Math 31 - Midterm Exam Solutions

July 23, 2013

Name: ____

Instructions: This is a closed-book exam. You may not use your textbook, notes, or written materials of any kind. No help will be given or received. You will have 50 minutes to complete this exam. Please write clearly and explain yourself thoroughly whenever necessary.

Honor statement:

I have neither given nor received any help on this exam, and I attest that all of the answers are my own work.

____

Signature

Question	Points	Score
1	20	
2	14	
3	15	
4	10	
5	11	
Total	70	

1. Definitions and theorems. Give a precise statement of each of the following definitions and theorems. Explain yourself thoroughly, and use complete sentences. Each part is worth five (5) points.

(a) Give the definition of a **group**. (Be sure to define any other terms that you use.)

> A **group** is a nonempty set G together with a **binary operation** $* : G \times G \to G$ (i.e., a function which takes an ordered pair of elements in G to another element of G) satisfying:
>
> 1. **Associativity:** For all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.
> 2. **Identity:** There is an element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.
> 3. **Inverses:** For each $a \in G$, there exists $a^{-1} \in G$ satisfying $a * a^{-1} = a^{-1} * a = e$.

(b) Define what it means for a group to be **abelian**.

> A group is **abelian** if its binary operation is commutative. That is, $a*b = b*a$ for all $a, b \in G$.

(c) State **Lagrange's theorem**.

> **Lagrange's Theorem:** Let G be a finite group, and let H be a subgroup of G. Then $|H|$ divides $|G|$.

(d) Complete the following theorem:

Theorem. *Let $G = \langle a \rangle$ be a finite cyclic group of order n. Then for any integer m,*

$$o(a^m) = \frac{n}{\gcd(n, m)}.$$

2. True/false. Mark each statement as "true" or "false." No justification is required. Each part is worth two (2) points.

(a) The operation $a * b = a/b$ for $a, b \in \mathbb{R}$ defines a binary operation on $\mathbb{R}$.

> **False**. (The operation is undefined when $b = 0$.)

(b) If G is a cyclic group, every element of G is a generator for G.

> **False**. (For example, 1 generates $\mathbb{Z}_4$, but 2 does not.)

(c) Every subset of a group is a subgroup.

> **False**.

(d) Every abelian group is cyclic.

> **False**. (We saw that the Klein 4-group is a counterexample.)

(e) If G is a finite cyclic group and m is a positive divisor of $|G|$, then G contains an element of order m.

> **True**.

(f) If G is a finite group and m is a positive divisor of $|G|$, then G contains an element of order m.

> **False**. (If G is a non-cyclic finite group of order n, there is no element of order n.)

(g) In any group G, $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

> **False**. (The actual formula is $(ab)^{-1} = b^{-1}a^{-1}$, and the two coincide if G is abelian.)

3. Examples. For each of the following statements, either provide an example with the given property, or explain why no such example exists. Each part is worth five (5) points.

(a) A one-to-one function from the set $\{1, 2, 3, 4\}$ to itself which is not onto.

Solution. No such example can exist. A one-to-one function must have a distinct output for each input. Therefore, a one-to-one function $f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ must take four different values. These are all the possible values, so the function is necessarily onto.

(b) A non-cyclic group in which every proper subgroup is cyclic.

Solution. We have seen that the Klein 4-group V_4 is an example, since every proper subgroup has order 1 or 2 (and is thus cyclic). Another example would be D_3 (every proper subgroup has order 1, 2, or 3).

(c) An equivalence relation $\sim$ on $\mathbb{R} - \{0\}$ for which every equivalence class contains exactly two elements.

Solution. Define $a \sim b$ if and only if $a = -b$. Equivalently, $a \sim b$ if and only if $|a| = |b|$. This is an equivalence relation, and the equivalence classes each have two elements:

$$[a] = \{a, -a\}.$$

Another possibility would be $a \sim b$ if and only if $a = 1/b$. Then the classes are

$$[a] = \{a, 1/a\}.$$

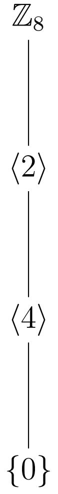
4. Short answer. Answer the following two questions. A proof is not necessary, but you should give some justification for each part. Each question is worth five (5) points.

(a) Consider the cyclic group $\mathbb{Z}_8$. Determine all the subgroups of this group, and draw its subgroup lattice.

Solution. Since $\mathbb{Z}_8$ is cyclic, each divisor of 8 yields a unique subgroup of that order. The divisors are 1, 2, 4, and 8, and the corresponding subgroups are

$$\begin{aligned}\langle 0\rangle &= \{0\}\\ \langle 4\rangle &= \{0,4\}\\ \langle 2\rangle &= \{0,2,4,6\}\\ \langle 1\rangle &= \mathbb{Z}_8\end{aligned}$$

Therefore, the subgroup lattice looks like:



(b) Let $G = \{e, a, b, c, d, f\}$. The following Cayley table partially defines a binary operation on G. Complete the table in such a way that $\langle G, *\rangle$ becomes an abelian group.

$*$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	f	c	e	a	d
c	c	d	e	b	f	a
d	d	c	a	f	b	e
f	f	b	d	a	e	c

5. Proof: Give a formal proof of the statement in part (a). Explain all of your arguments properly and thoroughly.

(a) [8 points] Let G be a group. If G is abelian and

$$H = \left\{a \in G : a^2 = e\right\},$$

prove that H is a subgroup of G.

Proof. To check that $H \leq G$, we need to verify that H is closed, the identity belongs to H, and that H is closed under taking inverses. First observe that if $a, b \in H$, then

$$(ab)^2 = abab = aabb = a^2b^2$$

since G is abelian. But $a^2 = b^2 = e$, so $(ab)^2 = e$, and $ab \in H$. Therefore, H is closed. Next, if $e \in G$ denotes the identity element of G, we have $e^2 = e$, so $e \in H$. Finally, note that if $a \in H$, then $a^2 = e$, so $a = a^{-1}$. Thus every element of H is equal to its own inverse, and $a^{-1} = a \in H$ for all $a \in H$. Therefore, H is a subgroup of G. □

(b) [3 points] Give an example of a nonabelian group G for which the set H given above is **not** a subgroup.

Solution. The simplest example is D_3. In this group,

$$H = \{i, m_1, m_2, m_3\},$$

which is not a subgroup. It is not closed, since the composition of two reflections is a rotation. (Also, if H were a subgroup, it would violate Lagrange's theorem.

Another example is the group $\mathrm{GL_n}(\mathbb{R})$. If we let

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

then $A, B \in H$, but

$$AB = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

is not.