Midterm 1

Abstract Algebra 1

MATH 3140

Fall 2022

Friday September 23, 2022

NAME: ______________________________

PRACTICE EXAM

SOLUTIONS

Question:	**1**	**2**	**3**	**4**	**5**	Total
Points:	20	20	20	20	20	100
Score:						

- The exam is closed book. You **may not use any resources** whatsoever, other than paper, pencil, and pen, to complete this exam.
- You **may not discuss the exam** with anyone except me, in any way, under any circumstances.
- You **must explain your answers**, and you will be **graded on the clarity of your solutions**.
- You must upload your exam as a single **.pdf** to **Canvas**, with the questions in the correct order, etc.
- You have 45 minutes to complete the exam.

1. • Consider the following subset of real 2×2 matrices:

$$H := \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \right\} \subseteq \mathrm{M}_2(\mathbb{R}).$$

(a) (10 points) *Show that matrix multiplication defines a binary operation on H.*

SOLUTION

Solution. We must show that for all $A, B \in H$, we have $AB \in H$. To this end, let $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Then we have $AB = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$ so that $AB \in H$. □

(b) (10 points) *Does the map (or "function") $\phi : H \to \mathbb{R}$, given by*

$$\phi\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right) = a,$$

give an isomorphism of the binary structure $\langle H, \cdot \rangle$ (here $\cdot$ denotes matrix multiplication) with the binary structure $\langle \mathbb{R}, + \rangle$? Explain.

SOLUTION

Solution. Yes, ϕ gives an isomorphism of $\langle H, \cdot \rangle$ with $\langle \mathbb{R}, + \rangle$.

First we will show that given $A, B \in H$, we have $\phi(AB) = \phi(A) + \phi(B)$. To this end, let $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Then we have

$$\phi(AB) = \phi\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right) = \phi\left(\begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}\right) = a + b = \phi(A) + \phi(B).$$

Next we will show that ϕ is bijective (or "one-to-one and onto"). To show it is injective (or "one-to-one"), let $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Then if $\phi(A) = \phi(B)$, this means that $a = b$, so that $A = B$.

To show ϕ is surjective (or "onto"), let $a \in \mathbb{R}$. Then $\phi\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right) = a$, so that ϕ is surjective (or "onto"). $\square$

1
20 points

2. (20 points) • Suppose that $\langle G, * \rangle$ is a binary structure such that:

1. The binary operation $*$ is associative.
2. There exists a **left** identity element; i.e., there exists $e \in G$ such that for all $g \in G$, we have $e * g = g$.
3. **Left** inverses exist; i.e., for all $g \in G$, there exists $g^{-1} \in G$ such that $g^{-1} * g = e$.

Show that $\langle G, * \rangle$ is a group.

SOLUTION

Solution. For brevity, I am going to drop the $*$ in what follows. Let $g \in G$, and let g^{-1} be a left inverse of g. Then we have $g^{-1}g = e$, which, multiplying on the right by g^{-1}, gives

$$\begin{aligned} (g^{-1}g)g^{-1} &= eg^{-1} \\ (g^{-1}g)g^{-1} &= g^{-1} && \text{(Def. of left id.)} \end{aligned}$$

Now let $(g^{-1})^{-1}$ be a left inverse of g^{-1}. Multiplying both sides of the equation above on the left by $(g^{-1})^{-1}$ we obtain:

$$\begin{aligned} (g^{-1})^{-1}(g^{-1}g)g^{-1} &= (g^{-1})^{-1}g^{-1} \\ ((g^{-1})^{-1}g^{-1})gg^{-1} &= e && \text{(Assoc., and def. of left inv.)} \\ egg^{-1} &= e && \text{(Def. of left inv.)} \\ gg^{-1} &= e && \text{(Def. of left id.)} \end{aligned}$$

In other words, the left inverse g^{-1} of g is also a right inverse of g.

Finally, multiplying the last equation above, i.e., $gg^{-1} = e$, on the right by g, we have

$$\begin{aligned} (gg^{-1})g &= eg \\ g(g^{-1}g) &= g && \text{(Assoc., and def. of left id.)} \\ ge &= g && \text{(Def. of left inv.)} \end{aligned}$$

so that e is also a right identity.

In conclusion, we have shown that the binary structure $\langle G, * \rangle$ satisfies:

1. The binary operation $*$ is associative.
2. There exists an identity element; i.e., there exists $e \in G$ such that for all $g \in G$, we have $e * g = g * e = g$.
3. Inverses exist; i.e., for all $g \in G$, there exists $g^{-1} \in G$ such that $g^{-1} * g = g * g^{-1} = e$.

Therefore, $\langle G, * \rangle$ is a group. $\square$

2
20 points

3. (20 points) • Let H be a subgroup of a group G. For $a, b \in G$, let $a \sim b$ if and only if $a^{-1}b \in H$. *Show that $\sim$ is an equivalence relation on G.*

SOLUTION

Solution. We must show that $\sim$ is reflexive, symmetric, and transitive:

1. (Reflexive) We must show that for all $a \in G$, we have $a \sim a$. So let $a \in G$. We have $a^{-1}a = e \in H$, so that $a \sim a$.
2. (Symmetric) We must show that for all $a, b \in G$, if $a \sim b$, then $b \sim a$. So let $a, b \in G$, with $a \sim b$. Then by definition we have $a^{-1}b \in H$. Since H is a subgroup, it is closed under taking inverses, so that we have $(a^{-1}b)^{-1} \in H$. But $(a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a$, so that $b \sim a$.
3. (Transitive) We must show that for all $a, b, c \in G$, we have $a \sim b$ and $b \sim c$ implies that $a \sim c$. So let $a, b, c \in G$, and assume that $a \sim b$ and $b \sim c$. That is to say, $a^{-1}b \in H$ and $b^{-1}c \in H$. Since H is a subgroup, it is closed under the binary operation, so that $(a^{-1}b)(b^{-1}c) \in H$. But $(a^{-1}b)(b^{-1}c) = a^{-1}ec = a^{-1}c$, so that $a \sim c$.

This completes the proof. $\square$

3
10 points

4. (a) (10 points) • *In the group $\mathbb{Z}_{28}$, what is the order of the subgroup generated by the element 18?*

SOLUTION:

$$\boxed{\text{The order of the subgroup generated by 18 is 14.}}$$

We have seen that for a nonzero element $m \in \mathbb{Z}_n$, the order of the group $\langle m \rangle$ is equal to $n/\gcd(n, m)$. Since $\gcd(28, 18) = 2$, we have that the order of the group $\langle 18 \rangle$ is equal to 14.

(b) (10 points) *How many generators are there for the group $\mathbb{Z}_{28}$?*

SOLUTION:

$$\boxed{\text{There are 12 generators for the group } \mathbb{Z}_{28}.}$$

The generators are given by the numbers in $\{0, \ldots, 27\}$ that are co-prime to 28. These are exactly the odd numbers (14 of these) that are not divisible by seven (7 and 21). To be explicit, the generators are $\{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$.

4
20 points

5. • **TRUE** or **FALSE**. For this problem, and this problem only, **you do not need to justify your answer**.

(a) (4 points) **TRUE** or **FALSE** (circle one). Every subgroup of a cyclic group is cyclic.

SOLUTION: TRUE. We proved this as a theorem in class.

(b) (4 points) **TRUE** or **FALSE** (circle one). If H and H' are subgroups of a group G, then $H \cap H'$ is a subgroup of G.

SOLUTION: TRUE. We have $e \in H \cap H'$, so let $a, b \in H \cap H'$. Then $ab^{-1} \in H$ and $ab^{-1} \in H'$, so $ab^{-1} \in H \cap H'$. It follows that $H \cap H'$ is a subgroup.

(c) (4 points) **TRUE** or **FALSE** (circle one). If $*$ is an associative binary operation on a set S, then for all $a, b, c \in S$, we have $(a * b) * c = c * (a * b)$.

SOLUTION: FALSE. For example, in $\mathrm{GL}_2(\mathbb{R})$ with matrix multiplication, we can take $b = I$ and then let a and c be noncommuting matrices. (For reference, a binary operation $*$ on a set S is associative if for all $a, b, c \in S$, we have $(a * b) * c = a * (b * c)$.)

(d) (4 points) **TRUE** or **FALSE** (circle one). Every finite group of at most 3 elements is abelian.

SOLUTION: TRUE. You can check this by writing out the group table, for instance (see, e.g., p.44–5 of Fraleigh).

(e) (4 points) **TRUE** or **FALSE** (circle one). Every subgroup of an infinite group is infinite.

SOLUTION: FALSE. For any infinite group G, consider the trivial subgroup $\{e\} \leq G$. Or, a little more interesting: consider the subgroup $\{\pm I\} \leq \mathrm{GL}_n(\mathbb{R})$, or the subgroup of n-th roots of unity in $\mathbb{C}^*$ for some natural number $n > 0$.

5
20 points