# Modern Algebra I Problem Set 3 Answer Key

Zheheng Xiao

Oct 7, 2023

# 1 Problem 1

## 1.1 Part (a)

Yes. For example, we can define the binary operation $\star$ to be

$$e \star e = f, \quad e \star f = f, \quad f \star e = f, \quad f \star f = e.$$

On one hand we have

$$(e \star e) \star f = f \star f = e,$$

while on the other hand we have

$$e \star (e \star f) = e \star f = f.$$

Therefore $\star$ is not associative.

## 1.2 Part (b)

No, $\star$ is not necessarily associative. Similar to part (a), we may define $\star$ to satisfy $f \star f = g$, $f \star g = g$, $g \star f = g$,$g \star g = f$. Then $(f \star f) \star g \neq f \star (f \star g)$.

# 2 Problem 2

The group $\mathbb{Z}/5\mathbb{Z}$ has two subgroups: the trivial subgroup $\{0\}$, and the group $\mathbb{Z}/5\mathbb{Z}$ itself. In this case, there are no subrgoups of 3 elements.

The group $\mathbb{Z}/6\mathbb{Z}$ has four subgroups: the trivial subgroup $\{0\}$, the subgroup $\{0, 3\}$, the subgroup $\{0, 2, 4\}$, and $\mathbb{Z}/6\mathbb{Z}$ itself. In this case, there is 1 subgroup that contains 3 elements.

# 3 Problem 3

## 3.1 Part(a)

In exponential function, the coordinates of the points in $\mu_n$ are $e^{2k\pi i/n}$, where $k \in \{0, 1, \cdots, n-1\}$. In trignometric functions, they are $\cos(2k\pi/n) + i\sin(2k\pi/n)$, where where $k \in \{0, 1, \cdots, n-1\}$.

### 3.2 Part (b)

Note that for $k_1, k_2 \in \{0, 1, \cdots, n-1\}$, we have

$$e^{2k_1\pi i/n} \cdot e^{2k_2\pi i/n} = e^{2k'\pi i/n} \in \mu_n,$$

where $k' \equiv k_1 + k_2 \pmod{n}$ and $k' \in \{1, 2, \cdots, n\}$. This shows that multiplication is a binary operation on the set $\mu_n$. It remains to check that $\mu_n$ satisfies the group axioms:

- Identity: Note that $1 = e^{2\cdot 0\pi i/n} \in \mu_n$, and for any $k$, we have

$$1 \cdot e^{2k\pi i/n} = e^{2k\pi i/n} \cdot 1 = e^{2k\pi i/n}.$$

- Inverse: Any $e^{2k\pi i/n} \in \mu_n$ has inverse $e^{2(n-k)\pi i/n} \in \mu_n$, satisfying $e^{2k\pi i/n} \cdot e^{2(n-k)\pi i/n} = 1$.
- Associativity: This is true because for any $e^{2k_1\pi i/n}, e^{2k_2\pi i/n}, e^{2k_3\pi i/n} \in \mu_n$, we have

$$(e^{2k_1\pi i/n} \cdot e^{2k_2\pi i/n}) \cdot e^{2k_3\pi i/n} = e^{2k_1\pi i/n} \cdot (e^{2k_2\pi i/n} \cdot e^{2k_3\pi i/n}) = e^{2(k_1+k_2+k_3)\pi i/n}.$$

Therefore, $\mu_n$ is a group under multiplication.

### 3.3 Part (c)

Define $f : \mathbb{Z}/n\mathbb{Z} \to \mu_n$, where $f(k) = e^{2k\pi i/n}$. We can find an inverse map $g : \mu_n \to \mathbb{Z}/n\mathbb{Z}$ by setting $g(e^{2k\pi i/n}) = k$, and noting that

$$f \circ g(e^{2k\pi i/n}) = f(k) = e^{2k\pi i/n}, \qquad g \circ f(k) = g(e^{2k\pi i/n}) = k.$$

This shows that $f$ is a bijection. Moreover, $f$ is a group homomorphism because for $k_1, k_2 \in \mathbb{Z}/n\mathbb{Z}$, we have

$$f(k_1) \cdot f(k_2) = e^{2k_1\pi i/n} \cdot e^{2k_2\pi i/n} = e^{2(k_1+k_2)\pi i/n} = f(k_1 + k_2).$$

Therefore, the map $f$ is an isomorphism of groups.

### 3.4 Part (d)

Part (c) has $\phi(n)$ solutions, where $\phi(n)$ is Euler's totient function of $n$. To see why, observe that the isomorphism $f$ must map generators to generators; in particular, once we determine where the generator $1 \in \mathbb{Z}/n\mathbb{Z}$ maps to, we determine the entire map $f$ from the group homomorphism property

$$f(k) = kf(1),$$

for each $k \in \mathbb{Z}/n\mathbb{Z}$. Finally, note that the generators of $\mu_n$ are the primitive roots of unity, and there are $\phi(n)$ of them. Therefore, the number of isomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mu_n$ is $\phi(n)$.

# 4 Problem 4

## 4.1 Part (a)

For any $A, B \in GL(2, \mathbb{R})$, their product $AB$ is a $2 \times 2$ matrix with determinant

$$\det(AB) = \det(A) \cdot \det(B) \neq 0,$$

and so $AB \in GL(2, \mathbb{R})$. This shows that multiplication is a binary operation on $GL(2, \mathbb{R})$. Next, we check that $GL(2, \mathbb{R})$ satisfies the group axioms:

- Identity: The identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbb{R})$.
- Inverse: For any $M \in GL(2, \mathbb{R})$, its inverse $M^{-1}$ exists because $\det(M) \neq 0$. Moreover, the matrix $M^{-1}$ is also a 2 by 2 matrix with nonzero determinant, i.e., $M^{-1} \in GL(2, \mathbb{R})$.
- Associativity: This is obvious since matrix multiplication is associative. In other words, we have
$$(AB)C = A(BC), \quad \forall A, B, C \in GL(2, \mathbb{R}).$$

Therefore, the set $GL(2, \mathbb{R})$ forms a group under matrix multiplication.

Next, we give an example that shows matrix multiplication is not commutative. Let

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

The matrices $A, B$ are in $GL(2, \mathbb{R})$ since their determinants are both 1. On the one hand, we have

$$A \cdot B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

On the other hand, we have

$$B \cdot A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

We see then that $A \cdot B \neq B \cdot A$.

## 4.2 Part(b)

We define subgroups $H_n$ of $GL(2, \mathbb{R})$ of a general order $n$ as follows:

$$H_n := \left\{ \begin{bmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{bmatrix} : k \in \{0, 1, \cdots, n\} \right\}.$$

Geometrically, this is the group generated by rotations of $\mathbb{R}^2$ by degree $2\pi k/n$, so $H_n$ indeed has order $n$. Thus, $H_2, H_3, H_4$ are subgroups of order $2, 3, 4$, respectively.

# 5 Problem 5

## 5.1 Exercise 2

- (a) $G$ is not a group, since it doesn't have an identity element.
- (b) $G$ is a group, and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The identity element is $a$. The inverses are given by
$$a^{-1} = a, \quad b^{-1} = b, \quad c^{-1} = c, \quad d^{-1} = d.$$
Associativity can be checked from the table.
- (c) $G$ is a group, and is isomorphic to $\mathbb{Z}/4Z$. The identity element is $a$. The inverses are given by
$$a^{-1} = a, \quad b^{-1} = d, \quad c^{-1} = a, \quad d^{-1} = b.$$
Associativity can be checked from the table.
- (d) $G$ is not a group, since the operation $\circ$ is not associative:
$$(bc)b = cb = b, \quad b(cb) = bb = a.$$

## 5.2 Exercise 10

We check that the Heisenberg group satisfies the group axioms:

- Identity: The identity matrix $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ belongs to the Heisenberg group.
- Inverse: We check that
$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix},$$
which belongs to the Heisenberg group.
- Associativity: Holds because matrix multiplication is associative. Therefore, matrices of the form
$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$$
is a group under matrix multiplication.