Ch 2 Exersices

Math343

Exercise 6: Group Operations

Part (b): In $GL(2, \mathbb{Z}_{13})$, find $\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}$

Solution:

For a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, the determinant is $ad - bc$.

$$\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix} = (7)(5) - (4)(1) = 35 - 4 = 31$$

Since we're working in $\mathbb{Z}_{13}$:

$$31 \equiv 5 \pmod{13}$$

Answer: $\det = 5$

Part (d): In $GL(2, \mathbb{Z}_7)$, find $\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}^{-1}$

Solution:

First, find the determinant:

$$\det \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} = (2)(3) - (1)(1) = 6 - 1 = 5 \equiv 5 \pmod{7}$$

For matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, the inverse is:

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

The multiplicative inverse of 5 modulo 7 is 3, since $5 \cdot 3 \equiv 1 \pmod{7}$.

$$A^{-1} = 3 \begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 9 & -3 \\ -3 & 6 \end{bmatrix} \equiv \begin{bmatrix} 2 & 4 \\ 4 & 6 \end{bmatrix} \pmod{7}$$

Answer: $\begin{bmatrix} 2 & 4 \\ 4 & 6 \end{bmatrix}$

Exercise 10: $U(20)$ and Inverses

Find all elements of $U(20)$ and their inverses

Solution:
$U(20) = \{k : 1 \leq k < 20, \gcd(k, 20) = 1\}$

Since $20 = 2^2 \cdot 5$, we need $\gcd(k, 20) = 1$:
$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

Finding Inverses (solve $ax \equiv 1 \pmod{20}$):

Element	Inverse	Verificati[No Title]
1	1	$1 \cdot 1 = 1 \equiv 1 \pmod{20}$
3	7	$3 \cdot 7 = 21 \equiv 1 \pmod{20}$
7	3	$7 \cdot 3 = 21 \equiv 1 \pmod{20}$
9	9	$9 \cdot 9 = 81 \equiv 1 \pmod{20}$
11	11	$11 \cdot 11 = 121 \equiv 1 \pmod{20}$
13	17	$13 \cdot 17 = 221 \equiv 1 \pmod{20}$
17	13	$17 \cdot 13 = 221 \equiv 1 \pmod{20}$
19	19	$19 \cdot 19 = 361 \equiv 1 \pmod{20}$

Exercise 13: Multiplication Modulo Analysis

Show that $\{1, 2, 3\}$ under multiplication mod 4 is not a group, but $\{1, 2, 3, 4\}$ under multiplication mod 5 is a group.

Part 1: $\{1, 2, 3\}$ under multiplication mod 4

Cayley Table:

$\times$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Problems:

1. **Not closed:** $2 \times 2 = 4 \equiv 0 \pmod 4$, but $0 \notin \{1, 2, 3\}$
2. **No inverse for 2:** No element x satisfies $2x \equiv 1 \pmod 4$

Part 2: $\{1, 2, 3, 4\}$ under multiplication mod 5

Cayley Table:

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

[No Title]

Verification of group properties:

- **Closure:** ✓ (all entries in table are in the set)
- **Identity:** 1 is the identity
- **Inverses:** $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$
- **Associativity:** ✓ (inherited from integer multiplication)

Exercise 14: Non-Abelian Nature of $GL(2, \mathbb{R})$

Show $GL(2, \mathbb{R})$ is non-Abelian

Solution:

We need matrices $A, B \in GL(2, \mathbb{R})$ such that $AB \neq BA$.

Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$

Compute AB:

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

Compute BA:

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

Since $AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = BA$, $GL(2, \mathbb{R})$ is non-Abelian.

Exercise 16: Show $\{5, 15, 25, 35\}$ is a group under multiplication mod 40

Cayley Table:

$\times$	**5**	**15**	**25**	**35**
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

Group Properties:

- **Closure:** ✓ (all products are in the set)
- **Identity:** 25 (since $25x \equiv x \pmod{40}$ for all x in the set)
- **Inverses:** Each element is its own inverse
- **Associativity:** ✓ (inherited from integer multiplication)

Relationship to $U(8)$:
$U(8) = \{1, 3, 5, 7\}$ under multiplication mod 8.

The mapping $\phi : U(8) \to \{5, 15, 25, 35\}$ defined by $\phi(x) = 5x \bmod 40$ is an isomorphism:

- $\phi(1) = 5$, $\phi(3) = 15$, $\phi(5) = 25$, $\phi(7) = 35$

Exercise 17: Translate multiplicative expressions to additive counterparts

Part (a): a^2b^3

In additive notation: $2a + 3b$

Part (b): $a^{-2}(b^{-1}c)^2$

Step by step:

- $a^{-2} \to -2a$
- $b^{-1}c \to -b + c$
- $(b^{-1}c)^2 \to 2(-b + c) = -2b + 2c$
- $a^{-2}(b^{-1}c)^2 \to -2a + (-2b + 2c) = -2a - 2b + 2c$

Part (c): $(ab^{-2})^{-3} = e$

Step by step:

- $ab^{-2} \to a + (-2b) = a - 2b$
- $(ab^{-2})^{-3} \to -3(a - 2b) = -3a + 6b$
- $(ab^{-2})^{-3} = e \to -3a + 6b = 0$

Exercise 27: Prove: G is Abelian iff $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$

Proof:

(⇒) If G is Abelian:
Assume G is Abelian, so $ab = ba$ for all $a, b \in G$.

We know $(ab)^{-1} = b^{-1}a^{-1}$ (socks-shoes property).

Since G is Abelian: $a^{-1}b^{-1} = b^{-1}a^{-1}$

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

(⇐) If $(ab)^{-1} = a^{-1}b^{-1}$ for all a, b:
Assume $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

By the socks-shoes property: $(ab)^{-1} = b^{-1}a^{-1}$

Therefore: $a^{-1}b^{-1} = b^{-1}a^{-1}$ for all $a, b \in G$

Taking inverses: $(a^{-1}b^{-1})^{-1} = (b^{-1}a^{-1})^{-1}$

Using socks-shoes: $ba = ab$ for all $a, b \in G$

Therefore G is Abelian. □

Exercise 34: Examples of Specific Group Orders

Give examples of groups with specified orders

Group with exactly 105 elements:

Example: $\mathbb{Z}_{105}$ under addition modulo 105

Three groups with 40 elements:

Examples:

1. $\mathbb{Z}_{40}$ under addition modulo 40
2. D_{20}
3. $U(41)$

Exercise 36: Prove: $(ab)^2 = a^2b^2$ iff $ab = ba$

(⇒) If $(ab)^2 = a^2b^2$:
$(ab)^2 = (ab)(ab) = a^2b^2$

Right-multiply by b^{-1}: $(ab)(ab)b^{-1} = a^2b^2b^{-1}$
$(ab)a = a^2b$

Left-multiply by a^{-1}: $a^{-1}(ab)a = a^{-1}a^2b$
$ba = ab$

(⇐) If $ab = ba$:
$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2b^2$

Second part: $(ab)^{-2} = b^{-2}a^{-2}$ iff $ab = ba$

Proof: $(ab)^{-2} = ((ab)^2)^{-1} = (a^2b^2)^{-1} = (b^2)^{-1}(a^2)^{-1} = b^{-2}a^{-2}$

This holds iff $(ab)^2 = a^2b^2$, which we proved above occurs iff $ab = ba$. □

Exercise 45: Prove: If $x^2 = e$ for all $x \in G$, then G is Abelian

Proof:

Let $a, b \in G$. We want to show $ab = ba$.

Since every element has order 2:

- $a^2 = e$, so $a^{-1} = a$
- $b^2 = e$, so $b^{-1} = b$
- $(ab)^2 = e$, so $(ab)^{-1} = ab$

Now, $(ab)^{-1} = b^{-1}a^{-1} = ba$ (socks-shoes property)

But also $(ab)^{-1} = ab$ (since $(ab)^2 = e$)

Therefore: $ab = ba$

Since this holds for arbitrary $a, b \in G$, the group G is Abelian. □

Exercise 47: List elements of $GL(2, \mathbb{Z}_2)$ and show non-Abelian

All possible matrices over $\mathbb{Z}_2$:

We need $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc \neq 0 \pmod 2$

The six elements are:

1. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (det = 1)
2. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (det = 1)
3. $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ (det = 1)
4. $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (det = 1)
5. $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ (det = 1)
6. $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ (det = 1)

Non-Abelian proof:

Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$

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

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

Since $AB \neq BA$, $GL(2, \mathbb{Z}_2)$ is non-Abelian. □