Math 344 Chapter 2 - Is it a group?

Directions: For each item, determine if the given set and operation form a group. If it is a group, prove it and determine if the group is abelian. If it is not a group, determine which properties fail and give counterexamples to each property that fails. If it is not a group, can you modify the set (e.g. throw out or add some elements) to make the set and operation a group, explain?

- **Definition of Group** Let G be a set and $\circ$ a binary operation on G that assigns to each ordered pair (a, b) of elements of G an element in G denoted by $a \circ b$. We say that G is a **GROUP** under the operation $\circ$ if the following three properties are satisfied:
  1. **Associative**. The operation is associative on the set G: $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$
  2. **Identity**. There is an element $e \in G$ (called the identity element) such that $a \circ e = e \circ a = a$ for all $a \in G$.
  3. **Inverses**. For each $a \in G$ there is an element $b \in G$ such that $a \circ b = b \circ a = e$ (b is called the inverse of a).
- Note that "hidden" in this definition is that the $\circ$ is CLOSED on G. Don't forget to check that property.
- We say the group is **Abelian** if it is commutative: $a \circ b = b \circ a \ \ \forall a, b \in G$.

1. Let the set be $Z_7^* = \{1, 2, 3, 4, 5, 6\}$ and the operation $\times_7$ (multiplication modulo 7). (Hint: Start by making a Cayley table.)

2. Let the set be $Z_9^* = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and the operation $\times_9$. (Hint: Start by making a Cayley table.)

3. Let the set be all 2×2 matrices: $S = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$ with the operation of matrix multiplication.

4. For a fixed pair a and b, define $T_{a,b} : \mathbb{R} \to \mathbb{R}$ by $T_{a,b}(x) = ax + b$. Let the set be $G = \{T_{a,b} \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}$ and let the operation be function composition.

Math 344 Chapter 2 - Elementary Properties of Groups

- **Definition of Group** Let G be a set and $\circ$ a binary operation on G that assigns to each ordered pair (a, b) of elements of G an element in G denoted by $a \circ b$. We say that G is a **GROUP** under the operation $\circ$ if the following three properties are satisfied:
  1. **Associative**. The operation is associative on the set G: $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$
  2. **Identity**. There is an element $e \in G$ (called the identity element) such that $a \circ e = e \circ a = a$ for all $a \in G$.
  3. **Inverses**. For each $a \in G$ there is an element $b \in G$ such that $a \circ b = b \circ a = e$ (b is called the inverse of a).
- Note that "hidden" in this definition is that the $\circ$ is CLOSED on G. Don't forget to check that property.
- We say the group is **Abelian** if it is commutative: $a \circ b = b \circ a \ \ \forall a, b \in G$.

Directions: Prove each of the following.

1. **Theorem 2.1 Uniqueness of the Identity** In a group G, there is only one identity element.

2. **Theorem 2.2 Cancellation** In a group G, the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

3. **Theorem 2.3 Uniqueness of Inverses** For each element a in a group G, there is a unique element b in G such that $ab = ba = e$. (Unless otherwise noted, we will always assume e is the identity element of the group.)

4. **Theorem 2.4 Socks-Shoes Property** For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

1. The following sets are subsets of some known group. Each is described in "set–builder" notation. Rewrite each set by listing its elements inside { }.

   Example: $\{t \in \mathbb{Z}_4 : t +_4 t = 0\} = \{0, 2\}$

   (a) $\{t \in D_4 : t^2 = R_0\}$

   (b) $\{s \in D_4 : s \circ V = V \circ s\}$

   (c) $\{t \in \mathbb{Z}_8 : t +_8 5 = 5 +_8 t\}$

   (d) $\{t \in D_3 : t^2 = R_0\}$

   (e) $\{u \in D_4 : u \circ R_{90} = R_{90} \circ u\}$

   (f) $\{c \in D_5 : c \circ x = x \circ c$ for every $x \in D_5\}$

   (g) $\{r \in D_3 : r^3 = R_0\}$

   (h) $\{c \in D_4 : c \circ x = x \circ c$ for every $x \in D_4\}$

   (i) $\{t \in U(10) : t^2 = 1\}$

   (j) $\{R_{90}^n : n \in Z\}$ (the universal set for this problem is D_4)

   (k) $\{D^n : n \in Z\}$ (the universal set for this problem is D_4)

2. For each of the sets in problem 1, tell whether the set forms a group using the operation of the larger group of which it is a subset. Believe it or not, you may just give a yes/no answer along with a note indicating what prevents it from being a group in the case of a "no" answer.

   (a)

   (b)

   (c)

   (d)

   (e)

   (f)

   (g)

   (h)

   (i)

   (j)

   (k)

[1] Taken from Mike Ward

Let G be a cyclic group of order 40 with generator, g, i.e., $G = \langle g \rangle$.

1. Let $b \in G$. What are the possible orders of b?

2. What is the order of each of the following elements?

   (a) $|g^2| =$

   (b) $|g^6| =$

   (c) $|g^8| =$

   (d) $|g^9| =$

3. Exactly how many subgroups does G have? List them all.

4. Fill in each blank with "$=$", "$\subset$", or "$\supset$".

   (a) $\langle g^2 \rangle \qquad \langle g^4 \rangle$

   (b) $\langle g^2 \rangle \qquad \langle g^6 \rangle$

   (c) $\langle g^{10} \rangle \qquad \langle g^5 \rangle$

   (d) $\langle g^7 \rangle \qquad \langle g^9 \rangle$

5. How many elements of order 8 does G have?

6. How many elements of order 12 does G have?

7. How many elements of order 10 does G have?

8. How many elements of order 20 does G have?

9. Write down the elements in $\langle g^4 \rangle \cap \langle g^5 \rangle$. Can you write that as $\langle g^k \rangle$ for some k?

Recall a set is cyclic if it can be written as $\langle a \rangle = \{a^n \mid n \in Z\}$ for some a in the set. If this is the case, then a is called a *generator* of the set. If G is an additive group, then we write $\langle a \rangle = \{na \mid n \in Z\}$

1. Consider the set $Z_7^* = \{1, 2, 3, 4, 5, 6\}$. We know this set forms a group under multiplication modulo 7.

   (a) Find $\langle 2 \rangle =$

   (b) Find $\langle 3 \rangle =$

   (c) Find $\langle 5 \rangle =$

   (d) Is Z_7^* cyclic?

   (e) Can Z_7^* have more than one generator?

   (f) Fill in the following(where all answers are in Z_7^* (i.e.,reduce everything (mod 7)).

$3^1 =$	$3^{11} =$
$3^2 =$	$3^{12} =$
$3^3 =$	$3^{13} =$
$3^4 =$	$3^{14} =$
$3^5 =$	$3^{15} =$
$3^6 =$	$3^{16} =$
$3^7 =$	$3^{17} =$
$3^8 =$	$3^{18} =$
$3^9 =$	$3^{19} =$
$3^{10} =$	$3^{20} =$

   (g) What is the order of 3 in this group?

   (h) i. For what values of x is $3^x = 1 \pmod 7$? $x =$
   ii. For what values of x is $3^x = 3^1 \pmod 7$? $x =$
   iii. For what values of x is $3^x = 3^2 \pmod 7$? $x =$
   iv. For what values of x is $3^x = 3^3 \pmod 7$? $x =$
   v. For what values of x is $3^x = 3^4 \pmod 7$? $x =$
   vi. For what values of x is $3^x = 3^5 \pmod 7$? $x =$
   vii. For what values of x is $3^x = 3^6 \pmod 7$? $x =$
   viii. What do you think 3^{159} will be?
   ix. Guess the rest of the conjecture: In Z_7^*, $3^x = 3^y$ if and only if ...

(i) Fill in the following(where all answers are in Z_7^* (i.e.,reduce everything (mod 7)).

$2^1 =$	$2^{11} =$
$2^2 =$	$2^{12} =$
$2^3 =$	$2^{13} =$
$2^4 =$	$2^{14} =$
$2^5 =$	$2^{15} =$
$2^6 =$	$2^{16} =$
$2^7 =$	$2^{17} =$
$2^8 =$	$2^{18} =$
$2^9 =$	$2^{19} =$
$2^{10} =$	$2^{20} =$

(j) What is the order of 2 in this group?

(k) i. For what values of x is $2^x = 1 \pmod 7$? $x =$

ii. For what values of x is $2^x = 3^1 \pmod 7$? $x =$

iii. For what values of x is $2^x = 3^2 \pmod 7$? $x =$

iv. For what values of x is $2^x = 3^3 \pmod 7$? $x =$

v. For what values of x is $2^x = 3^4 \pmod 7$? $x =$

vi. For what values of x is $2^x = 3^5 \pmod 7$? $x =$

vii. For what values of x is $2^x = 3^6 \pmod 7$? $x =$

viii. What do you think 2^{159} will be?

ix. Guess the rest of the conjecture: In Z_7^*, $2^x = 2^y$ if and only if ...

(l) Try to make a general conjecture (and then prove it!): Let G be a group and let $a \in G$. Then $a^i = a^j$ if and only if ...

Recall a set is cyclic if it can be written as $\langle a \rangle = \{a^n \mid n \in Z\}$ for some a in the set. If this is the case, then a is called a *generator* of the set. If G is an additive group, then we write $\langle a \rangle = \{na \mid n \in Z\}$

1. Consider the set $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. We know that Z_{12} is a group under addition modulo 12. Fill in the table below:

a	Subset generated by a, $\langle a \rangle$	order of a
0	{ }	
1	{ }	
2	{ }	
3	{ }	
4	{ }	
5	{ }	
6	{ }	
7	$\{7, 2, 9, 4, 11, 6, 1, 8, 3, 10, 5, 0\}$	
8	{ }	
9	{ }	
10	{ }	
11	{ }	

   (a) What is the order of Z_{12}?

   (b) Which elements are generators of Z_{12}?

   (c) Make a conjecture about how the order of an element is related to the order of the group.

   (d) How many *different* cyclic subgroups are generated by elements of Z_{12}?

   (e) Which elements generate the same subgroups? E.g. $\langle 1 \rangle = \langle 5 \rangle = \cdots$ - Write down all such equalities.

   (f) What relationships do you notice between two elements of Z_{12} that generate the same subgroup? List all you can.

   (g) Give a formula for the order of an element $a \in Z_{12}$ in terms of a and $12 =\mid Z_{12} \mid$. Check your formula on several elements.

2. Consider the set $Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. We know this set forms a group under multiplication modulo 13 ($\times_{13}$). Complete the table below and **ignore the last two columns for now.**

a	Subset generated by a, $\langle a \rangle$	order of a	2^k	7^k
1	$\{$ $\}$			
2	$\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$	12		
3	$\{3, 9, 1\}$	3		
4	$\{$ $\}$			
5	$\{5, 12, 8, 1\}$	4		
6	$\{$ $\}$			
7	$\{7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1\}$	12		
8	$\{8, 12, 5, 1\}$	4		
9	$\{$ $\}$			
10	$\{$ $\}$			
11	$\{11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1\}$	12		
12	$\{$ $\}$			

(a) What is the order of Z_{13}^*?

(b) Which elements are generators of Z_{13}^*?

(c) Make a conjecture about how the order of an element is related to the order of the group.

(d) How many *different* cyclic subgroups are generated by elements of Z_{13}^*?

(e) Which elements generate the same subgroups? E.g. $\langle 2 \rangle = \langle 7 \rangle = \cdots$ - Write down all such equalities.

(f) Since 2 is a generator of Z_{13}^*, every element can be written as a power of 2; i.e. for each $a \in Z_{13}^*$, we can write $a = 2^k$ for some integer k. Go back to the table and write in the correct powers of 2 in the 2^k column. (Hint, the subgroup generated by 2 was filled in in order - i.e., as $2, 2^2, 2^3, ...$).

(g) Since 7 is also a generator of Z_{13}^*, every element can also be written as a power of 7; i.e. for each $a \in Z_{13}^*$, we can write $a = 7^j$ for some integer j. Go back to the table and write in the correct powers of 7 in the 7^k column. (Hint, the subgroup generated by 7 was filled in in order - i.e., as $7, 7^2, 7^3, ...$)

(h) Go back to part (e) where you wrote down the equal subgroups. This time rewrite the equalities where you write the elements as their corresponding powers of two (e.g. instead of $\langle 2 \rangle = \langle 7 \rangle = \cdots$, write $\langle 2^1 \rangle = \langle 2^{11} \rangle = \cdots$ since $7 = 2^{11}$).

(i) Go back and do the same thing, but this time with powers of 7.

(j) What relationships do you notice between two elements of Z_{13}^* that generate the same subgroup? List all you can.

(k) Give a formula for the order of an element $a = 2^k \in Z_{13}^*$ in terms of k and $12 =\mid Z_{13}^* \mid$. Check your formula on serveral elements.

(l) Does your formula still work when you write $a = 7^j$ if you replace k by j in the above formula? Check several elements.

(m) Let's generalize... Suppose G is a group of order n. Let $a \in G$ and let k be a positive integer. Give a formula for $\mid a^k \mid$.

Exam 1 is an in class exam to be given on Friday, February 8th.

- Exam 1 covers material through Chapter 4 (not including Thm 4.4).
- I will provide a copy of the Assumed Background Knowledge and Chapter 4 Theorem list.
- You may have one $3x5$ card (both sides) of notes. You may have no more than 2 worked out problems or theorem proofs on your note card. You will turn in your note card with your exam.
- If you need it, I will provide a copy of the back cover of your book (the Cayley tables for D_4 and D_3).
- Suggestions for study:
  - Review the theorems and proofs from the class and book. Work out the proofs on your own, then check with the book or notes.
  - Redo (not just look at) assigned homework problems.
  - Do additional problems from the text.
  - Work out the practice problems below.
  - Make a notecard.
- **Disclaimer:** The set of problems below is not meant to be an exhaustive list of the type of problems that may be on the exam, it is simply for your practice.

1. Circle TRUE or FALSE. Note to be TRUE, it must ALWAYS be true, no exceptions.
   (a) TRUE FALSE Any subgroup of a cyclic group is cyclic.
   (b) TRUE FALSE $\mid D_n \mid = n$
   (c) TRUE FALSE The intersection of two subgroups is a subgroup.
   (d) TRUE FALSE The union of two subgroups is a subgroup.
   (e) TRUE FALSE A nonempty subset of a group that is closed is a subgroup.
   (f) TRUE FALSE If a, b, and c are integers, and $a \mid c$ and $b \mid c$, then $ab \mid c$.
   (g) TRUE FALSE If g is a group element and $g^n = e$, then $\mid g \mid = n$.
   (h) TRUE FALSE Z_n is a subgroup of Z
   (i) TRUE FALSE The set Q^* forms a group under the operation of addition.
   (j) TRUE FALSE The set Q^* forms a group under the operation of multiplication.
2. Let $S = \{(a, b)\text{where } a \in Q^*\text{and } b \in Q\}$, and define a new operation $\#$ as follows: $(a, b)\#(c, d) = (ac + d, b)$.
   (a) What is $(4, 5)\#(-2, 3)$?

(b) Is # an operation on S (defined, well-defined, closed)? Carefully check each property and show which hold and which fail.

(c) Is # commutative on S? (Prove or give a counterexample.)

(d) Does S have an identity element under #? Explain. (If yes, what is the identity?)

3. Prove that a group of order 4 must be Abelian.

4. Let $G = \{a + b\sqrt{2} \mid$ a and b are rational numbers not both $0\}$. Prove that G is a group under ordinary multiplication.

5. Carefully prove the socks and shoes theorem (justify each step): Let a, b be elements of a group G, then $(ab)^{-1} = b^{-1}a^{-1}$.

6. Find a cyclic subgroup of order 4 in U(40).

7. Prove that if $f : A \to B$ and $g : B \to C$ are $1 - 1$ functions, then so is $(f \circ g)(x)$.

8. Find $C(D)$ in D_4.

9. What are all the subgroups of D_3?

10. Let G be a finite Abelian group and let $a, b \in G$. Prove that the set $\langle a, b\rangle = \{a^i b^j \mid i, j \in Z\}$ is a subgroup of G.

11. How many different subgroups does Z_{20} have? Write them all down.

12. Let G be the cyclic group $U(25)$ (under the operation of multiplication modulo 25).

    (a) Given that 2 is a generator of G, i.e., $\langle 2\rangle = U(25)$, find all generators of $U(25)$.

    (b) let H be the subgroup of $U(25)$ generated by 2^2, $H = \langle 2^2\rangle$. Find all other elements of $U(25)$ that generate H.

An *isomorphism* ϕ from a group G to a group $\overline{G}$ is a one-to-one mapping (or function) from G onto $\overline{G}$ that preserves the group operation. That is

$$\phi(ab) = \phi(a)\phi(b) \quad \text{for all } a, b \text{ in } G$$

We write $G \approx \overline{G}$.

1. Consider the group Z of integers under ordinary multiplication, let G be the subgroup generated by 2, i.e. $G = \langle 2 \rangle = \{2k \mid k \in Z\}$. Prove that $G \approx Z$ under the mapping

$$\phi : \langle 2 \rangle \to Z$$

$$\phi(2k) = k$$

(You do not need to show ϕ is a function.)

2. Let G be the real numbers under **addition** $((R, +))$ and let $\overline{G}$ be the positive real numbers under **multiplication** $(R^+, \times)$. show $G \approx \overline{G}$ under the mapping

$$\phi : R \to R^+$$

$$\phi(x) = 2^x$$

(You do not need to show ϕ is a function.)

3. NON-EXAMPLES:

(a) Let R be the group of Real numbers under **addition**. Show that the mapping $\phi : R \to R$ defined by $\phi(x) = x^3$ is not an isomporphism. Which property fails?

(b) Show that there is no isomorphism from Q, the group of rational numbers under **addition**, to Q^*, the group of nonzero rational numbers under **multiplication**.

To do so, condsider the fact that if such an isomorphism $\phi : Q \to Q^*$ existed then there would exist a rational number $a \in Q$ such that $\phi(a) = -1$. Use the operation preserving properties of the isomorphism to show this leads to a contradiction. Hint: $a = \frac{1}{2}a + \frac{1}{2}a$.

4. $U(10)$, $U(12)$ and $U(5)$ all have 4 elements. Two of these groups are isomorphic to each other and the third is not. Which two are isomporphic? How do you know? How can you tell the third is not?

MTH 344 **Introduction to Cosets**

I. In this problem, we are working in the group D_4 with the operation of composition.

(a) Consider $< V >$, the subgroup generated by V, in D_4. Calculate $< V >$, which means list the elements, inside { }, of course.

(b) Calculate the left coset $\{D \circ y : y \in < V >\}$.

(c) Repeat the above with D replaced by each of the other elements of D_4. (That's 7 more sets to compute. Sorry about that, but it is a necessary evil. Divide up the work.)

(d) Calculate the right coset $\{y \circ D : y \in < V >\}$. (Note the D and y have changed places.) Then, as before, repeat that with D replaced by each of the other elements of D_4.

II. Again, we are working in the group D_4 with the operation of composition. Follow the directions of (I) except use the subgroup $K := \{R_0, R_{180}, V, H\}$ of D_4 in place of $< V >$ *wherever* $< V >$ *occurs* in the instructions. Part (a) has no analog here so you can skip that.

III. In this problem we are working in the permutation group A_4 (a subgroup of S_4) with the operation of composition.

(a) List the elements of the group A_4. There are 12 of them. Ignore the table in the book.

(b) Consider $< (1\ 2\ 3) >$, the subgroup generated by (1 2 3). Calculate $< (1\ 2\ 3) >$, which means list the elements, inside { }, of course.

(c) Calculate the left coset $\{(1\ 2)(3\ 4) \circ y : y \in < (1\ 2\ 3) >\}$.

(d) Repeat the above with (1 2)(3 4) replaced by each of the other elements of A_4. (That's 11 more sets to compute. Sorry about that, but it is a necessary evil. Divide up the work.)

(e) Calculate the right coset $\{y \circ (1\ 2)(3\ 4) : y \in < (1\ 2\ 3) >\}$. (Note the (1 2)(3 4) and y have changed places.) Then, as before, repeat that with (1 2)(3 4) replaced by each of the other elements of A_4.

Answer the following questions by using your results.

1. For each of the subgroups in (I), (II) and (III), look at your list of left cosets.

   (a) How many *different* left cosets are there?

   (b) How many elements are in each coset?

   (c) Is every element of the "big" group in at least one left coset? Is any element in two different cosets?

2. Answer the above questions for the right cosets.

3. Are your left cosets the same as your right cosets?

Lemma: Properties of Cosets Let H be a subgroup of G, and let $a, b \in G$. Then,

1. $a \in aH$,
2. $aH = H$ if and only if $a \in H$,
3. $aH = bH$ if and only if $a \in bH$,
4. $aH = bH$ or $aH \cap bH = \emptyset$,
5. $aH = bH$ if and only if $a^{-1}b \in H$,
6. $|aH| = |bH|$,
7. $aH = Ha$ if and only if $H = aHa^{-1}$,
8. aH is a subgroup of G if and only if $a \in H$.

Lagrange's Theorem If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.

We define the *index* of H in G to be the number of left (right) cosets of H in G. We denote the index by $|G : H|$. A direct consequence of Legrange's theorem is a formula for this as recorded by Corollary 1:

Corollary 1 If G is a finite group and H is a subgroup of G, then $|G : H| = |G|/|H|$.

1. The following corollary is often our most used application of Lagrange's Theorem. Prove it please: (Hint: Remember each element forms a cyclic subgroup. hmm. Which Theorem was that? How was the order related to the order of the element?Which Theorem was that?)

   Corollary 2: In a finite group, the order of each element divides the order of the group.

2. **NOTE:** The converse of this is false! Just because a number divides the order of a group does not guarantee that there exists an element of that order. Prove this by finding a group of order n with divisor k of n, but no element of order k. (Hint: Examples abound in Chapter 5.)

3. In the past the following problem was a little complicated to prove, but Lagrange's theorem and its corollary make it easy: Prove that a group of order 5 is cyclic.

4. Prove the more general version of this problem which is recorded as a Corollary to Lagrange's Theorem:
   Corollary 3 A group of prime order is cyclic.

5. Prove the following Corollaries:
   Corollary 4**:** Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.(Hint: Use Cor. 2.)

   Corollary 5**: Fermat's Little Theorem** For every integer a and every prime p,

$$a^p = a \pmod{p}.$$

   Note:This is pretty easy using Cor. 4, but there are 2 cases to consider: 1) $gcd(a, p) = 1$, and 2) $gcd(a, p) \neq 1$. Note the second case implies $p \mid a$. Do you see why?

6. Use the ideas in the previous corollaries to quickly find $7^{26} \pmod{15}$ (do not use your calculator program to do it, but you can use it to check if you're correct).

7. Find the last digit of 97^{12345}. (Hint: How does thinking modulo 10 help?)

8. Let a and b be non-identity elements of different orders in a group of order 155. Prove that the only subgroup of G that contains both a and b is G itself.

Exam 2 "Computational" Review

1. Let $\beta = (12346)(1345)(2643)$

   (a) Write β in array notation.

   (b) What is the order of β?

   (c) Is β an even or odd permutation?

   (d) What is β^{-1}?

   (e) What is β^{101}?

   (f) What is the order of $\alpha = (134)(5678)$?

2. Let H be the subgroup generated by $\langle 5 \rangle$. Write down all of the left cosets of H in Z_{20}.

3. Let G be a cyclic group of order 20, $G = \langle a \rangle$.

   (a) How many right cosets does the subgroup $\langle a^4 \rangle$ have in G?

   (b) List them.

4. How many elements of order 4 are there in S_7?

5. How many elements of order 2 are there in S_7?

6. Let G be a group of order 30.

   (a) What are the possible number of elements of order 5 in G?

   (b) Suppose further that G is cyclic. Does your answer change? If so, how?

7. Find $8^{242} \pmod{13}$ without using your calculator program. Show work.

8. Suppose $\phi : Z_{50} \to Z_{50}$ with $\phi(11) = 13$. Find a formula for $\phi(x)$. It is OK to use your calculator program if necessary, but write "calculator" next to the computation.

9. Go back to each problem and write down any Theorems, Corollaries or Lemmas you used when solving them. Would they always apply to questions like this or only for particular types of questions like this?

10. When studying for the test, redo these problems until you can do them quickly without looking. Go back and write new problems similar to these (change numbers, groups, etc.) and do those. Be sure if you see a problem similar to this on the exam, you know exactly what to do.

MTH 344 Exam 2 "Proof" Review

One aspect of successful test taking is to be able to quickly do proofs in a timed, test-like environment. Below are examples of proofs of reasonable length that may be asked on a 50 minute exam. My expectation would be that you could complete them start to finish in a rather short amount of time. This requires you have some idea of what a successful strategy would be and an idea of which Theorems, Proofs, or Definitions would be applicable. This only comes with practice. I recommend you do the problems below over and over until you fully understand each step and justification and could reproduce the proof without notes in a timely manner. Although you cannot practice proofs that will be exactly like the ones on your test, knowing a variety of proofs well helps with your recall and identification of key parts of many proofs.

1. Prove or disprove $D_4 \approx S_4$.

2. Prove or disprove $D_{12} \approx S_4$.

3. Prove Property 3 of the Chapter 7 Lemma: Let H be a subgroup of G, and let a and b belong to G. Then $aH = bH$ if and only if $a \in bH$. You may use Properties 1 and/or 2 in your proof, but no other properties from the Lemma.

4. Let G be a finite group and $a \in G$ a fixed element of G. Prove that the mapping $\phi : G \to G$ given by $\phi(x) = axa^{-1}$ is an isomorphism from G onto itself. (Remember a stays fixed for every x.)

5. Suppose G is a group and K and H are subgroups of G. If $\mid K \mid = 15$ and $\mid H \mid = 6$, prove $K \cap H$ must be cyclic.

6. Given that G is a finite abelian group of order 55 and G has an element a of order 5 and an element b of order 11. Prove or disprove that G must be cyclic.

7. Prove that A_4, the set of even permutations in S_4 is a subgroup of S_4.

8. Prove Property 4 of Theorem 6.2: Suppose $\phi : G \to \overline{G}$ is a group isomorphism. Prove that $G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$. Do not cite Theorem 6.3, but you may use parts 1-3 of Theorem 6.2.

Exam 2 is an in class exam to be given on Monday, March 11th.

- Exam 2 covers Chapters $5-7$ and the last part of Chapter 4 (Thm. 4.4 and its Corollary).
- You may have one sheet of notes, one side only (regular size paper). You may have no more than 3 worked out problems or theorem proofs on your note sheet. You will turn in your sheet of notes with your exam.
- If you need it, I will provide a copy of the back cover of your boook (the Cayley tables for D_4 and D_3) or of the elements of A_4.
- Suggestions for study:
  - Review the theorems and proofs from the class and book. Work out the proofs on your own, then check with the book or notes.
  - Redo (not just look at) assigned homework problems.
  - Do additional problems from the text.
  - Work out the practice problems below. Make up a new sheet of practice problems and trade with a friend.
  - Make a sheet of notes.
  - Practice problems in a timed environment. Redo problems until you can do them quickly without looking at notes. This better simulates the exam environment.
- **Disclaimer:** The set of problems below is not meant to be an exhaustive list of the type of problems that may be on the exam, it is simply for your practice.

1. (a) TRUE FALSE S_n is non-Abelian for all $n \geq 3$.
   (b) TRUE FALSE If a is a permutation that is an $m-$cycle and b is a permutation that is an $n-$cycle, then $|ab| = lcm(m, n)$.
   (c) TRUE FALSE If a group has an element of order 10, then the number of elements of order 10 is divisible by 4.
   (d) TRUE FALSE A $1-1$ mapping from a set to itself is onto.
   (e) TRUE FALSE If a finite group has order n then the group contains a subgroup of order d for every divisor d of n.
   (f) TRUE FALSE If H is a subgroup of G and a and b belong to G, then aH and Hb are either identical or disjoint.
   (g) TRUE FALSE If H is a subgroup of a finite group G, then the number of distinct left cosets of H in G divides $|G|$.
   (h) TRUE FALSE A group can be isomorphic to a proper subgroup of itself.
   (i) TRUE FALSE Two groups isomorphic to the same group are isomorphic to each other.

2. Give an example of a group that has subgroups of orders $1, 2, 3, 4, 5$, and 6 but does not have a subgroup of order 7 or 8.

3. Find the order of the permutation $\alpha = (124)(2345)$. Is α even or odd? What is α^{16} (don't compute it out, use some theorems)

4. In the group S_n, let $\alpha = (12)(123)(1234)(12345)...(123...n)$. If $n = 99$, determine whether α is even or odd.

5. Suppose that ϕ is an automorphism of Z_9 (isomorphism of Z_9 to itself) and $\phi(4) = 1$. Determine a formula for ϕ.

6. Find all the left cosets of $\{1, 11\}$ in $U(20)$.

7. Given that $|a| = 20$, find all left cosets of $\langle a^{12} \rangle$ in $\langle a \rangle$.

8. Let p be a prime and let n be a positive integer. How many subgroups does Z_{p^n} have (including the trivial subgroup and the group itself)?

1. The following is a partially completed Cayley table for a group.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1			
6	6	5	7	8		1		
7	7	8	5	6			1	
8	8	7	6	5				1

   (a) Complete the Cayley table.

   (b) Find the centralizer of each member of the group.

   (c) Find $Z(G)$.

   (d) What is the order of 2? 3? 4?

   (e) Find a proper subgroup, H, containing 2 and 3.

   (f) Is H cyclic? If so, what is a generator?

   (g) Is H a normal subgroup? Explain.

2. Let $H_1, H_2, H_3, ...$ be a sequence of subgroups of a group with the property that $H_1 \subseteq H_2 \subseteq H_3 ....$ Prove that the union of the sequence is a subgroup.

3. Prove that the subset of elements of finite order in an Abelian group forms a subgroup.

4. What is the order of the element $6 + \langle 4 \rangle$ in the factor group $Z_{48}/\langle 4 \rangle$? What is the order of $5 + \langle 4 \rangle$?

5. If H is a normal subgroup of G and K is *any* subgroup of G, prove that the subgroup $H \cap K$ is normal **in K**.

6. Prove that in any group $|ab| = |ba|$.

7. Prove that the group R^* under multiplication is isomorphic to a subset of itself. (Hint: You must define the subset and produce an isomorphism. Think about using a familiar function for your isomorphism.)

The Final Exam is an in class exam to be given on Monday, March 18th, 12:00 - 1:50pm, MNB 104 (NOTE ROOM CHANGE).

- I will have office hours Monday from $9:00-10:00$ and $10:30-12:00$.
- The final is a cumulative exam and covers the sections we covered in Chapters $1-7, 9$.
- You may have one sheet of notes, both sides (regular size paper). You may have no more than 3 worked out problems or theorem proofs on your note sheet. You will turn in your sheet of notes with your exam.
- Suggestions for study:
  - Write out summaries of each chapter and include important ideas, examples and theorems.
  - Review the theorems and proofs from the class and book. Work out the proofs on your own, then check with the book or notes.
  - Redo (not just look at) assigned homework problems.
  - Do additional problems from the text:
    - Write out the problems from various sections on slips of paper and then put your book away. Mix up the sheets and try to do the problem without looking at the book (you might want to write the section and problem number on the back of the paper so you can check your answer).
    - Examples that are worked out in the section are good ones to put down as you can go back and look at how the book does the problem.
    - Also note there are supplementary exercises for chapters 1-4 starting on p. 91 and for chapters 5-8 starting on p. 174.
  - Make up a set of T/F problems and trade them with your friends.
  - Redo the practice problems on the review sheets for Exam 1 and Exam 2.
  - Work out the practice problems and worksheets given in class (blank copies posted online in the "Worksheets" file under course resources.) Be able to do all problems quickly and without looking at notes.
  - Make a sheet of notes.