Midterm

Abstract Algebra 1

MATH 3140

Summer 2021

Monday June 14, 2021

NAME: ____

PRACTICE EXAM

SOLUTIONS

Question:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	Total
Points:	20	20	10	10	20	10	10	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 90 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 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 must 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 must show that ϕ is one-to-one and onto. To show it is 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 onto, let $a \in \mathbb{R}$. Then $\phi\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right) = a$, so that ϕ is 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 $gg^{-1} = e$ 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. (10 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. □

3
10 points

4. (a) (5 points) • *In the group $\mathbb{Z}_{28}$, what is the order of the subgroup generated by the element 18?*

SOLUTION:

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

SOLUTION:

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
10 points

5. (a) (5 points) • *Is the permutation* $\sigma = (1,6,4)(2,5) \in S_6$ *even or odd?*

SOLUTION:

σ is odd.

We have

$$\sigma = (1,6,4)(2,5) = (1,6)(6,4)(2,5)$$

is the product of an odd number of transpositions.

(b) (5 points) *Is the permutation* σ^2 *even or odd?*

SOLUTION:

σ^2 is even.

The square of any permutation is even.

(c) (5 points) *Compute* $|\sigma|$*; i.e., the order of* σ *in* S_6.

SOLUTION:

$|\sigma| = 6$

The order of $(1,6,4)$ is 3 and the order of $(2,5)$ is 2. As σ is equal to the product of these disjoint cycles, it follows that $|\sigma| = \text{lcm}(3,2) = 6$.

(d) (5 points) *With* σ *as above and* $\tau = (5,3,2)$*, compute* $\sigma\tau$ *(as a product of disjoint cycles).*

SOLUTION:

$\sigma\tau = (1,6,4)(3,5)$

We have

$$\sigma\tau = (1,6,4)(2,5)(5,3,2) = (1,6,4)(3,5).$$

5
20 points

6. • Let A be a set, and let $G \leq S_A$ be a subgroup of the group of permutations S_A of A. For an element $a \in A$, define $G_a := \{\sigma \in G : \sigma(a) = a\}$.

(a) (5 points) *For $a \in A$, show that G_a is a subgroup of G.*

SOLUTION

Solution. Certainly we have $e \in G_a$ so that G_a is nonempty. Now if $\sigma, \tau \in G_a$, then $(\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$, so that $\sigma\tau \in G_a$. Finally, if $\sigma \in G_a$, I claim that $\sigma^{-1}(a) = a$, so that $\sigma^{-1} \in G_a$. Indeed, $\sigma(a) = a$, so that applying σ^{-1} to both sides we obtain $\sigma^{-1}(\sigma(a)) = \sigma^{-1}(a)$. Focusing on the left hand side, we have $\sigma^{-1}(\sigma(a)) = (\sigma^{-1}\sigma)(a) = e(a) = a$, proving the claim. Thus G_a is a subgroup. □

(b) (5 points) Let $a, b \in A$, and suppose there exists $\sigma \in G$ such that $b = \sigma(a)$. *Show that G_a and G_b have the same cardinality.*

SOLUTION

Solution. Let $a, b \in A$, and suppose there exists $\sigma \in G$ such that $b = \sigma(a)$. Note that this also implies that $\sigma^{-1}(b) = a$. I claim there is a one-to-one and onto function

$$f : G_a \longrightarrow G_b, \quad \tau \mapsto \sigma\tau\sigma^{-1}.$$

First, let us check this function is well-defined; i.e., that $\sigma\tau\sigma^{-1} \in G_b$. To this end, suppose $\tau \in G_a$. Then $(\sigma\tau\sigma^{-1})(b) = \sigma(\tau(\sigma^{-1}(b)) = \sigma(\tau(a)) = \sigma(a) = b$. Thus $\sigma\tau\sigma^{-1} \in G_b$.

Now let us check that f is one-to-one and onto by constructing an inverse function

$$f^{-1} : G_b \longrightarrow G_a, \quad \mu \mapsto \sigma^{-1}\mu\sigma.$$

The same argument above shows this function is well-defined. Now observe that $f^{-1}f(\tau) = f^{-1}(\sigma\tau\sigma^{-1}) = \sigma^{-1}(\sigma\tau\sigma^{-1})\sigma = \tau$, and $ff^{-1}(\mu) = \sigma(\sigma^{-1}\mu\sigma)\sigma^{-1} = \mu$. Thus f^{-1} is the inverse function of f, and so f is one-to-one and onto. Thus, by definition, the cardinality of G_a is the same as the cardinality of G_b. □

6
10 points

7. (10 points) • Let H be a subgroup of a group G, and let $a, b \in G$.

TRUE or **FALSE**: *If $aH = bH$, then $Ha^{-1} = Hb^{-1}$.*

SOLUTION

Solution. This is TRUE. Recall that $aH = bH$ if and only if $b^{-1}a \in H$, and similarly, $Ha = Hb$ if and only if $ab^{-1} \in H$. Applying this second condition to Hb^{-1} and Ha^{-1}, we see that $Hb^{-1} = Ha^{-1}$ if and only if $b^{-1}(a^{-1})^{-1} \in H$; or, in other words, if and only if $b^{-1}a \in H$. In other words, $aH = bH \iff b^{-1}a \in H \iff Hb^{-1} = Ha^{-1}$. □

Alternate Solution. This is TRUE. Indeed, suppose that $aH = bH$. Then we have that $b = ah$ for some $h \in H$. It follows that $Hb^{-1} = H(ah)^{-1} = Hh^{-1}a^{-1} = Ha^{-1}$. □

7
10 points