

SAMPLE MIDTERM

Structure of the test. There will be four questions. The first two will be theoretical, the second two computational.

1. A proof of one of the theorems from Sections 5 and 6. (10pt)
2. A theoretical problem on isomorphisms. (10pt)
3. Computing the cyclic subgroup of a given group when the generator is given. There will be two subgroups to compute. (5pt + 5pt)
4. Determining whether a given map is an isomorphism between two structures. There will be two maps given. (5pt + 5pt)

Sample Problems.

1. Prove that if $(G, *)$ is a group, $a \in G$ and $m, n \in \mathbb{Z}$ then

(a) $a^{m+n} = a^m * a^n$;

(b) $(a^m)^n = a^{m \cdot n}$.

2. Let $(G, *)$ be a group and $g \in G$. Let $f : G \rightarrow G$ be a map defined by

$$f(x) = g^{-1} * x * g.$$

Prove that $f : (G, *) \rightarrow (G, *)$ is an isomorphism.

3. In each of the following cases compute the cyclic subgroup of the given group generated by the given element.

(a) $(G, *)$ is $(\mathbb{Z}_{12}, +_{12})$ and $a = 10$. Find $\langle a \rangle$.

(b) $(G, *)$ is $\text{GL}(2, \mathbb{C})$, i.e. the set of all 2×2 matrices with matrix multiplication and $A = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$ Find $\langle A \rangle$.

4. In each of the following cases determine whether the given map is an isomorphism between the two structures. Give a rigorous proof that justifies your solution.

- (a) (\mathbb{C}, \cdot) are complex numbers with usual multiplication. (\mathcal{M}, \cdot) is the set of all 2×2 matrices from $M_2(\mathbb{R})$ of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

with matrix multiplication. The map $f : \mathbb{C} \rightarrow \mathcal{M}$ is given by:

$$f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Determine whether $f : (\mathbb{C}, \cdot) \rightarrow (\mathcal{M}, \cdot)$ is an isomorphism.

- (b) (\mathbb{Q}^+, \cdot) are positive rational numbers with multiplication. $(\mathbb{Q}^+, *)$ are positive rational numbers with the operation $*$ defined by:

$$a * b = \frac{a \cdot b}{2}.$$

The map $g : \mathbb{Q}^+ \rightarrow \mathbb{Q}^+$ is given by:

$$g(a) = 2a.$$

Determine whether $g : (\mathbb{Q}^+, \cdot) \rightarrow (\mathbb{Q}^+, *)$ is an isomorphism.

Sample Solutions

1. (a). We first prove it for $n \geq 0$. We proceed by induction on n .

Base Step: $m = 0$. Then $a^{m+0} = a^m = a^m * e = a^m * a^0$. Induction Step: Assume $a^{m+n} = a^m * a^n$. Then

$$a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n} * a = a^m * a^n * a = a^m * a^{n+1}.$$

The second equality here follows from the definition of $a^{(m+n)+1}$, the third equality follows from the induction hypothesis, and the last equality follows from the definition of a^{n+1} . This proves the formula for $n \geq 0$.

Now assume that $n < 0$. We first observe that

$$a^{-n} * a^n = e. \tag{1}$$

Because $-n$ is positive, we can apply the instance of the formula we proved above. We get: $a^n * a^{-n} = a^{n+(-n)} = a^0 = e$. But since $(G, *)$ is a group, we see that a^{-n} is the inverse to a^n , so $a^{-n} * a^n = e$ as well. Now again by the instance of the formula proved above,

$$a^{m+n} * a^{-n} = a^{m+n+(-n)} = a^m.$$

Now multiply this equation by a^n from the right; you get

$$a^{m+n} * a^{-n} * a^n = a^m * a^n.$$

From (1) we then get $a^{m+n} = a^m * a^n$. This completes the proof.

(b). We first prove it for $n \geq 0$. We proceed by induction on n .

Base Step: $m = 0$. Then $a^{m \cdot 0} = a^0 = e = (a^m)^0$. Induction Step: Assume $a^{m \cdot n} = (a^m)^n$. Then

$$a^{m \cdot (n+1)} = a^{(m \cdot n) + m} = a^{m \cdot n} * a^m = (a^m)^n * a^m = (a^m)^{n+1}.$$

This proves the formula for $n \geq 0$.

Now assume that $n < 0$. Then $|n| = -n$ and $-|n| = n$, and we have

$$(a^m)^n = (a^m)^{-|n|} = ((a^m)^{-1})^{|n|} = (a^{-m})^{|n|} = a^{-m \cdot |n|} = a^{m \cdot (-|n|)} = a^{m \cdot n}.$$

The second equality follows from the definition of a^n for negative n , the third equality follows from the observation we made in the proof of (a) that a^{-m} is the inverse to a^m and the fourth equality follows from the instance of our formula we proved above for nonnegative n . This completes the proof.

2. We have to verify three things:

- f is injective;
- f is surjective;
- f has the homomorphism property.

Injectivity. We have to show for every $x, y \in G$: $f(x) = f(y) \Rightarrow x = y$. So assume $f(x) = f(y)$. Thus,

$$g^{-1} * x * g = g^{-1} * y * g.$$

By the left cancellation law, it follows that

$$x * g = y * g.$$

By the right cancellation law, we then get $x = y$. This proves the injectivity of f .

Surjectivity. We have to show that for every $y \in G$ there is some $x \in G$ such that $y = f(x)$, i.e. $y = g^{-1} * x * g$. The element x can be found by solving this equation. Assuming that

$$y = g^{-1} * x * g,$$

we multiply this equation by g from the left and get:

$$g * y = g * g^{-1} * x * g = e * (x * g) = x * g,$$

So $g * y = x * g$. Now we multiply this equation by g^{-1} from the right, and obtain

$$g * y * g^{-1} = x * g * g^{-1} = x * e = x.$$

Then $x = g * y * g^{-1}$. Indeed,

$$f(x) = g^{-1} * g * y * g^{-1} * g = e * y * e = y.$$

Homomorphism property. Let $x, y \in G$. Then

$$f(x) * f(y) = g^{-1} * x * g * g^{-1} * y * g = g^{-1} * x * e * y * g = g^{-1} * x * y * g = f(x * y).$$

Since f has all three properties, f is an isomorphism.

3. We use the lemma from the lecture which says that if a is a generator of a cyclic group $(H, *)$ and $a^s = e$ for some $s \in \mathbb{Z}$ then $H = \{e, a, a^2, \dots, a^{s-1}\}$.

(a). We compute the “powers” 10^i in $(\mathbb{Z}_{12}, +_{12})$.

$$\begin{aligned} 10^1 &= 10 \\ 10^2 &= 10 +_{12} 10 = 8 \\ 10^3 &= 8 +_{12} 10 = 6 \\ 10^4 &= 6 +_{12} 10 = 4 \\ 10^5 &= 4 +_{12} 10 = 2 \\ 10^6 &= 2 +_{12} 10 = 0. \end{aligned}$$

Thus, $\langle 10 \rangle = \{0, 2, 4, 6, 8, 10\}$.

(b). We compute the “powers of A ” in $\text{GL}(2, \mathbb{C})$.

$$\begin{aligned} A^1 &= \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \\ A^2 &= \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \\ A^3 &= \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ i & 0 \end{pmatrix} \\ A^4 &= \begin{pmatrix} 0 & -1 \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ A^5 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -1 & 0 \end{pmatrix} \\ A^6 &= \begin{pmatrix} 0 & -i \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} \\ A^7 &= \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix} \\ A^8 &= \begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e \end{aligned}$$

Thus,

$$\langle A \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ i & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 0 & -i \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

4. In either case, we check the properties injectivity, surjectivity and homomorphism property apply to the map in question.

(a). Injectivity. We need to check whether $f(x) = f(y) \Rightarrow x = y$. So let $x, y \in \mathbb{C}$. Thus x and y are of the form $x = a + bi$ and $y = c + di$ for some $a, b, c, d \in \mathbb{R}$. Assume $f(x) = f(y)$, so $f(a + bi) = f(c + di)$. By the definition of f , we have

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}.$$

This means that $a = c$ and $b = d$, so $x = a + bi = c + di = y$. So f is injective.

Surjectivity. Let $A \in \mathcal{M}$ be arbitrary. We have to check whether $A = f(x)$ for some $x \in \mathbb{C}$. But if

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

for some $a, b \in \mathbb{R}$, then $A = f(a + bi)$ by the definition of f , so it suffices to set $x = a + bi$ and $f(x) = A$. So f is surjective.

Homomorphism property. Let $x, y \in \mathbb{C}$ be arbitrary, say $x = a + bi$ and $y = c + di$ for some $a, b, c, d \in \mathbb{R}$. Then:

$$f(x \cdot y) = f((a + bi) \cdot (c + di)) = f((ac - bd) + (ad + bc)i) = \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix}$$

and

$$f(x) \cdot f(y) = f(a + bi) \cdot f(c + di) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix}.$$

Thus, $f(x \cdot y) = f(x) \cdot f(y)$, so f has the homomorphism property. Since f has all three properties, f is an isomorphism.

(b). As before, we check whether g is injective, surjective and has the homomorphism property.

Injectivity. Assume $g(x) = g(y)$ for some $x, y \in \mathbb{Q}^+$. This means that $2x = 2y$, so $x = y$. Hence, g is injective.

Surjectivity. Now let $y \in \mathbb{Q}^+$ be arbitrary. We check whether $y = f(x)$ for some $x \in \mathbb{Q}^+$. But if $x = y/2$ then $g(x) = 2x = 2 \cdot (y/2) = y$, so such an x exists. So g is surjective.

Homomorphism Property. Let $x, y \in \mathbb{Q}^+$ be arbitrary. Then

$$g(x \cdot y) = 2xy$$

and

$$g(x) * g(y) = \frac{g(x) \cdot g(y)}{2} = \frac{2x \cdot 2y}{2} = 2xy.$$

Thus, $g(x \cdot y) = g(x) * g(y)$, so g has the homomorphism property. Since g has all three properties, g is an isomorphism.