b$:
Not associative. $3 \star (2 \star 1) = 3 - 1 = 2$ but $(3 \star 2) \star 1 = 3 - 2 = 1$.
- b) The operation \star on \mathbb{R} defined by $a \star b = a + b + ab$:
Associative.
$$a \star (b \star c) = a \star (b + c + bc) = a + b + c + bc + ab + ac + abc = (a + b + ab) \star c = (a \star b) \star c$$
- c) The operation \star on \mathbb{Q} defined by $a \star b = \frac{a+b}{5}$:
Not associative. $0 \star (1 \star 1) = 0 + 2/5 = 2/5$ but $(0 \star 1) \star 1 = 1/5 \star 1 = 6/5 \star 1/5 = 6/25$.
- d) The operation \star on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$:
Associative.
$$\begin{aligned} ((a, b) \star (c, d)) \star (e, f) &= (ad + bc, bd) \star (e, f) = \\ (adf + bcf + bde, bdf) &= (a, b) \star (cf + de, df) = (a, b) \star ((c, d) \star (e, f)). \end{aligned}$$
- e) The operation \star on $\mathbb{Q} - \{0\}$ defined by $a \star b = a/b$:
Not associative. $(1 \star 2) \star 3 = 1/6$ but $1 \star (2 \star 3) = 3/2$.

2. (11/14/22)

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

- a) Not commutative. $1 - 2 = -1$ but $2 - 1 = 1$.
- b) Commutative. $a \star b = a + b + ab = b + a + ba = b \star a$.
- c) Commutative. $a \star b = \frac{a+b}{5} = \frac{b+a}{5} = b \star a$.
- d) Commutative. $(a, b) \star (c, d) = (ad + bc, bd) = (cb + da, db) = (c, d) \star (a, b)$.
- e) Not commutative. $1/2 \neq 2/1$ but $2/1 = 2$.

3. (11/16/22)

Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative.

Proof. First, we will show that subtraction in $\mathbb{Z}/n\mathbb{Z}$ is well-defined. Given a representative element \bar{a} , $1 \leq \bar{a} \leq n-1$, the element $n - \bar{a}$ is \bar{a} 's inverse. $1 \leq n - \bar{a} \leq n-1$, so $n - \bar{a}$ is also a representative element. Also, $\bar{a} + (n - \bar{a}) = n \sim 0$. Thus, subtracting an element \bar{a} from \bar{b} is the same as adding $n - \bar{a}$ to \bar{b} , and so subtraction is well-defined.

Now, to show that addition is associative, let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$. Suppose that $(\bar{a} + \bar{b}) + \bar{c} = \bar{d}$ and $\bar{a} + (\bar{b} + \bar{c}) = \bar{e}$. Then:

$$\bar{d} - \bar{c} = \bar{a} + \bar{b} \Rightarrow \bar{a} = (\bar{d} - \bar{c}) - \bar{b}$$

And:

$$\bar{e} - \bar{a} = \bar{b} + \bar{c} \Rightarrow \bar{e} = ((\bar{d} - \bar{c}) - \bar{b}) + \bar{b} + \bar{c} = \bar{d} - \bar{c} + \bar{c} = \bar{d}$$

Therefore $\bar{d} = \bar{e}$, so $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$. □

4. (11/16/22)

Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative.

Proof. Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$. Then:

$$\overline{\bar{a}(\bar{b}\bar{c})} = \overline{\bar{a}(\overline{bc})} = \overline{a(bc)}$$

Since the latter expression involves arbitrary integers a, b, c whose representative elements in $\mathbb{Z}/n\mathbb{Z}$ are $\bar{a}, \bar{b}, \bar{c}$, we can use the associative property of standard multiplication:

$$\overline{a(bc)} = \overline{(ab)c} = (\overline{ab})\bar{c} = (\overline{ab})\bar{c}$$

Therefore multiplication of residue classes is associative. □

5. (11/16/22)

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

Proof. Let $\mathbb{Z}/n\mathbb{Z}$ with $n > 1$. The element 1 is the identity element, since (by multiplication of standard integers), $1 \cdot \bar{a} = \bar{a}$ for all $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. However, the element 0 has no inverse, since (again by standard multiplication), there is no element \bar{a} such that $0 \cdot \bar{a} = 1$. Thus, $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication. □

6. (11/18/22)

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

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

This is a group. The identity element is 0 and addition is associative by definition, so we only need to show that it is closed. Let $\frac{a}{b}$ and $\frac{c}{d}$ be two elements of the set. Then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. The product of two odd numbers is odd, so bd is odd. Further, if $\frac{ad+bc}{bd}$ is not in lowest terms, then the denominator must remain negative, since an odd number has no even divisors. Thus the set is closed under addition.

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

Not a group. $1/2 + 1/2 = 1/1$, a rational number whose denominator is odd.

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

Not a group. $3/4 + 3/4 = 3/2$, a rational number whose absolute value is ≥ 1 .

- d) the set of rational numbers of absolute value ≥ 1 together with 0.

Not a group. $3/2 + (-3/4) = 1/4$, a rational number whose absolute value is < 1 .

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

This is a group. Let a, b be members of the set. If both have denominator 1 or 2, then their sum has denominator 1. Otherwise, if one has denominator 1 and the other denominator 2, their sum has denominator 2. Therefore the set is closed under addition.

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

Not a group. $1/2 + 1/3 = 5/6$.

7. (11/xx/22)

Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$. Prove that \star is a well-defined binary operation on G and that G is an abelian group under \star .

Proof. \star is a well-defined binary operation on G . Let $x, y \in G$. Then $x, y \in [0, 1)$. Suppose that $x + y = z \in \mathbb{R}$. By definition, $x \star y$ is the fractional part of z , which is unique. Therefore \star is well-defined, and commutative, since $+$ is commutative.

The identity element of G is 0, since for all $x \in [0, 1)$, $0 + x = x$.

G is closed under \star . For any $z = x + y$, the fractional part of z is (by definition) greater than or equal to 0 and strictly less than 1. Therefore $x \star y$ is in G .

Finally, \star is associative. Let $a, b, c \in G$. $(a \star b) \star c$ is equal to the fractional part of $(a \star b) + c$. And, $a \star b$ is equal to the fractional part of $a + b$. Now, taking the fractional part of a number is an idempotent operation; that is, performing it more than once yields the same value. So the fractional part of $(a \star b) + c$, that is, the fractional part of the fractional part of $(a + b) + c$ is just the fractional part of $(a + b) + c = a + b + c$. Similarly, $a \star (b \star c)$ is equal to the fractional part of $a + b + c$, and so \star is associative.

Thus G is an abelian group under \star . □