PRINT Last name: $\qquad$ First name: $\qquad$

Signature: $\qquad$ Student ID: $\qquad$

## Math 430 Exam 1, Fall 2006

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 $\langle a\rangle=\left\{e, a^{1}, \ldots, a^{n-1}\right\}$ is a set of $n$ distinct elements, and $a^{i}=a^{j}$ iff $n$ divides $i-j$.

Theorem $4.2\left\langle a^{k}\right\rangle=\left\langle a^{\operatorname{gcd}(n, k)}\right\rangle$.
Let $a$ be an element of order $n$ in a group and let $k$ be a positive integer.
Then $\left\langle a^{k}\right\rangle=\left\langle a^{\operatorname{gcd}(n, k)}\right\rangle$ and $\left|a^{k}\right|=n / \operatorname{gcd}(n, k)$.
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, $\left\langle a^{n / k}\right\rangle$.
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 $a \mid c$ and $b \mid c$, but $a b \nmid c$.
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?
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.
4. Draw the subgroup diagram of the dihedral group $D_{4}=\left\{R_{0}, R_{90}, R_{180}, R_{270}, H, V, D, D^{\prime}\right\}$. Each subgroup appears once, and there is a line between subgroups if one is contained in the other with no subgroup in between.
5. List all of the generators for the subgroup of order 8 in $\mathbb{Z}_{24}$.
6. Give two reasons why the set of odd permutations of $S_{n}$ is not a subgroup.
7. What is the order of the following permutation?

$$
\left[\begin{array}{lllllll}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
7 & 6 & 1 & 2 & 3 & 4 & 5
\end{array}\right]
$$

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.
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.
(a) Find the center $Z(G)$.
(b) Find the centralizer $C(j)$.
(c) Name a group that is isomorphic to $G$.

| $G$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ | $g$ | $h$ | $i$ | $j$ | $k$ | $l$ |
| $a$ | $a$ | $b$ | $c$ | $d$ | $f$ | $e$ | $h$ | $i$ | $j$ | $k$ | $l$ | $g$ |
| $b$ | $b$ | $c$ | $d$ | $f$ | $e$ | $a$ | $i$ | $j$ | $k$ | $l$ | $g$ | $h$ |
| $c$ | $c$ | $d$ | $f$ | $e$ | $a$ | $b$ | $j$ | $k$ | $l$ | $g$ | $h$ | $i$ |
| $d$ | $d$ | $f$ | $e$ | $a$ | $b$ | $c$ | $k$ | $l$ | $g$ | $h$ | $i$ | $j$ |
| $f$ | $f$ | $e$ | $a$ | $b$ | $c$ | $d$ | $l$ | $g$ | $h$ | $i$ | $j$ | $k$ |
| $g$ | $g$ | $l$ | $k$ | $j$ | $i$ | $h$ | $e$ | $f$ | $d$ | $c$ | $b$ | $a$ |
| $h$ | $h$ | $g$ | $l$ | $k$ | $j$ | $i$ | $a$ | $e$ | $f$ | $d$ | $c$ | $b$ |
| $i$ | $i$ | $h$ | $g$ | $l$ | $k$ | $j$ | $b$ | $a$ | $e$ | $f$ | $d$ | $c$ |
| $j$ | $j$ | $i$ | $h$ | $g$ | $l$ | $k$ | $c$ | $b$ | $a$ | $e$ | $f$ | $d$ |
| $k$ | $k$ | $j$ | $i$ | $h$ | $g$ | $l$ | $d$ | $c$ | $b$ | $a$ | $e$ | $f$ |
| $l$ | $l$ | $k$ | $j$ | $i$ | $h$ | $g$ | $f$ | $d$ | $c$ | $b$ | $a$ | $e$ |

10. Find $\operatorname{gcd}(233,55)$ using the Euclidean algorithm. Find $s, t \in \mathbb{Z}$ such that $\operatorname{gcd}(233,55)=$ $233 \cdot s+55 \cdot t$.
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 $U(12)$.
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 $\operatorname{gcd}(x, k)=$ 1. Prove that the converse of this statement is not true; i.e., that $\operatorname{gcd}(x, k)=1$ does not imply $x \bmod k=1$.
13. Let $H$ be a subgroup of $\mathbb{R}$ under addition. Let $K=\left\{2^{a} \mid a \in H\right\}$. Prove that $K$ is a subgroup of $\mathbb{R}^{*}$ under multiplication.

Prove $\boldsymbol{O N E}$ 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 $\left\langle x^{r}\right\rangle \leq\left\langle x^{s}\right\rangle$.
15. Suppose that $n$ is odd and $\sigma$ is an $n$-cycle in $S_{n}$. Show that $\sigma$ 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 $\sigma$ commutes with an order 2 permutation.)

