MTH 4441 Test #1 - Solutions

FALL 2017

Pat Rossi Name _____

Part #1 - Definitions and Theorems

Express the definitions and statements of the theorems CLEARLY

1. Define **Group**

   Let G be a set and let $*$ be a binary operation defined on the elements of G. Then $(G, *)$ is a group exactly when the following conditions hold:

   i. G is **closed** under $*$. (i.e. $x * y \in G$, $\forall x, y \in G$)

   ii. $*$ is **associative.** (i.e. $(x * y) * z = x * (y * z)$, $\forall x, y, z \in G$)

   iii. G has an identity element e. (i.e., $\exists\ e \in G$ such that $x * e = e * x$, $\forall x \in G$.)

   iv. Each element $x \in G$ has an inverse x^{-1}, such that $x * x^{-1} = e = x^{-1} * x$

2. Define **isomorphism, isomorphic**

   A function $\phi : (G_1, *_1) \to (G_2, *_2)$ is an **isomorphism** if:

   (a) $\phi : G_1 \to G_2$ is one-to-one and onto

   and

   (b) $\phi(a *_1 b) = \phi(a) *_2 \phi(b)$, $\forall a, b \in G_1$

   If such an isomorphism exists, then $(G_1, *_1)$ and $(G_2, *_2)$ are said to be **isomorphic.**

3. Define **congruent (congruence) modulo** n.

   Let $n \geq 2$ be a natural number. Then integers x and y are **congruent modulo** n, denoted $x \equiv y \pmod{n}$, exactly when $x - y = kn$, for some integer k. (i.e., $x \equiv y \pmod{n}$ exactly when $x - y$ is a multiple of n.)

   Alternatively:

   Let $n \geq 2$ be a natural number. Then integers x and y are **congruent modulo** n, denoted $x \equiv y \pmod{n}$, exactly when x and y have the same "proper remainder" (i.e., $r \in \{0, 1, 2, \ldots, n-1\}$) when divided by n.

4. Define **cyclic subgroup.**

   Let $a \in (G, *)$. The **cyclic subgroup** generated by a, denoted $\langle a \rangle$, is the smallest subgroup of $(G, *)$ that contains both a and a^{-1}.

   If $(H, *)$ is a cyclic subgroup of $(G, *)$, generated by a, then we write $(H, *) = \langle a \rangle$.

   If $(G, *) = \langle a \rangle$, then we say that $(G, *)$ is a **cyclic group** generated by a.

5. Name five properties of groups that are preserved by isomorphisms

   Some possibilities include:

   (a) **Cardinality -** (Isomorphic groups have the "same number of elements")

      1. If G_1 is finite and contains n elements, then G_1 is finite and contains n elements.
      2. If G_1 is countably (denumerably) infinite, then G_2 is countably (denumerably) infinite.
      3. If G_1 is uncountably (non-denumerably) infinite, then G_2 is uncountably (non-denumerably) infinite.

   (b) **Identities**

      1. If e_1 is the identity of $(G_1, *_1)$, then e_2 is the identity of $(G_2, *_2)$

   (c) **Inverses**

      1. If x^{-1} is the inverse of x in $(G_1, *_1)$, then $\phi\left(x^{-1}\right)$ is the inverse of $\phi(x)$ in $(G_2, *_2)$

   (d) **Commutativity -** if $(G_1, *_1)$ is commutative (abelian), then $(G_2, *_2)$ is commutative (abelian)

   (e) **Cyclic Groups and generators**

      1. If $(G_1, *_1)$ is cyclic with generator a, then $(G_2, *_2)$ is cyclic with generator $\phi(a)$

   (f) **Subgroups**

      1. If $(H, *_1) \leq (G_1, *_1)$, then $(\phi(H), *_2) \leq (G_2, *_2)$
      2. If $(H, *_1)$ is a **cyclic subgroup** of $(G_1, *_1)$, of order k and having generator a; then $(\phi(H), *_2)$ is a **cyclic subgroup** of $(G_2, *_2)$, of order k and having generator $\phi(a)$

   (g) **Number and Order of Subgroups**

      1. If $(G_1, *_1)$ has k subgroups of order n, then $(G_2, *_2)$ has k subgroups of order n

6. State three theorems concerning cyclic groups

   Some possibilities include:

   (a) **Thm 1** - every subgroup of a cyclic group is cyclic

   (b) **Thm 2** - Any two finite cyclic groups of order n are isomorphic (i.e., Any two finite cyclic groups of the same order are isomorphic.)

   (c) **Thm 3 -** An isomorphism ϕ between two finite cyclic groups of order n is completely defined by the value of $\phi(a)$, where a is a generator (*any* generator) of the first group. Since isomorphisms map "generator to generator," $\phi(a)$ must be a generator (*any* generator) of the second group. The value of $\phi(b)$ for any element b of the first group is completely determined by the value of $\phi(a)$.

   (d) **Thm 5 -** The generators of the cyclic group $(\mathbb{Z}_n, +)$ are exactly those non-zero "proper remainders" $\{1, 2, 3, \ldots, n-1\}$ that are relatively prime to n.

(e) **Thm 6 -** Given the cyclic group $(\mathbb{Z}_n, +)$, if $a \in \{1, 2, 3, \ldots, n-1\}$, then a generates a cyclic subgroup of order $\frac{|G|}{d}$ where $d = \gcd(a, n)$.

(f) **Thm 7 -** $k \in U_n$ is a generator of $(U_n, \cdot)$ exactly when n is the least positive integer such that $k^{n-1} \equiv 1 \bmod n$

(g) **Cor** - $k \in U_n$ is a generator of $(U_n, \cdot)$ exactly when n is the least positive integer such that $k^{\frac{n-1}{2}} \equiv n-1 \bmod n$

(h) **Thm 8 -** Let $(G, *) = \langle a \rangle$ be a finite cyclic group of order n. Then a^m is a generator of G exactly when m and n are relatively prime. (i.e., exactly when $\gcd(m, n) = 1$).

(i) **Thm 9** - If G is cyclic with generator a, and $H < G$, then either:

1. $H = \langle e \rangle$ (i.e., $H = (\{e\}, *)$

   or

2. $H = \left\langle a^k \right\rangle$, where k is the least natural number such that $a^k \in H$.

(j) **Thm 10 -** Let $G = \langle a \rangle$ be a *finite* cyclic group of order n. For any integer m, $\langle a^m \rangle = \left\langle a^d \right\rangle$, where $d = \gcd(m, n)$.

(k) **Thm 11 -** Suppose that G is a finite cyclic group of order n. Then:

1. for any generator $a \in G$, n is the least natural number such that $a^n = e$.

   and

2. if $a^s = a^t$, then $s \equiv t \bmod n$

Part #2 - Proofs

7. **Prove:** The identity of a group is unique. (Do NOT appeal to the cancellation laws.)

   Remark: We will show that the identity element is unique by assuming that there are (at least) **two** identity elements in the group and showing that they must be one, and the same, element.

   pf/ Suppose that there are two identity elements, e and e_1 in G.

   Observe: $e = e * e_1$ (because e_1 is an identity)

   Also: $e * e_1 = e_1$ (because e is an identity)

   $\Rightarrow e = e * e_1 = e_1$

   i.e., $e = e_1$ ■

8. **Prove:** Given a group $(G, *)$, and an element $x \in (G, *)$, the inverse of x is unique. (Do NOT appeal to the cancellation laws.)

   Remark: We will show that an element x has a unique inverse by assuming that x has (at least) two inverses elements in the group and showing that they must be one, and the same element.

   pf/ Suppose that x has (at least) two inverses, y and z in G.

   Then $xy = e$ and $yx = e$ (because y is an inverse of x)

   Also: $xz = e$ and $zx = e$ (because z is an inverse of x)

   Observe: $y = ye = y(xz) = (yx)z = ez = z$

   i.e., $y = z$ ■

Part #3 - Exercises

9. Part of the multiplication group table for the group $G = \{a, b, c, d\}$ is given. Complete the table.

$\times$	a	b	c	d
a		d		
b				
c				c
d				d

   Since $(G, \times)$ is a **group,** it must have an **identity.**

   Since $c \times d = c$ and $d \times d = d$, it follows that d is the identity. (i.e. d is the element that we multiply c by in order to get c, and d is the element that we multiply d by in order to get d. Thus, d must be the identity.)

   Thus, we have:

$\times$	a	b	c	d
a		d		a
b				b
c				c
d	a	b	c	d

   Next, observe that $a \times b = d$ (remember: d is the identity)

   Thus, b is the inverse of a, and vice versa.

   Hence, $b \times a = d$ also.

   Thus, we have:

$\times$	a	b	c	d
a		d		a
b	d			b
c				c
d	a	b	c	d

We proceed to fill in the rest of the table, using the fact that in a group table, every element appears exactly once in each row and in each column.

In the row headed by a, note that $a \times a \neq a$, and $a \times a \neq d$, because a and d already appear in that row.

Furthermore, $a \times a \neq b$, because that would force us to have $a \times c \neq c$, but c already appears in the column headed by c.

Thus, $a \times a = c$, and consequently, $a \times c = b$.

This yields:

$\times$	a	b	c	d
a	c	d	b	a
b	d			b
c				c
d	a	b	c	d

There is only one "opening" in the column headed by a. It must be occupied by b.

$\times$	a	b	c	d
a	c	d	b	a
b	d			b
c	b			c
d	a	b	c	d

Using the fact the each element must appear exactly once in each row and in each column, the remainder of the table can be filled in as follows:

$\times$	a	b	c	d
a	c	d	b	a
b	d	c	a	b
c	b	a	d	c
d	a	b	c	d

10. Find all generators of $(\mathbb{Z}_8, +)$

The generators of $(\mathbb{Z}_n, +)$ are exactly those elements of $\{1, 2, \ldots, n-1\}$ that are relatively prime to n.

Thus, 1, 3, 5, 7 are the generators of $(\mathbb{Z}_8, +)$.

i.e., $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

(a) Find all proper subgroups of $(\mathbb{Z}_8, +)$ and list their generators

Observe: $d = \gcd(2, 8) = \gcd(6, 8) = 2$.

Thus (by Thm 6), both 2 and 6 generate cyclic subgroups of order $\frac{|G|}{d} = \frac{8}{2} = 4$

Do 2 and 6 generate the **same** cyclic subgroup of order 4?

Because of the closure axiom of groups, they do if either element is contained in the subgroup generated by the other.

Observe: $2 + 2 = 4$ (i.e., $2 \cdot 2 = 4$)
$2 + 4 = 6$ (i.e., $3 \cdot 2 = 6$)
$2 + 6 = 0$ (i.e., $4 \cdot 2 = 0$)
$2 + 8 = 2$ (i.e., $5 \cdot 2 = 2$)

$\boxed{\langle 2 \rangle = \langle 6 \rangle = (\{0, 2, 4, 6\}, +)}$

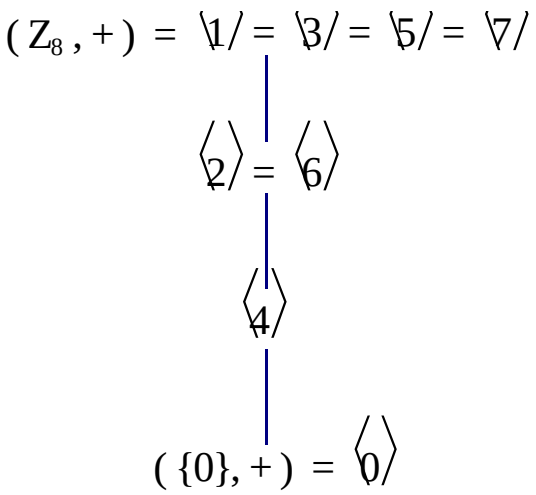
Observe: $4 + 4 = 0$ (i.e., $2 \cdot 4 = 0$)
$4 + 0 = 4$ (i.e., $3 \cdot 4 = 4$)

$\boxed{\langle 4 \rangle = (\{0, 4\}, +)}$

Finally:

$\boxed{\langle 0 \rangle = (\{0\}, +)}$

(b) Draw a subgroup diagram of $(\mathbb{Z}_8, +)$



11. Construct the group table for $(\mathbb{Z}_4, +)$

    The operation in this group is addition modulo 4.

    $(\mathbb{Z}_4, +)$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

12. Construct the group table for $(U_5, \cdot)$

    The operation in this group is multiplication modulo 5.

    $(U_5, \cdot)$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

13. With reference to exercises 11 and 12, define two different isomorphisms $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$

$(\mathbb{Z}_4, +)$ and $(U_5, \cdot)$ are both cyclic groups of order 4. So they must be isomorphic.

Any isomorphism $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$ must map **identity to identity.**

Hence, 0 (the identity of $(\mathbb{Z}_4, +)$) must get mapped to 1 (the identity of $(U_5, \cdot)$).

i.e. $\phi(0) = 1$. This must be true for ANY isomorphism between $(\mathbb{Z}_4, +)$ and $(U_5, \cdot)$.

Also: Any isomorphism $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$ must map **inverse to inverse. (i.e.** $\phi\left(x^{-1}\right) = (\phi(x))^{-1}$

Note that the element $2 \in \mathbb{Z}_4$ is its own inverse (i.e., $2 = 2^{-1}$).

Since $\phi(2)$ is its own inverse, ϕ must map 2 to an element in U_5 that is its own inverse

The element $4 \in U_5$ is its own inverse (i.e., $4 = 4^{-1}$).

Hence, ϕ must map 2 to 4. (i.e., $\phi(2) = 4$).

Finally, in an isomorphism of cyclic groups, ϕ must map **generator to generator.**

1 and 3 are generators of $(\mathbb{Z}_4, +)$ and 2 and 3 are generators of $(U_5, \cdot)$.

Since an isomorphism between cyclic groups is completely determined by the generators, we can map either generator of $(\mathbb{Z}_4, +)$ either generator of $(U_5, \cdot)$, and all of the other assignments will automatically be satisfied.

Case 1: let $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$ be defined by the assignment: $\phi(1) = 2$

Then all other assignments will **automatically** be satisfied:

$\phi(0) = 1$ (identity to identity)

$\phi(1) = 2$ (generator to generator)

$\phi(2) = 4$ (inverse to inverse)

$\phi(3) = 3$ (generator to generator)

Case 2:, let $\phi : (\mathbb{Z}_4, +) \to (U_5, \cdot)$ be defined by the assignment: $\phi(1) = 3$

Then all other assignments will **automatically** be satisfied:

$\phi(0) = 1$ (identity to identity)

$\phi(1) = 3$ (generator to generator)

$\phi(2) = 4$ (inverse to inverse)

$\phi(3) = 2$ (generator to generator)