PRINT Last name: KEY First name: ____________

Signature: ____________ Student ID: ____________

Math 430 Exam 2, Fall 2008

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

Theorem U: Structure of $U(n)$.
The groups $U(n)$ have the following structure. $U(2) = \{0\}$. $U(4) \approx \mathbb{Z}_2$.

$$\begin{aligned} U(2^n) &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}, && \text{for } n \geq 3; \\ U(p^n) &\approx \mathbb{Z}_{p^n - p^{n-1}}, && \text{for } p \text{ an odd prime.} \end{aligned}$$

Theorem I1: Criterion 1 for Isomorphism
$H \oplus G \approx K \oplus G$ iff $H \approx K$.

Theorem I2: Criterion 2 for Isomorphism
If there exists a permutation $\sigma \in S_n$ such that $H_i \approx K_{\sigma(i)}$ for all i, then $H_1 \oplus H_2 \oplus \cdots \oplus H_n \approx K_1 \oplus K_2 \oplus \cdots \oplus K_n$. (The reverse is not true!)

I. Examples, Counterexamples and short answer. (5 pts ea.) Do not give proofs, but clearly indicate your proposed example or counterexample, or short answer where appropriate.

1. Find a pair of permutations in S_3 that commute. Find a pair of permutations in S_3 that do not commute. Clearly distinguish which pair is which.

(123), (132)
commute

(12), (23)
don't commute

2. How many different groups of each of the following orders are there up to isomorphism?

3: 1 5: 1

2: 1 4: 2 6: 2

3. Assume the following facts:
   - $K \leq H$
   - $H \leq G$
   - There are 6 left cosets of K in H.
   - There are 4 left cosets of H in G.

   How many left cosets of K are there in G? $\boxed{24}$

   $|G| = 4 \cdot |H|$

   $|H| = 6 \cdot |K|$

   $\therefore |G| = 24 \cdot |K|$

4. How many elements of order 2 are there in $D_6 \oplus D_4$?

forms: (a) (e, x), $|x| = 2$
(b) (x, e), $|x| = 2$
(c) (x, y), $|x| = |y| = 2$

order 2 elts in $D_6 = 7$
order 2 elts in $D_4 = 5$

(a) $1 \cdot 5$
(b) $7 \cdot 1$
(c) $7 \cdot 5$

$= \boxed{47}$

20

5. What is the largest n such that the group of permutations S_n **does not** have a permutation of order 12? (I.e., what is $\max\{n \in \mathbb{Z}^+ \mid \nexists \alpha \in S_n, |\alpha| = 12\}$?)

$n = 6$. (largest order is 9)

6. Give two infinite groups not isomorphic to $\mathbb{Z}$. $\mathbb{Q}$, $\mathbb{Q}^*$

under $+$ under $*$

7. Find a group G, a subgroup H of G, and an element $a \in G$ such that $aH \neq Ha$. (You can name the group without listing all of its elements, but the element a must be explicitly named or described.)

$\boxed{G = D_4, \quad H = \{R_0, H\}, \quad a = R_{90}}$

$R_{90} H = \{R_{90}, H\}$ $\quad$ $H R_{90} = \{R_{90}, V\}$

horizontal reflection, not the subgroup H

8. Find values $m, n \in \mathbb{Z}^+$ such that $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic. Find values $m, n \in \mathbb{Z}^+$ such that $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is **not** cyclic. (Clearly identify which is which!)

$m=2$, $n=3$ cyclic

$m=2$, $n=2$ not cyclic

II. Constructions and Algorithms. (10 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.
   3 **(a)** Compute the left cosets of $\{e, l\}$ in G. Try to minimize the number of computations.
   3 **(b)** Compute the right cosets of $\{e, l\}$ in G.
   2 **(c)** Give a reason why you get the answers in (a) and (b).
   2 **(d)** What are the left cosets of $\{e, i, l, m\}$?

G	e	i	j	k	l	m	n	o
e	e	i	j	k	l	m	n	o
i	i	l	k	n	m	e	o	j
j	j	o	l	i	n	k	e	m
k	k	j	m	l	o	n	i	e
l	l	m	n	o	e	i	j	k
m	m	e	o	j	i	l	k	n
n	n	k	e	m	j	o	l	i
o	o	n	i	e	k	j	m	l

(a) $\{e, l\}$ $\quad j\{e,l\} = \{j, n\}$

$i\{e,l\} = \{i, m\}$ $\quad k\{e,l\} = \{k, o\}$

(b) $\{e, l\}$ $\quad \{e,l\}j = \{j, n\}$

$\{e,l\}i = \{i, m\}$ $\quad \{e,l\}k = \{k, o\}$

(c) $\{e, l\} \leq Z(G)$

(d) $\{e, i, l, m\}, \{j, k, n, o\}$

10. Refer to the Cayley table of Question 9 for this question. Compute the orders of the elements k and l in G in the following manner:

(i) Find the permutation defined in the proof of Cayley's Theorem corresponding to the element,
(ii) Find the cycle form of the permutation, and then
(iii) Compute the order of the permutation.
(Recall that Cayley's Theorem states that every group is isomorphic to a group of permutations.)

(i) $k \leftrightarrow \begin{bmatrix} e & i & j & k & l & m & n & o \\ k & j & m & l & o & n & i & e \end{bmatrix}$ (ii) $= (e, k\, l\, o)(i\, j\, m\, n)$ (iii) $\mathrm{lcm}(4,4) = \boxed{4}$

(i) $l \leftrightarrow \begin{bmatrix} e & i & j & k & l & m & n & o \\ l & m & n & o & e & i & j & k \end{bmatrix}$ (ii) $= (e\, l)(i\, m)(j\, n)(k\, o)$ (iii) $\mathrm{lcm}(2,2,2,2) = \boxed{2}$

11. Determine whether $U(176) \oplus \mathbb{Z}_3$ is isomorphic to $U(140) \oplus \mathbb{Z}_5$. Give a justification for **each step**. If any of the theorems on the cover apply you could just cite them.

$U(176) \approx U(11) \oplus U(16)$ $U(140) \approx U(4) \oplus U(5) \oplus U(7)$ since $U(st) \approx U(s) \oplus U(t)$ when $\gcd(s,t) = 1$.

$U(176) \approx \mathbb{Z}_{10} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$ $U(140) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$ by Thm U

$U(176) \approx \mathbb{Z}_{10} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$ $U(140) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5$ by Thm I1

$U(176) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5$ Since $\mathbb{Z}_{10} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_5$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_6$ and Thm I2

Therefore $U(176) \oplus \mathbb{Z}_3 \approx U(140) \oplus \mathbb{Z}_5$.

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 the proof is direct, contrapositive, contradiction, induction, etc.). Partial credit will be awarded for this as well.

12. Let β be some fixed odd permutation in S_n. Prove that every odd permutation in S_n can be written as the product of β and some even permutation. (If you make an assumption along the way, clearly state it.)

(Direct)
Let $\alpha \in S_n$ be an odd permutation.
Since β is odd, so is β^{-1} by closure of A_n.

$\alpha = \beta(\beta^{-1}\alpha)$, where $\beta^{-1}\alpha$ is even as the product of 2 odd permutations.
Therefore any odd $\alpha \in S_n$ can be written as the product of β and some even permutation. $\square$

13. Let G be a group of order 49. Prove that either G is cyclic, or $g^7 = e$ for all elements $g \in G$.

(Direct)
By Lagrange's theorem, every element $g \in G$ satisfies $|g| \mid |G|$.
(since $|g| = |\langle g \rangle|$ and $\langle g \rangle \leq G$.)
The divisors of $|G|$ are $1, 7, 49$.

<u>Case 1</u> G has an order 49 element.
Then G is cyclically generated by this element.

<u>Case 2</u> G has only order 7 and 1 elements.
Let $g \in G$. $|g| = 7 \Rightarrow g^7 = e$.
$|g| = 1 \Rightarrow g^7 = e^7 = e$.

Therefore either G is cyclic or $g^7 = e$ for all elements $g \in G$. $\square$

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

14. Suppose that G is a finite Abelian group that has at least 3 elements of order 3. Prove that 9 divides $|G|$.

15. The *exponent* of a group is the smallest positive integer n such that $x^n = e$ for all x in the group. Prove that every finite group has an exponent that divides the order of the group. (I.e., that $\min\{n \in \mathbb{Z}^+ \mid \forall x \in G, x^n = e\}$ divides $|G|$.)

14. (Direct).

Let $a \in G$ haver order 3. Then so does a^2, and $a \neq a^2$.

Let $b \in G$ be a third distinct order 3 element of G.

Now define $H = \{a^i b^j \mid 0 \leq i, j \leq 3\}$.

Claim $H \leq G$.

identity $a^0 b^0 = e \in H$.

closure/inverse Let $g_1, g_2 \in H$. Then $g_1 = a^{i_1} b^{j_1}$, $g_2 = a^{i_2} b^{j_2}$ for $0 \leq i_1, j_1, i_2, j_2 \leq 3$.

$$g_1 g_2^{-1} = a^{i_1} b^{j_1} (a^{i_2} b^{j_2})^{-1} = a^{i_1} b^{j_1} (b^{j_2})^{-1} (a^{i_2})^{-1}$$

$$= a^{i_1} b^{j_1} b^{-j_2} a^{-i_2} = a^{i_1 - i_2} b^{j_1 - j_2} \quad \text{since Abelian.}$$

$$= a^{i_1 - i_2 \bmod 3} b^{j_1 - j_2 \bmod 3} \quad \text{since } \langle a \rangle, \langle b \rangle \approx \mathbb{Z}_3$$

Thus $g_1 g_2^{-1} \in H$.

By 1-step subgroup test, $H \leq G$. this proves the claim.

Furthermore $|H| = 9$ since $a^i b^j$ is uniquely determined by (i, j):

$$a^i b^j = a^k b^l \quad \text{and } 0 \leq i, j, k, l \leq 3$$

$$\text{iff } a^{i-k} b^{j-l} = a^0 b^0 \quad \text{"} \quad \text{"}$$

$$\text{iff } i = k \text{ and } j = l \quad \text{"} \quad \text{"}$$

By Lagrange's Theorem, $|H| \mid |G|$, and so $9 \mid |G|$. $\square$

(15 on reverse)

15. (Direct)

Let G be a finite group.

Let n = smallest positive integer such that $g^n = e$ for all $g \in G$.

Then $|g| \mid n$ for all $g \in G$.

$\operatorname{lcm}(g : g \in G)$ is the smallest positive integer such that $|g| \mid n$ for all $g \in G$.

Thus $n = \operatorname{lcm}(g : g \in G)$.

By Lagranges Theorem, $|g| \mid |G|$ for all $g \in G$. Thus $|G|$ is a common multiple of all $g \in G$.

But n is the least common multiple, and so $n \mid |G|$. $\square$