Name: Solutions

Modern Algebra I: Group Theory Midterm Exam

1. Group Fundamentals. Be sure to write precise proofs and justify each of your steps.

   a. Write a precise mathematical definition for group: [5 points]

A group is a set G with a binary operation $\cdot : G \times G \to G$ s.t

associativity (1) For all $a,b,c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

identity (2) There exists an $e \in G$ s.t $a \cdot e = a = e \cdot a$ for all $a \in G$.

inverse (3) For all $a \in G$ there exists an $a^{-1} \in G$ s.t $a \cdot a^{-1} = e = a^{-1} \cdot a$.

   b. Let $(G,\cdot)$ be a group and $a \in G$. Use the definition of group to prove that $a \cdot a = a$ if and only if a is the identity of G. [5 points]

($\Longrightarrow$) Suppose $a \cdot a = a$. Then

$$a^{-1}(a \cdot a) = a^{-1}a$$
$$(a^{-1} \cdot a) \cdot a = e$$
$$e \cdot a = e$$
$$a = e \quad \blacksquare$$

($\Longleftarrow$) Suppose $a = e$. Then $a \cdot a = e \cdot e = e = a$. $\blacksquare$

   c. State and prove (using the definition of group) the cancellation law. [5 points]

Let $a,b,c \in G$ and suppose $ab = ac$. Then $b = c$.

Proof:

$ab = ac$	
$a^{-1}(ab) = a^{-1}(ac)$	inverses
$(a^{-1}a)b = (a^{-1}a)c$	associativity
$eb = ec$	inverses
$b = c$	identity

$\blacksquare$

Name:_____

2. Determine if each of the following statements is true or false. Give a counterexample for each false statement. [13 points]

a. The center of a group must be abelian. True

b. The centralizer of a group element must be abelian. False: $C_{D_3}(e) = D_3$, which is not abelian

c. If a subgroup of a group is abelian, then the larger group is abelian. False
C_3 (abelian) is a subgroup of D_3 (not abelian)

d. D_3 is isomorphic to $(\mathbb{Z}_{14}^{\times}, \cdot_{14})$. False – D_3 is not abelian, $(\mathbb{Z}_{14}^{\times}, \cdot_{14})$ is

e. $(\mathbb{Z}, +)$ is isomorphic to $(n\mathbb{Z}, +)$. True

f. If $ab = ca$ in a group, then $b = c$. False.

g. There is essentially one group of order three. True.

h. There is essentially one group of order four. False: C_4 and V_4 both have 4 elements but are not isomorphic

Name:_____

3. Give an example of each of the following (or explain why one does not exist): [7 points + 2 bonus]

   a. An infinite group that is not commutative. $GL_2(\mathbb{R})$ w/ matrix mult.

   b. A finite group that is commutative. V_4 w/ composition

   c. Two subgroups (of the same group) that are not isomorphic to each other even though they have the same number of elements.

   in D_4: $\{e, R, R^2, R^3\}$ $\{e, R^2, RF, FR\}$

   d. *Bonus*: a binary operation that is commutative but not associative.

   $\text{average}(a,b) = \frac{a+b}{2}$

4. For each of the following, prove or disprove that it is a group. You may assume that the operations are associative. [15 points]

   a. The set {-2, 0, 2} with regular addition.

   no; 2+2=4, so the set is not closed
   group

   b. The set {-1, 0, 1} with regular multiplication.

   no; 0 has no inverse
   group

   c. The set {-1, 1} with regular multiplication.

·	1	-1
1	1	-1
-1	-1	1

closure ✓
associativity ✓
identity ✓
inverse ✓

Name:_____

5. This problem involves the concept of subgroup: [20 points]

a. Write a precise mathematical definition for subgroup.

A subgroup of a group $(G,\cdot)$ is a subset H of G that is a group with respect to the same operation.

b. Prove that $(n\mathbb{Z},+), n \in \mathbb{N}$, is a subgroup of $(\mathbb{Z},+)$.

By the subgroup test, we need only check closure and inverses:

① closure: let $a,b \in n\mathbb{Z}$. Then $a=nk, b=n\ell$ where $k,\ell \in \mathbb{Z}$.

Then $a+b=nk+n\ell=n(k+\ell) \in n\mathbb{Z}$ since $k+\ell \in \mathbb{Z}$.

② inverse: let $a \in n\mathbb{Z}$. Then $a=nk \Rightarrow -a=-nk=n(-k) \in n\mathbb{Z}$ since $-k \in \mathbb{Z}$.

$\therefore (n\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$. ▩

c. Let G be a group, and let $a \in G$. Show that the centralizer of a, $C_G(a) = \{g \in G : ag = ga\}$, is a subgroup of G.

Subgroup test:

① closure: let $x,y \in C_G(a) \iff ax=xa, ay=ya$.

Then $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$.

($ya=ay$ since $y \in C_G(a)$; $xa=ax$ since $x \in C_G(a)$)

$\therefore xy \in C_G(a)$.

② inverses: let $x \in C_G(a) \iff ax=xa$

$x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1}$

$(x^{-1}a)(xx^{-1}) = (x^{-1}x)(ax^{-1})$

$(x^{-1}a)e = e(ax^{-1})$

$x^{-1}a = ax^{-1}$

$\therefore x^{-1} \in C_G(a)$ ▩

Name:_____

6. Let $(G,\cdot)$ and $(H,*)$ be groups and $\phi: G \to H$ an isomorphism: [20 points]

a. Write a precise mathematical definition for isomorphism.

An isomorphism is a bijective function $\phi: G \to H$ (groups) s.t $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

b. Let e_G be the identity of G and e_H the identity of H. Prove that $\phi(e_G) = e_H$.

$\phi(e_G) = \phi(e_G \cdot e_G) = \underbrace{\phi(e_G)}_{\in H} * \underbrace{\phi(e_G)}_{\in H}$

So $\phi(e_G) = \phi(e_G)\phi(e_G)$

$\Rightarrow e_H = \phi(e_G)$ by the cancellation law on H. ▩

c. Let $a, b \in G$. Prove that if a is the inverse of b, then $\phi(a)$ is the inverse of $\phi(b)$.

a is the inverse of $b \Rightarrow ab = e_G = ba$

Then $\phi(ab) = \phi(e_G) = e_H$ (by (b))

On the other hand, $\phi(ab) = \phi(a)\phi(b)$.

$\Rightarrow \phi(a)\phi(b) = e_H$. Proceed similarly to show $\phi(b)\phi(a) = e_H$.

$\therefore \phi(a)$ is the inverse of $\phi(b)$. ▩

d. Let $a \in G$. Prove that if $|a| = 2$ then $|\phi(a)| = 2$.

$|a| = 2 \Rightarrow a^2 = e_G$.

So $\phi(a^2) = \phi(e_G) = e_H$.

On the other hand, $\phi(a^2) = \phi(a \cdot a) = \phi(a)\phi(a) = \phi(a)^2$.

$\Rightarrow \phi(a)^2 = e_H$.

To show that $|\phi(a)| = 2$, we need to show that 2 is the smallest n for which this is possible. But if $n = 1$ then $\phi(a) = e_H \Rightarrow e_G = a \Rightarrow |a| = 1$, a contradiction. $\therefore |\phi(a)| = 2$. ▩

Name:_____

7. Prove or disprove that the following groups are isomorphic: [15 points]

a. V_4 (the symmetries of a non-square rectangle with composition) and $(\mathbb{Z}_{12}^{\times}, \cdot_{12})$.

$V_4 = \{e, R, F, RF\}$ $\quad$ $\mathbb{Z}_{12}^{\times} = \{1, 5, 7, 11\}$

V_4	e	R	F	RF
e	e	R	F	RF
R	R	e	RF	F
F	F	RF	e	R
RF	RF	F	R	e

$\mathbb{Z}_{12}^{\times}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Define ϕ: $\begin{cases} e \leftrightarrow 1 \\ R \leftrightarrow 5 \\ F \leftrightarrow 7 \\ RF \leftrightarrow 11 \end{cases}$ ϕ is clearly a bijection, and (by the operation tables) preserves the operations

b. $(\mathbb{R}_{>0}, \cdot)$ and $(\mathbb{R}, +)$.

Define a map $\phi: (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$

ϕ is injective (one-one): Suppose $\phi(x) = \phi(y)$.

$\Rightarrow e^x = e^y \Rightarrow \ln e^x = \ln e^y \Rightarrow x = y$. ✓

ϕ is surjective (onto): Let $t \in \mathbb{R}_{>0}$. Then $\ln t \in \mathbb{R}$.

$\phi(\ln t) = e^{\ln t} = t$. ✓

ϕ is operation preserving: $\phi(a+b) = e^{a+b} = e^a \cdot e^b$

$= \phi(a) \cdot \phi(b)$ ✓