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 $(0 \star 1) \star 1 = 1/5 \star 1 = 6/5 * 1/5 = 6/25$.

d) The operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$:

   Associative.

   $$((a, b) \star (c, d)) \star (e, f) = (ad + bc, bd) \star (e, f) =$$
   $$(adf + bcf + bde, bdf) = (a, b) \star (cf + de, df) = (a, b) \star ((c, d) \star (e, f)).$$

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. $1/2 = 1/2$ 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:

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

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

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

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. Each element a has an inverse in $-a = -1 \cdot a$. It remains to be shown that the set is closed under addition. 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. Identity, associativity, and inverses are trivial. 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. (11/18/22)

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 $\star$ (called the *real numbers mod 1*).

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 $x \in [0, 1)$, $0 + x = x$.

For all $x \in G$, x has an inverse $1 - x \in G$, since $x + (1 - x) = 1$, and so $x \star (1 - x) = 0$.

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 $\star$. □

8. (11/18/22)

Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that G is a group under multiplication (called the *roots of unity*) but not under addition.

Proof. 1 is the identity element of G. $1^1 = 1$, so $1 \in G$, and by definition $1 \cdot z = z$ for all $z \in \mathbb{C}$. Multiplication is by definition associative, so it remains to be shown that elements in G have inverses and that G is closed under multiplication.

Let $z \in G$ (to show elements have inverses). Then $z^n = 1$ for some $n \in \mathbb{Z}^+$. Since $1/1 = 1$, we also have $1/(z^n) = 1$. It follows that $(1/z)^n = 1$, and so $1/z \in G$. $z \cdot 1/z = 1$, and therefore z has an inverse $1/z$.

Let $a, b \in G$ (to show that G is closed under multiplication). It follows that $a^n = 1$ and $b^m = 1$ for some $n, m \in \mathbb{Z}^+$. Then $1 = a^n b^m = (ab)^{nm}$. The product of ab raised to the nm power is 1, so it is an element of G, and thus G is closed under addition.

G is not a group under addition. Both 1 and the imaginary number i are elements of G, but their sum $1 + i$ is not. Consider the modulus of a complex number $z = x + iy$, $\sqrt{x^2 + y^2}$. The modulus of $1 + i$ is $\sqrt{2}$. The modulus of the product of two complex numbers is equal to the product of the modulus of each number (proof omitted). The modulus of $(1 + i)^2$ is $\sqrt{2} \cdot \sqrt{2} = 2$. The modulus of $(1 + i)^3$ is then $2\sqrt{2}$. For each successive n, then, the modulus of $(1 + i)^n$ is strictly increasing. However, the modulus of $1 \in \mathbb{C}$ is 1, so $(1 + i)^n$ is never 1, and therefore $1 + i$ is not in G. □

9. (11/19/22)

Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Prove that G is a group under addition and that the nonzero elements of G are a group under multiplication.

Proof. For addition, let $0 = 0 + 0\sqrt{2}$ be the identity element and note that addition is by definition is associative. The inverse of $a+b\sqrt{2}$ is simply $-a-b\sqrt{2}$. To show that G is closed, let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be elements of G. Then $a + b\sqrt{2} + c + d\sqrt{2} = (a + c) + (b + d)\sqrt{2}$. Since the rational numbers are closed under addition, $a + c, b + d \in \mathbb{Q}$ and so G is closed under addition. Thus G is a group under addition.

Next consider the set $G - \{0\}$ under multiplication. $1 = 1 + 0\sqrt{2}$ is the identity element and multiplication is by definition associative. The inverse of $a + b\sqrt{2}$ is:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = (\frac{a}{a^2 - 2b^2}) - (\frac{b}{a^2 - 2b^2})\sqrt{2}$$

The expressions inside the parentheticals are rational numbers, so elements in $G - \{0\}$ have inverses that are in G (note that the denominator $a^2 - 2b^2$ is only 0 when $a = b\sqrt{2}$; however, this is impossible, as $a \notin \mathbb{Q}$).

To show that $G - \{0\}$ is closed, let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be elements of $G - \{0\}$. Then

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}$$

Therefore $G - \{0\}$ is closed under multiplication, and is thus a group under multiplication.

□

10. (11/20/22)

Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

Proof. Let G be a finite group with elements $\{g_1, g_2, ..., g_n\}, g_1 = 1$ and let A be its group table, a matrix with the i, j-th entry equal to $g_i g_j$.

First, suppose that G is an abelian group. So for all $g_i, g_j \in G$, $g_i g_j = g_j g_i$. Then the i, j-th entry, $g_i g_j$, is equal to the j, i-th entry, $g_j g_i$. Thus A is symmetric.

Next, suppose that A is a symmetric matrix. Then the i, j-th entry is equal to the j, i-th entry, that is, $g_i g_j = g_j g_i$. Since all possible combinations of elements of G commute with each other, G is thus an abelian group. □

11. (11/20/22)

Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

* $\bar{0}$: 1.
* $\bar{1}$: 12.
* $\bar{2}$: 6.
* $\bar{3}$: 4.
* $\bar{4}$: 3.
* $\bar{5}$: 12.
* $\bar{6}$: 2.
* For each subsequent element $\bar{a}$, the order is the same as that of its inverse (listed above), $12 - \bar{a}$.

12. (11/20/22)

Find the orders of the following elements of the multiplicative group $\left(\mathbb{Z}/12\mathbb{Z}\right)^{\times}$.

* $\overline{1}$: 1.
* $\overline{-1}$: $-1 \times -1 = 1$. Order 2.
* $\overline{5}$: $5 \times 5 = 25 \sim 1$. Order 2.
* $\overline{7}$: $7 \times 7 = 49 \sim 1$. Order 2.
* $\overline{-7}$: $-7\ 5$. Order 2.
* $\overline{13}$: $13 \sim 1$. Order 1.

13. (11/20/22)

Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$.

* $\overline{1}$: 36.
* $\overline{2}$: 18.
* $\overline{6}$: 6.
* $\overline{9}$: 4.
* $\overline{10}$: 18.

* $\overline{12}$: 3.
* $\overline{-1}$: 36.
* $\overline{-10}$: 18.
* $\overline{-18}$: 2.

14. (11/30/22)

Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^{\times}$.

* $\overline{1}$: 1.
* $\overline{-1}$: 2.
* $\overline{5}$: 6.
* $\overline{13}$: 3.
* $\overline{-13}$: 6.
* $\overline{17}$: 2.

15. (11/30/22)

Prove that $(a_1 a_2 ... a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_1^{-1}$ for all $a_1, a_2, ..., a_n \in G$.

Proof. Let $a_1 a_2 ... a_n = b$. Then $a_1 a_2 ... a_{n-1} = b a_n^{-1}$. We can continue multiplying by the inverse of each right-most element until $1 = b a_n^{-1} a_{n-1}^{-1} ... a_2^{-1} a_1^{-1}$. Then $b^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_2^{-1} a_1^{-1}$, and so $(a_1 a_2 ... a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_1^{-1}$. □

16. (12/20/22)

Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

Proof. First, suppose that $|x|$ is 1. Then $x = 1$, so $x^2 = 1 \cdot 1 = 1$. If $|x|$ is 2, then by definition $x^2 = 1$. So if $|x|$ is either 1 or 2, then $x^2 = 1$.

Next, suppose that $x^2 = 1$. By definition, the order of x cannot be greater than 2, so it must be either 1 or 2. □

17. (12/19/22)

Let $x \in G$ with $|x| = n$, $n \in \mathbb{Z}^+$. Prove that $x^{-1} = x^{n-1}$.

Proof. Let $x \in G$ with $|x| = n$. So $x^n = 1$.

Multiply both sides by x^{-1} to obtain $x^n x^{-1} = x^{-1}$. Thus $x^{n-1} = x^{-1}$. □

18. (12/20/22)

Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

Proof. First, to prove that $xy = yx$ implies that $y^{-1}xy = x$, let $xy = yx$ and left-multiply both sides by y^{-1}. Then $y^{-1}xy = y^{-1}yx = x$.

Next, to prove that $y^{-1}xy = x$ implies that $x^{-1}y^{-1}xy = 1$, let $y^{-1}xy = x$ and left-multiply both sides by x^{-1}. Then $x^{-1}y^{-1}xy = x^{-1}x = 1$.

Finally, to prove that $x^{-1}y^{-1}xy = 1$ implies that $xy = yx$, let $x^{-1}y^{-1}xy = 1$ and left-multiply both sides by x, then y. Then $xy = yx$. □

19. (12/29/22)

Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.

a) Prove that $x^a x^b = x^{a+b}$ and $(x^a)^b = x^{ab}$.
$x^a x^b = \underbrace{x \cdot \ldots \cdot x}_{a \text{ times}} \cdot \underbrace{x \cdot \ldots \cdot x}_{b \text{ times}} = \underbrace{x \cdot \ldots \cdot x}_{a+b \text{ times}} = x^{a+b}$.
Similarly, $(x^a)^b = \underbrace{x^a \cdot \ldots \cdot x^a}_{b \text{ times}} = \underbrace{\underbrace{x \cdot \ldots \cdot x}_{a \text{ times}} \cdot \ldots \cdot \underbrace{x \cdot \ldots \cdot x}_{a \text{ times}}}_{b \text{ times}} = \underbrace{x \cdot \ldots \cdot x}_{ab \text{ times}} = x^{ab}$.

b) Prove that $(x^a)^{-1} = x^{-a}$.
Let $x^a = b$. Right-multiply this equation by x^{-1} to obtain $x^a x^{-1} = x^{a-1} = bx^{-1}$. Continue doing this until we obtain $1 = b\underbrace{x^{-1} \cdot \ldots \cdot x^{-1}}_{a \text{ times}}$, that is, $1 = bx^{-a}$. Then, left-multiply by b^{-1} to obtain $b^{-1} = x^{-a}$. Since $b = x^a$, $(x^a)^{-1} = x^{-a}$.

c) Establish part a) for arbitrary integers a and b.
In the case where either a or b is 0, the equalities hold because for any $x \in G$, by definition $x^0 = 1$, and so $x^a x^0 = x^a \cdot 1 = x^a = x^{a+0}$ and $(x^a)^0 = 1 = x^0 = x^{a \cdot 0}$ (also, $(x^0)^a = 1 = x^0 = x^{0 \cdot a}$).

Next, consider $x^a x^b$ with both exponents negative, written differently, $x^{-a}x^{-b}$. From part b), this is equal to $(x^a)^{-1}(x^b)^{-1} = (x^b x^a)^{-1} = (x^{a+b})^{-1} = x^{-a-b}$, as desired. If a and b have different signs, that is, $x^a x^{-b}$, we have $x^a(x^{-1})^b = \underbrace{x \cdot \ldots \cdot x}_{a \text{ times}} \cdot \underbrace{x^{-1} \cdot \ldots \cdot x^{-1}}_{b \text{ times}}$. Each pair of $x \cdot x^{-1}$ reduces to the identity, leaving us with (in the case where $a > -b$) x^{a-b}, or (if $a < -b$), $(x^{-1})^{b-a} = x^{a-b}$, as desired.

Finally, consider $(x^a)^{-b}$. From part b), this is equal to $((x^a)^b)^{-1} = (x^{ab})^{-1} = x^{-ab}$. Similarly, $(x^{-a})^b = ((x^{-1})^a)^b = (x^{-1})^{ab} = x^{-ab}$. And, if both a and b are negative, then:

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

20. (12/29/22)

For an element $x \in G$, show that x and x^{-1} have the same order.

Proof. Let $x \in G$. Suppose that $|x| = n$. Then $x^n = 1$. Multiply both sides of this equation by x^{-n} to obtain $x^n x^{-n} = x^{n-n} = x^0 = 1$ on the left, and $x^{-n} = (x^{-1})^n$ on the right. Thus the order of x^{-1} is at most n. However, if its order were any natural number m less than n, then we would have
$(x^{-1})^m = 1 \Rightarrow 1 = x^m$, contradicting $|x| = n$. The same logic shows that if x has infinite order, x^{-1} cannot have finite order and vice-versa. Thus x and x^{-1} must have the same order. $\square$

21. (12/31/22)

Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

Proof. Let $x \in G$ with $|x| = 2k - 1$ for some $k \in \mathbb{N}$. Then $x^{2k-1} = 1$, which implies that $x^{2k}x^{-1} = 1$. Right-multiplying both sides of the equation by x, we have $x^{2k} = x$, so $x = (x^2)^k$, as desired. $\square$