

Dummit & Foote Ch. 1: Groups

Scott Donaldson

Nov. 2022 - Jan. 2023

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. $1/2 = 1/2$ 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:

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

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:

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

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. \square

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 multiplication.

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 . \square

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 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:

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

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. \square

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 $\{g_1, g_2, \dots, g_n\}$, $g_1 = 1$ 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. \square

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 $(\mathbb{Z}/12\mathbb{Z})^\times$.

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

13. (11/20/22)

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

- * $\bar{1}$: 36.
- * $\bar{2}$: 18.
- * $\bar{6}$: 6.
- * $\bar{9}$: 4.
- * $\bar{10}$: 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 $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$ for all $a_1, a_2, \dots, a_n \in G$.

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

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. \square

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 $x^{n-1} = x^{-1}$. \square

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 $xy = yx$. \square

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

$$x^a x^b = \underbrace{x \cdot \dots \cdot x}_{a \text{ times}} \cdot \underbrace{x \cdot \dots \cdot x}_{b \text{ times}} = \underbrace{x \cdot \dots \cdot x}_{a+b \text{ times}} = x^{a+b}.$$

$$\text{Similarly, } (x^a)^b = \underbrace{x^a \cdot \dots \cdot x^a}_{b \text{ times}} = \underbrace{\underbrace{x \cdot \dots \cdot x}_{a \text{ times}} \cdot \dots \cdot \underbrace{x \cdot \dots \cdot x}_{a \text{ times}}}_{b \text{ times}} = \underbrace{x \cdot \dots \cdot x}_{ab \text{ times}} = x^{ab}.$$

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

Let $x^a = b$. Right-multiply this equation by x^{-1} to obtain $x^a x^{-1} = b x^{-1}$. Continue doing this until we obtain $1 = b \underbrace{x^{-1} \cdot \dots \cdot x^{-1}}_{a \text{ times}}$,

that is, $1 = b x^{-a}$. 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 $x^a (x^{-1})^b = \underbrace{x \cdot \dots \cdot x}_{a \text{ times}} \cdot \underbrace{x^{-1} \cdot \dots \cdot x^{-1}}_{b \text{ times}}$. 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. (12/30/22)

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

22. (12/31/22)

If x and g are elements of the group G , prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Proof. First, we will prove a useful lemma, that $(g^{-1}xg)^n = g^{-1}x^n g$.

$$(g^{-1}xg)^n = \underbrace{(g^{-1}xg) \dots (g^{-1}xg)}_{n \text{ times}} = g^{-1} \underbrace{(xgg^{-1}) \dots (xgg^{-1})}_{n-1 \text{ times}} xg = g^{-1}x^{n-1}xg = g^{-1}x^n g.$$

Now if $|x|$ is infinite, then there is no $n \in \mathbb{Z}^+$ such that $x^n = 1$. Suppose toward contradiction that $|g^{-1}xg| = n$. Then we have $(g^{-1}xg)^n = 1 \Rightarrow g^{-1}x^n g = 1$. We can left-multiply by g and then right-multiply by g^{-1} to obtain $x^n = gg^{-1} = 1$, contradicting x having infinite order. Therefore $|g^{-1}xg|$ is also infinite.

Suppose then that $|x| = n$, $n \in \mathbb{Z}^+$. So $x^n = 1$. Left-multiply by g^{-1} and then right-multiply by g to obtain $g^{-1}x^n g = g^{-1}g = 1$. From the above lemma, then, we have $(g^{-1}xg)^n = 1$. So the order of $g^{-1}xg$ must be less than or equal to n . Suppose that the order is m , $m < n$. Then $(g^{-1}xg)^m = 1 \Rightarrow g^{-1}x^m g = 1 \Rightarrow x^m = 1$, contradicting the order of x being n . Thus the order of $g^{-1}xg$ is the same as the order of x .

Suppose for some $a, b \in G$ that $|ab| = n$. Then $(ab)^n = 1 \Rightarrow \underbrace{ab \dots ab}_{n \text{ times}} \Rightarrow a(ba)^{n-1}b = 1$. Now we can left-multiply both sides of this equation by b and

then right-multiply by b^{-1} to obtain $ba(ba)^{n-1}bb^{-1} = bb^{-1} \Rightarrow (ba)^n = 1$. By similar logic to above, the order of ba must be at most n , and can in fact be no less than it, and is thus equal to the order of ab . \square

23. (12/31/22)

Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t , prove that $|x^s| = t$.

Proof. The order of x is n , so $x^n = 1$. Then $x^{st} = 1$. From 19., $(x^s)^t = 1$. So the order of x^s is at most t .

Suppose that the order of x^s is $r < t$. Then $(x^s)^r = 1 \Rightarrow x^{sr} = 1$, and so the order of x is at most $sr < st = n$, a contradiction. Therefore the order of x^s is exactly t . \square

24. (1/5/23)

If a and b are commuting elements of G , prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.

Proof. We will prove this statement first for non-negative integers only, using induction. First, note that (trivially) $(ab)^0 = 1$ and $a^0 b^0 = 1 \cdot 1 = 1$, so $(ab)^0 = a^0 b^0$.

Next, suppose that $(ab)^n = a^n b^n$ for some positive integer n (in order to show that the statement holds for $n+1$). By our inductive hypothesis, $(ab)^{n+1} = (ab)^n ab = a^n b^n ab$. Since a and b commute, so do any non-negative powers of a and b , specifically, $ab^n = b^n a$. Thus $a^n b^n ab = a^n ab^n b = a^{n+1} b^{n+1}$, as desired.

Having established this for positive integers, we can now do the same for negative integers. For the base case of -1 , let $ab = ba = x$. Then $(ab)^{-1} = x^{-1}$, which implies that $b^{-1}a^{-1} = x^{-1}$. Also, we have $(ba)^{-1} = a^{-1}b^{-1} = x^{-1}$, so $(ab)^{-1} = x^{-1} = a^{-1}b^{-1}$.

Now suppose that $(ab)^{-n} = a^{-n}b^{-n}$ for some positive integer n . Following the logic for non-negative integers, we see that $(ab)^{-(n+1)} = (ab)^{-n}(ab)^{-1} = a^{-n}b^{-n}a^{-1}b^{-1}$. Having established that negative powers of a and b commute just as do non-negative powers, we have $a^{-n}b^{-n}a^{-1}b^{-1} = a^{-(n+1)}b^{-(n+1)}$, as desired. \square

25. (1/12/23)

Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Proof. Suppose that G is a group such that, for all $x \in G$, $x^2 = 1$. Left-multiplying by x^{-1} , this implies that $x = x^{-1}$; that is, each element of G is its own inverse.

Let $a, b \in G$. Then $ab = (ab)^{-1} = b^{-1}a^{-1}$, and since each element is its own inverse, this equals ba . Thus all elements of G commute, so G is an abelian group. \square

26. (1/12/23)

Assume H is a nonempty subset of (G, \star) which is closed under the binary operation on G and is closed under inverses, i.e., for all $h, k \in H$, hk and $h^{-1} \in H$. Prove that H is a group under the operation \star restricted to H (a *subgroup* of G).

Proof. For H to be a group under the operation \star , it must fulfill associativity, existence of identity, and existence of inverses.

Associativity is given by the fact that the operation \star is associative on G , since G is a group. Inverses are also given. It remains to be proven that H contains the identity element.

Let $h \in H$. Since H is closed under inverses, $h^{-1} \in H$. H is closed under \star , so $hh^{-1} \in H$. By definition, $hh^{-1} = 1$, so $1 \in H$. \square

27. (1/12/23)

Prove that if x is an element of G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G (called the *cyclic subgroup* of G generated by x).

Proof. Let $x \in G$ and let $X = \{x^n \mid n \in \mathbb{Z}\}$. We must prove that X is associative and contains the identity element and inverses for each element.

Let $x^n, x^m, x^k \in X$.

$$(x^n x^m) x^k = (x^{n+m}) x^k = x^{n+m+k} = x^n (x^{m+k}) = x^n (x^m x^k),$$

so X is associative.

$0 \in \mathbb{Z}$, so $x^0 = 1 \in X$, and so X contains the identity element.

Finally, let $x^n \in X$. $-n \in \mathbb{Z} \Rightarrow x^{-n} \in X$. Since $x^n x^{-n} = x^0 = 1$, there is an inverse for each element of X in X . Thus X is a subgroup of G . \square

28. (1/14/23)

Let (A, \star) and (B, \diamond) be groups and let $A \times B$ be their direct product. Verify all the group axioms for $A \times B$: associativity, identity, and inverses.

Proof. To prove that $A \times B$ is associative, let $a_1, a_2, a_3 \in A$ and $b_1, b_2, b_3 \in B$. Consider $(a_1, b_1)[(a_2, b_2)(a_3, b_3)]$. This equals $(a_1, b_1)(a_2 \star a_3, b_2 \diamond b_3)$, which equals $(a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3))$. Now since A and B are themselves associative, we can rewrite this as $((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3)$, which is equal to $(a_1 \star$

$a_2, b_1 \star b_2)(a_3, b_3)$, which in turn equals $[(a_1, b_1)(a_2, b_2)](a_3, b_3)$. Thus $A \times B$ is associative.

Next, since A and B are groups, they each contain an identity element, $1_A, 1_B$, respectively. By definition, $A \times B$ contains $(1_A, 1_B)$. For any $(a, b) \in A \times B$, $(a, b)(1_A, 1_B) = (a \star 1_A)(b \diamond 1_B) = (a, b)$. Thus $A \times B$ contains the identity element $(1_A, 1_B)$.

Finally, let $(a, b) \in A \times B$. A and B contain inverses for each element, so $(a^{-1}, b^{-1}) \in A \times B$. Now $(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1_A, 1_B)$, the identity element of $A \times B$. Thus $A \times B$ also contains an inverse for each element.

$A \times B$ satisfies the three group axioms of associativity, identity, and inverses, and is thus a group itself. \square

29. (1/17/23)

Prove that $A \times B$ is an abelian group if and only if A and B are both abelian.

Proof. First, we will show that if A and B are abelian groups under their respective operations \star and \diamond , then $A \times B$ is as well. We see that $(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$. Since elements of A and B commute, this is equal to $(a_2 \star a_1, b_2 \diamond b_1)$, which, by definition of $A \times B$, is equal to $(a_2, b_2)(a_1, b_1)$. Thus $A \times B$ is an abelian group.

Next, let $A \times B$ be an abelian group. So we have $(a_2 \star a_1, b_2 \diamond b_1) = (a_1 \star a_2, b_1 \diamond b_2)$. Therefore we have $a_2 \star a_1 = a_1 \star a_2$ and $b_2 \diamond b_1 = b_1 \diamond b_2$, so A and B must both be abelian groups. \square

30. (1/17/23)

Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

Proof. To show that $(a, 1)$ and $(1, b)$ commute, we note that:

$$(a, 1)(1, b) = (a \star 1, 1 \diamond b) = (a, b) = (1 \star a, b \diamond 1) = (1, b)(a, 1).$$

Suppose that $|a| = n, |b| = m$, with n and m both positive integers (if one is infinite then the element (a, b) of $A \times B$ obviously has infinite order). If we let k be the least common multiple of n and m , then $(a, b)^k = (a^k, b^k) = (1, 1)$, the identity element of $A \times B$ (since k is a multiple of both n and m). Further, $(a, b)^j = (a^j, b^j) \neq (1, 1)$ for any $j < k$: If $a^j = 1$, then $b^j \neq 1$ (and vice-versa), or else j would be the least common multiple of n and m . \square

31. (1/17/23)

Prove that any finite group G of even order contains an element of order 2.

Proof. Let $t(G) = \{g \in G \mid g \neq g^{-1}\}$. For all $x \in t(G)$, $x \neq x^{-1} \Rightarrow x^2 \neq 1$, that is, $t(G)$ is a subset of G consisting of elements of order not equal to 2. Also, $1 \notin t(G)$ (since $1 = 1^{-1}$), so $|G| > |t(G)|$.

Let $x \in t(G)$. Then $x \neq x^{-1}$. Since $x = (x^{-1})^{-1}$, we also have $x^{-1} \neq (x^{-1})^{-1}$, and so $x^{-1} \in t(G)$. For every element in $t(G)$, its inverse must also be in $t(G)$. Because (from above), $t(G)$ cannot contain the identity element, its order must be even. The order of G is even, and since the difference of two even numbers is also even, the order of $G - t(G)$ is even as well.

Now since the order of $t(G)$ is both even and strictly less than that of G , we know that G contains (at least) 2 elements not in $t(G)$, namely, the identity and some other element whose order is 2. Thus any finite group G of even order contains an element of order 2. \square

32. (1/22/23)

If x is an element of finite order n in G , prove that the elements $1, x, x^2, \dots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Proof. Let $x \in G$ with $x^n = 1$. Suppose for some $k < m < n$, we have $x^m = x^k$. Then $x^m = x^k \Rightarrow x^m x^{-k} = 1 \Rightarrow x^{m-k} = 1$. Since $m - k < n$, this contradicts x having order n . Therefore for no two elements x^m and x^k , with m and k less than n , are those elements equal.

If $|G|$ is infinite, then the order of x is by definition less than that of G . Suppose $|G| = p$, and that $|x| = n > p$. Then the cyclic subgroup generated by x , $\{x^k \mid 0 \leq k < n\}$, which has n distinct elements and is a subset of G , contains more elements than G 's p elements, a contradiction. Therefore the order of x must be no greater than $|G|$. \square

33. (1/22/23)

Let x be an element of finite order n in G .

- (a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \dots, n-1$.

Proof. Consider the smallest even k such that $x^k = 1$. The order of x is n , so $k > n$. And since $x^{2n} = x^n x^n = 1 \cdot 1 = 1$, k is at most $2n$. Suppose $n < k < 2n$. Then we have $x^{2n} = x^k x^{2n-k}$. We know that x^{2n} and x^k are both the identity, so it follows that $1 = x^{2n-k}$. However, since $k > n$, $2n - k < 2n - n = n$, which contradicts $|x| = n$. Therefore k cannot be less than $2n$, and so $k = 2n$ is the smallest even power of x equaling identity.

Note that if $x^i = x^{-i}$, then $x^{2i} = 1$. However, from above, the smallest possible value of i for this to occur is n . That is, for no $1 \leq i < n$ do we have $x^{2i} = 1$, and therefore $x^i \neq x^{-i}$ for all such values of i . \square

- (b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

Proof. Let $|x| = n = 2k$ and let $1 \leq i < n$. First, in order to show that $i = k$, let $x^i = x^{-i} \Rightarrow x^{2i} = 1$. Suppose that $i \neq k$. Because $|x| = 2k$, we cannot have $i < k$, or else $x^{2i} = 1$ would be a contradiction. So we must have $k < i < n$. Additionally, we have $2k = n \Rightarrow 2i > n$. $x^n = 1$ implies that $x^{-n} = 1$, so we see that $x^{2i}x^{-n} = x^{2i-n} = 1$. By assumption,

$$k = \frac{n}{2} < i < n \Rightarrow n < 2i < 2n \Rightarrow 0 < 2i - n < n.$$

Thus $2i - n$ is a positive integer less than n such that $x^{2i-n} = 1$, a contradiction. Therefore $i = k$.

Next, in order to show that $x^i = x^{-i}$, let $i = k$. Then we have $x^n = x^{2k} = x^{2i} = 1$. Multiplying both sides by x^{-i} , it follows that $x^i = x^{-i}$. \square

34. (1/22/23)

If x is an element of infinite order in G , prove that the elements $x^n, n \in \mathbb{Z}$ are all distinct.

Proof. Toward contradiction, suppose that for some $m > n \in \mathbb{Z}$, $x^m = x^n$. Then $x^m x^{-n} = 1 \Rightarrow x^{m-n} = 1$. Since $m \neq n$, $m - n$ is a positive integer such that $x^{m-n} = 1$, and so $|x|$ is an integer greater than or equal to $m - n$, contradicting x having infinite order. Therefore the elements $x^n, n \in \mathbb{Z}$ are all distinct. \square

35. (1/22/23)

If x is an element of finite order n in G , use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \dots, x^{n-1}\}$.

Proof. Let $k > n$. From the Division Algorithm, there are unique $q, r \in \mathbb{Z}$ such that $k = qn + r$ and $0 \leq r < n$. Now:

$$x^k = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = 1^q x^r = x^r,$$

and since $0 \leq r < n$, $x^r = x^k$ is an element of the cyclic subgroup of G generated by x . Therefore any integral power of x is contained in its cyclic subgroup. \square

36. (1/22/23)

Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Exercise 32, every element has order ≤ 3). Use the cancellation laws to show that there is a unique group table for G . Deduce that G is abelian.

Proof. Suppose, toward contradiction (and without loss of generality), that $ab \neq ba$. We know that a and b are both distinct from 1. If ab equals either a or b , this is a contradiction, since it implies that either b or a is 1, respectively (the same holds for ba). Therefore we must have either $ab = c$ or $ab = 1$. Suppose that $ab = c$. Then, since $ab \neq ba$, it follows that $ba = 1$. But then $b = a^{-1}$, and so $ab = c \Rightarrow aa^{-1} = c \Rightarrow 1 = c$, a contradiction. Therefore we must have $ab = ba$. The same logic holds for any pair among a, b , and c , and so G is an abelian group. \square