PRINT Last name: KEY First name:

Signature: Student ID:

Math 430 Exam 1, Fall 2008

These theorems may be cited at any time during the test by stating "By Theorem ..." or something similar.

Theorem 4.1 Criterion for $a^i = a^j$.
Let G be a group, and let $a \in G$. If $|a| = \infty$, then all distinct powers of a are distinct elements. If a has finite order $n \in \mathbb{Z}^+$, then $\langle a \rangle = \{e, a^1, \ldots, a^{n-1}\}$ is a set of n distinct elements, and $a^i = a^j$ iff n divides $i - j$.

Theorem 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.
Let a be an element of order n in a group and let k be a positive integer.
Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

Theorem 4.3 Fundamental Theorem of Cyclic Groups.
Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k — namely, $\langle a^{n/k} \rangle$.

Part	I	56
	II	42
	III	30
		128

I. Examples, Counterexamples and short answer. (7 pts ea.) Do not give proofs, but clearly indicate your proposed example or counterexample, or short answer where appropriate.

1. Find integers a, b, and c such that $a\,|\,c$ and $b\,|\,c$, but $ab \nmid c$.

   $a = 4 \quad b = 6 \quad c = 12$

   $4 \mid 12$ and $6 \mid 12$ but $4 \cdot 6 = 24 \nmid 12$.

2. Suppose that $x_1, x_2, \ldots, x_t$ are elements from a dihedral group, and that the product $x_1 x_2 \cdots x_t$ is a reflection. What can you say about the number of x_i that are reflections?

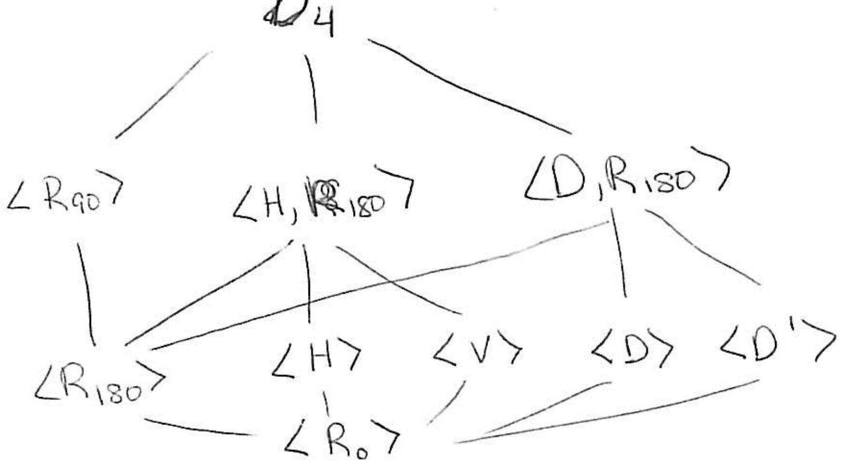
   This number must be odd.

3. Give an example of a group G that has an element of finite order greater than 1, and an element of infinite order. Write down these elements and their orders.

   $\mathbb{R}^*$ (multiplication)

   $\underbrace{|-1| = 2}_{\text{finite} > 1} \qquad \underbrace{|2| = \infty}_{\text{infinite}}$

4. Draw the subgroup diagram of the dihedral group $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$. Each subgroup appears once, and there is a line between subgroups if one is contained in the other with no subgroup in between.



28

5. List all of the generators for the subgroup of order 8 in $\mathbb{Z}_{24}$.

$|\langle 3\rangle| = 8$ $\quad\quad$ $\langle 3\rangle = \langle 3^3\rangle = \langle 3^5\rangle = \langle 3^7\rangle$

$3, 9, 15, 21 = 3^1, 3^3, 3^5, 3^7$

(the powers k satisfy $\gcd(8,k) = 1$)

6. Give two reasons why the set of odd permutations of S_n is not a subgroup.

(1) ε is an even permutation

(2) the product of two odd permutations is an even permutation.

7. What is the order of the following permutation?

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}$$

$\alpha = (1753)(264)$

cycle lengths 4 + 3

$\text{lcm}(4,3) = 12 = |\alpha|$

8. Describe two groups of order 4 that are not isomorphic. You could give the sets and the operations or give the Cayley Tables, for example.

(1) The set of 180 degree rotations of the tetrahedron plus the identity, or $U(8)$

(2) $\mathbb{Z}_4$ (addition), or $U(10)$

$U(12) \cong U(8) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$U(5) \cong U(10) \cong \mathbb{Z}_4$

28

II. Constructions and Algorithms. (14 pts ea.) Do not write proofs, but do give clear, concise answers, including steps to algorithms where applicable.

9. For this question, the group G has Cayley Table as given.

6 **(a)** Find the center $Z(G)$.

6 **(b)** Find the centralizer $C(j)$.

2 **(c)** Name a group that is isomorphic to G.

G	e	a	b	c	d	f	g	h	i	j	k	l
e	e	a	b	c	d	f	g	h	i	j	k	l
a	a	b	c	d	f	e	h	i	j	k	l	g
b	b	c	d	f	e	a	i	j	k	l	g	h
c	c	d	f	e	a	b	j	k	l	g	h	i
d	d	f	e	a	b	c	k	l	g	h	i	j
f	f	e	a	b	c	d	l	g	h	i	j	k
g	g	l	k	j	i	h	e	f	d	c	b	a
h	h	g	l	k	j	i	a	e	f	d	c	b
i	i	h	g	l	k	j	b	a	e	f	d	c
j	j	i	h	g	l	k	c	b	a	e	f	d
k	k	j	i	h	g	l	d	c	b	a	e	f
l	l	k	j	i	h	g	f	d	c	b	a	e

(a) $Z(G) = \{e, c\}$ (the element's column downward must equal the elements row rightward)

(b) $C(j) = \{e, C, j, g\}$ (the elements in the row of j that match the elements in the column of j at the corresponding position)

(c) D_6

14

10. Find $\gcd(233, 55)$ using the Euclidean algorithm. Find $s, t \in \mathbb{Z}$ such that $\gcd(233, 55) = 233 \cdot s + 55 \cdot t$.

$233 = 55 \cdot 4 + 13$

$55 = 13 \cdot 4 + 3$

$13 = 3 \cdot 4 + \boxed{1}$

$3 = 1 \cdot 3 + 0$

$\gcd(233, 55) = 1$

backsolve: $1 = 13 - 3 \cdot 4$ ①

$3 = 55 - 13 \cdot 4$ ②

$13 = 233 - 55 \cdot 4$ ③

③ into ②: $3 = 55 - (233 - 55 \cdot 4$

② into ①: $1 = 13 - (55 - 13 \cdot 4) \cdot 4$

$= 13 \cdot 17 - 55 \cdot 4$

③ into result: $1 = (233 - 55 \cdot 4) \cdot 17 - 55 \cdot 4$

$= 233 \cdot 17 - 55 \cdot 72$

11. Find a group of permutations that is isomorphic to the group $U(12)$ (which is possible by Cayley's Theorem). Hint: starting with the Cayley Table of $U(12)$.

$U(12) = \{1, 5, 7, 11\}$

		ⓐ	ⓑ	ⓒ	ⓓ
	U(12)	1	5	7	11
ⓐ	1	1	5	7	11
ⓑ	5	5	1	11	7
ⓒ	7	7	11	1	5
ⓓ	11	11	7	5	1

row of ⓐ: $\begin{bmatrix} a & b & c & d \\ a & b & c & d \end{bmatrix} = (a)$

row of ⓑ: $\begin{bmatrix} a & b & c & d \\ b & a & d & c \end{bmatrix} = (ab)(cd)$

row of ⓒ: $\begin{bmatrix} a & b & c & d \\ c & d & a & b \end{bmatrix} = (ac)(bd)$

row of ⓓ: $\begin{bmatrix} a & b & c & d \\ d & c & b & a \end{bmatrix} = (ad)(bc)$

or $\{\varepsilon, (1,5)(7,11), (1,7)(5,11), (1,11)(5,7)\}$

28

III. Proofs. (10 pts ea.) Part of the score is determined by careful formatting of the proof (forward and reverse directions, assumptions, conclusions, stating whether you are proving by direct proof, contrapositive, contradiction, induction, etc.). Partial credit will be awarded for this as well.

12. Let x be an integer and k a positive integer. Prove that if $x \bmod k = 1$, then $\gcd(x, k) = 1$. Prove that the converse of this statement is not true; i.e., that $\gcd(x, k) = 1$ does not imply $x \bmod k = 1$.

6 ($\Rightarrow$) Assume $x \bmod k = 1$.

(direct) By definition, $x = k \cdot q + 1$ for some $q \in \mathbb{Z}$.

rearranging, $1 = x \cdot 1 - k \cdot q$

Thus 1 is a linear combination of k and q, and 1 is the smallest positive integer.

Taken together this implies $\gcd(x, k) = 1$.

4 ($\not\Leftarrow$) Fix $k = 6$ and $x = 5$ (generally $k \geq 3$, $x = k-1$)

(by c/ex) $\gcd(6,5) = 1$ since $1 = 6 \cdot 1 + 5(-1)$

but $5 \bmod 6 = 5 \neq 1$.

13. Let H be a subgroup of $\mathbb{R}$ under addition. Let $K = \{2^a \mid a \in H\}$. Prove that K is a subgroup of $\mathbb{R}^*$ under multiplication.

By 2-step subgroup test.

identity $H \leq \mathbb{R}$ implies that $0 \in H$. Thus $2^0 = 1 \in K$, and so K contains the identity of $\mathbb{R}^*$.

closure Let $k_1, k_2 \in H$. By definition,

$$\left.\begin{array}{l} k_1 = 2^{a_1} \\ k_2 = 2^{a_2} \end{array}\right\} \text{ for some } a_1, a_2 \in H.$$

H is closed under $+$, so $a_1 + a_2 \in H$. By definition of K, $2^{a_1 + a_2} \in K$. But this is the same as $2^{a_1} 2^{a_2} = k_1 k_2$, which is in K.

inverses Let $k \in K$. Then $k = 2^a$ for some $a \in H$. H contains inverses, and so $-a \in H$. By definition, $2^{-a} \in K$. But $2^a 2^{-a} = 2^0 = 2^{-a} 2^a$ by rule of exponent, and so K contains the inverse of 2^a. Thus $K \leq \mathbb{R}^*$ by 2-step subgroup test.

20

Prove ***ONE*** out of 14-15. Clearly indicate which proof you want graded.

14. Suppose that $|x| = n$, where x is a group element and n is a positive integer. Find a necessary and sufficient condition on r and s such that $\langle x^r \rangle \leq \langle x^s \rangle$.

15. Suppose that n is odd and σ is an n-cycle in S_n. Show that σ does not commute with any permutation of order 2. (Hints: What is the cycle structure of an order 2 permutation? It is helpful to consider whether a particular power of σ commutes with an order 2 permutation.)

14. By Theorem 4.2, $\langle x^r \rangle = \langle x^{\gcd(n,r)} \rangle$ and $\langle x^s \rangle = \langle x^{\gcd(n,s)} \rangle$

Now set $a = x^{\gcd(n,s)}$, so that $|a| = n/\gcd(n,s)$ by Thm. 4.2

By Theorem 4.3, $|\langle x^r \rangle| \overset{\text{Thm 4.2}}{=} n/\gcd(n,r)$ must be a divisor of $|\langle x^s \rangle| = n/\gcd(n,s)$ in order for $\langle x^r \rangle \leq \langle x^s \rangle$.

The condition $n/\gcd(n,r) \mid n/\gcd(n,s)$ is equivalent to $\boxed{\gcd(n,s) \mid \gcd(n,r)}$.

15. Let β be an order 2 permutation in S_n. Since $|\beta|$ is the lcm, of it's cycle lengths in disjoint cycle notation, β has at least one 2-cycle and no cycles longer than 2. Since n is odd, β has at least one 1-cycle, say (j). Let $k \in [n]$ be an element of a 2-cycle of β, so β looks like

$$\cdots (j) \cdots (k\ l) \cdots \quad \text{for some } l \in [n].$$

In disjoint cycle notation.

Since σ is an n-cycle, σ looks like (shifting if necessary)

$$(\cdots j \cdots k \cdots)$$

so that $\sigma^t(j) = k$ for some $1 \leq t < n$.

Now $\sigma^t \beta(j) = k$, but $\beta \sigma^t(j) = l$, so σ^t and β don't commute. If σ and β commute, then so would σ^t and β. Thus by contrapositive $\sigma\beta \neq \beta\sigma$. □

10