MATH 343 · Group Theory

Chapter 2 Assigned Problems

Exercises 5, 10, 13, 14, 16, 21, 27, 36, 42, and 45

Solutions based on Gallian, Contemporary Abstract Algebra, 10th edition

Exercise 5: Question

Question

Find the inverse of each element under the indicated group operation.

(a) Additive group $13 \in \mathbb{Z}_{20}$

(b) Multiplicative group $13 \in U(14)$

(c) Multiplicative group $n-1 \in U(n),\ n>2$

(d) Multiplicative group $3-2i \in \mathbb{C}^*$

Exercise 5: Solution

Find the inverse of each element under the indicated group operation.

(a) Additive group	$\mathbb{Z}_{20}$	$-13 \equiv 7 \ (mod\ 20)$
(b) Multiplicative group	$U(14)$	$13^{-1} = 13, \qquad 13 \cdot 13 \equiv 1 \ (mod\ 14)$
(c) Multiplicative group	$U(n), n > 2$	$(n-1)^{-1} = n-1, \qquad (n-1)^2 \equiv 1 \ (mod\ n)$
(d) Multiplicative group	$\mathbb{C}^*$	$(3-2i)^{-1} = \frac{1}{3-2i} = \frac{3+2i}{13}$

Exercise 10: Question

Question

List the elements of the group below and find the inverse of each element.

$$U(20)$$

Exercise 10: Solution

List the elements of U(20) and find the inverse of each one.

$$U(20) = \{1,3,7,9,11,13,17,19\}$$

a	1	3	7	9	11	13	17	19
a^{-1}	1	7	3	9	11	17	13	19

$$3 \cdot 7 \equiv 1, \qquad 13 \cdot 17 \equiv 1, \qquad 9^2 \equiv 11^2 \equiv 19^2 \equiv 1 \pmod{20}$$

Thus 1, 9, 11, and 19 are self-inverse; the remaining inverse pairs are 3 with 7 and 13 with 17.

Exercise 13: Question

Question

Show that the first set is not a group under multiplication modulo 4, while the second set is a group under multiplication modulo 5.

$\{1,2,3\}$ multiplication modulo 4

$\{1,2,3,4\}$ multiplication modulo 5

Exercise 13: Solution

Compare {1,2,3} under multiplication modulo 4 with {1,2,3,4} under multiplication modulo 5.

Modulo 4: not a group

$$2 \cdot 2 \equiv 0 \ (mod\ 4), \qquad 0 \notin \{1,2,3\}$$

Closure fails. Equivalently, 2 has no multiplicative inverse modulo 4.

Modulo 5: a group

$$\{1,2,3,4\} = U(5)$$

Associativity comes from integer multiplication. The identity is 1, and multiplication modulo 5 is closed on these nonzero residues.

$$1^{-1} = 1, \qquad 4^{-1} = 4, \qquad 2^{-1} = 3, \qquad 3^{-1} = 2$$

Exercise 14: Question

Question

Show that the group of invertible real 2×2 matrices is non-Abelian by finding two matrices whose products depend on the order of multiplication.

$$A, B \in GL(2, \mathbb{R}), \quad AB \neq BA$$

Exercise 14: Solution

Exhibit invertible real matrices A and B such that AB ≠ BA.

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \qquad \det(A) = \det(B) = 1$$

Compute in both orders

$$AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

$$AB \neq BA$$

Exercise 16: Question

Question

Under multiplication modulo 40, show that the following set is a group.

$$S = \{5, 15, 25, 35\}$$

What is the identity element? How does its multiplication table compare with the multiplication table for U(8)?

Exercise 16: Solution

Show that S = {5,15,25,35} is a group under multiplication modulo 40. Identify its identity and its relationship with U(8).

·	25	5	15	35
25	25	5	15	35
5	5	25	35	15
15	15	35	25	5
35	35	15	5	25

The table gives closure. Associativity comes from modular multiplication.

$$e_S = 25$$

Every element is its own inverse, as the diagonal entries are 25.

Reduce each label modulo 8.

$$25 \equiv 1, \qquad 5 \equiv 5, \qquad 15 \equiv 7, \qquad 35 \equiv 3 \pmod 8$$

After this relabeling, the table matches the multiplication table for U(8). The two groups have the same multiplication pattern.

Exercise 21: Question

Question

Prove that the real 2×2 matrices with determinant 1 form a group under matrix multiplication.

$$G = \{A \in M_2(\mathbb{R}) : \det(A) = 1\}$$

Exercise 21: Solution

Prove that the real 2 × 2 matrices with determinant 1 form a group under matrix multiplication.

$$G = \{A \in M_{2(\mathbb{R})} : \det(A) = 1\}$$

Closure

$$A, B \in G \;\Rightarrow\; \det(AB) = \det(A)\det(B) = 1$$

Associativity Matrix multiplication is associative.

Identity

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$$

Inverses

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \;\Rightarrow\; A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$\det\left(A^{-1}\right) = \det(A)^{-1} = 1$$

Therefore G is a group under matrix multiplication.

Exercise 27: Question

Question

Prove that a group G is Abelian if and only if the following equation holds for every pair of elements a and b in G.

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

Exercise 27: Solution

Prove that G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a,b \in G$.

Forward direction

$$G \text{ Abelian} \;\Rightarrow\; (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$$

Reverse direction

Assume the displayed inverse identity holds for every a and b. The usual product-inverse law also holds in every group.

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

Taking inverses reverses both products:

$$ba = ab$$

Exercise 36: Question

Question

Prove each statement for arbitrary elements a and b of a group.

(a) $(ab)^2 = a^2b^2$ if and only if $ab = ba$

(b) $(ab)^{-2} = b^{-2}a^{-2}$ if and only if $ab = ba$

Exercise 36(a): Solution

Prove that $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

If the squares are equal

$$(ab)^2 = a^2b^2 \;\Rightarrow\; abab = aabb$$

Cancel a on the left, then cancel b on the right.

$$bab = abb \;\Rightarrow\; ba = ab$$

If a and b commute

$$ab = ba \;\Rightarrow\; (ab)^2 = abab = a(ba)b = a(ab)b = a^2b^2$$

Both implications hold, which proves the equivalence.

Exercise 36(b): Solution

Prove that $(ab)^{-2} = b^{-2}a^{-2}$ if and only if $ab = ba$.

Use the product-inverse law to rewrite the left side.

$$(ab)^{-2} = \left((ab)^{-1}\right)^2 = \left(b^{-1}a^{-1}\right)^2$$

Part (a), applied to b^{-1} and a^{-1}, gives

$$\left(b^{-1}a^{-1}\right)^2 = b^{-2}a^{-2} \;\Leftrightarrow\; b^{-1}a^{-1} = a^{-1}b^{-1}$$

Taking inverses of the final equality gives

$$ab = ba$$

Every step is reversible, so the two conditions are equivalent.

Exercise 42: Question

Question

Let R be a rotation and F a reflection in the dihedral group D_n. Prove the equation below for every integer k.

$$FR^kF = R^{-k}$$

Why does this show that D_n is non-Abelian?

Exercise 42: Solution

In D_n, prove that $FR^kF = R^{-k}$ for a rotation R and a reflection F. Explain why D_n is non-Abelian.

The product FR^k is a reflection, so it has order 2.

$$\left(FR^k\right)^2 = e$$

$$FR^kFR^k = e \;\Rightarrow\; FR^kF = R^{-k}$$

Let r be the basic rotation of the regular n-gon, where n ≥ 3. If D_n were Abelian, then F and r would commute.

$$FrF = r^{-1}, \qquad \text{but commutativity would give } FrF = r$$

$$r \neq r^{-1} \; because \; |r| = n > 2$$

Exercise 45: Question

Question

Suppose every element of a group G squares to the identity. Prove that G is Abelian.

$$x^2 = e, \quad x \in G$$

Exercise 45: Solution

Suppose $x^2 = e$ for every x in a group G. Prove that G is Abelian.

For each $x \in G$, the hypothesis gives

$$x^2 = e \quad \Rightarrow \quad x = x^{-1}$$

Now let $a,b \in G$. The hypothesis also applies to the product ab.

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

Thus every pair of elements commutes, and G is Abelian.