PRINT Last name: KEY First name: ____________

Signature: ____________ Student ID: ____________

Math 430 Exam II, Fall 2006

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. Give an example of a cyclic group G and two subgroups H_1, H_2 such that

   (i) $\{e\} \leq H_1 \leq H_2 \leq G$ (ascending subgroup condition), and
   (ii) $1 < |H_1| < |H_2| < |G|$ (subgroup distinctness condition).

   1 bonus point for minimizing $|G|$.

   $G = \mathbb{Z}_8 \quad H_1 = \langle 4 \rangle \quad H_2 = \langle 2 \rangle$

   $\mathbb{Z}_8$
   |
   $\langle 2 \rangle$
   |
   $\langle 4 \rangle$
   |
   $\langle 0 \rangle$

   minimum $|G| = p^3$ for $p = 2$
   $= 8$

2. Give an example of two permutations α and β from the permutation group S_n such that

   (i) α is an odd permutation
   (ii) β is an even permutation, and
   (iii) $\alpha\beta \neq \beta\alpha$.

   1 bonus point for minimizing n.

   $\alpha = (12)$
   $\beta = (12)(13)$

   (check: $\alpha\beta = (12)(12)(13) = (13)$
   $\beta\alpha = (12)(13)(12) = (1)(23) \neq \alpha\beta$

   minimum n is 3 since $S_2 \approx \mathbb{Z}_2$ is abelian)

3. Give an example of two non-isomorphic infinite groups.

$\mathbb{Z}$ under + and $\mathbb{R}$ under +

since one is countable, other uncountable (no bijection exists)

or $\mathbb{Z}$ under +, $\mathbb{Q}^+$ under $\cdot$

or $\mathbb{Z}$ under +, $\mathbb{R}$ under + ...

4. Let G be a finite group of permutations on $\{1, \ldots, n\}$. Recall that
   $\text{stab}_G(i) = \{\phi \in G : \phi(i) = i\}$,
   $\text{orb}_G(i) = \{\phi(i) : \phi \in G\}$, and that
   $|G| = |\text{stab}_G(i)| \cdot |\text{orb}_G(i)|$.

   Now, find a G such that

   (i) $n > 2$,
   (ii) $|\text{stab}_G(1)| = \left(\frac{n}{2}\right)! \cdot \left(\frac{n}{2} - 1\right)!$ and
   (iii) $|\text{orb}_G(1)| = \frac{n}{2}$.

   (Hint: Pick an n and pick the $n/2$ elements, including 1, which are in the orbit of 1, and build permutations in G.) 1 bonus point for minimizing n.

$n = 4$ (minimum)

pick $\text{orb}_G(1) = \{1, 2\}$ so $|\text{orb}_G(1)| = 2 = \frac{n}{2}$.

Need $|\text{stab}_G(1)| = \left(\frac{4}{2}\right)! \left(\frac{4}{2} - 1\right)! = 2$ and

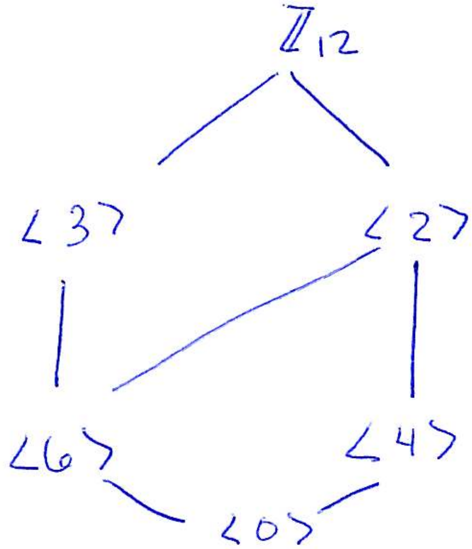
$|G| = |\text{orb}_G(1)| \cdot |\text{stab}_G(1)| = \frac{n}{2} \cdot \left(\frac{n}{2}\right)! \left(\frac{n}{2} - 1\right)! = \left[\left(\frac{n}{2}\right)!\right]^2 = 2^2 = 4$

$G = \{ \underbrace{(1), (12), (34)}_{\text{stab}_G(1) = \{(1),(34)\}}, (12)(34) \}$

other possibilities permute 2,3,4 in this group.

5. Select a composite integer of the form $n = p^2q$ with p, q distinct primes. Draw the subgroup diagram of $\mathbb{Z}_n$ (under addition). All subgroups $H \leq \mathbb{Z}_n$ should appear, with an edge between H_1 and H_2 if $H_1 \leq H_2$ and there is no distinct subgroup $H \notin \{H_1, H_2\}$ with $H_1 \leq H \leq H_2$. (E.g., you would not connect $\langle R_0 \rangle$ and $\langle R_{90} \rangle$ in D_4 since the distinct subgroup $\langle R_{180} \rangle$ lies between them.) 1 bonus point for minimizing n.

minimum n when $p=2$, $q=3$. $n = 4 \cdot 3 = 12$.



6. Recall that an inner automorphism on a group G is an isomorphism $\phi_a : G \to G$ for a given $a \in G$ defined by

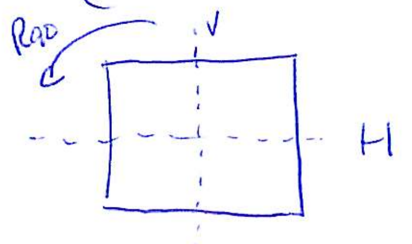
$$\phi_a(x) = axa^{-1} \text{ for all } x \in G.$$

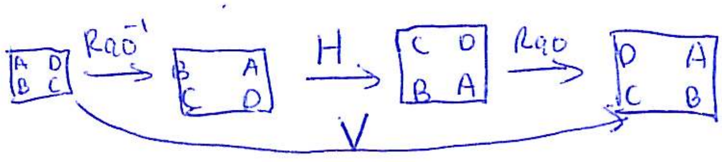
(a) Find $a \in D_4$ such that ϕ_a is a nontrivial inner automorphism of D_4, **and**
(b) Find an x that certifies this; that is, such that $\phi_a(x) \neq x$.

Let $a = R_{90}$.

Let $x = H$

(then $\phi_a(x) = \phi_{R_{90}}(H) = R_{90} H R_{90}^{-1}$
$= V$
$\neq H$)





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

7. Construct the partition of the group of even permutations A_4 into the left cosets of $H = \{(1), (12)(34)\}$. Clearly indicate your partition. (Hint: You should be able to do this with only 4 permutation product computations.)

$H = \{(1), (12)(34)\}$

$(123)H = \{(123), (134)\}$

$(132)H = \{(132), (234)\}$

$(143)H = \{(143), (124)\}$

$(243)H = \{(243), (142)\}$

$$\underbrace{\begin{array}{l}(123)(12)(34) = (134)\\ (132)(12)(34) = (1)(234)\\ (143)(12)(34) = (124)\\ (243)(12)(34) = (142)\end{array}}_{\text{4 computations}}$$

by elimination, the last coset must be

$(13)(24)H = \{(13)(24), (14)(23)\}$

8. **WARNING: look at the rest of the test before starting this problem.**
The group of Quaternions Q has Cayley table below.

8 (a) Compute a subgroup $H \le S_8$ such that $Q \approx H$. (This implements Cayley's Theorem. Think $T_g(x) = gx$ and look at g's row in the Cayley table.)

3 (b) Does H contain any odd permutations? If so, list one.

3 (c) Let $\phi : Q \to H$ be the isomorphism you have constructed. Express the image of the subgroup $\phi(\{U, I, -U, -I\})$ as $\langle h_1, h_2, \ldots \rangle$, with a minimum number of generators $h_1, h_2, \ldots$ from H.

	1	2	3	4	5	6	7	8
	U	I	J	K	$-U$	$-I$	$-J$	$-K$
U	U	I	J	K	$-U$	$-I$	$-J$	$-K$
I	I	$-U$	K	$-J$	$-I$	U	$-K$	J
J	J	$-K$	$-U$	I	$-J$	K	U	$-I$
K	K	J	$-I$	$-U$	$-K$	$-J$	I	U
$-U$	$-U$	$-I$	$-J$	$-K$	U	I	J	K
$-I$	$-I$	U	$-K$	J	I	$-U$	K	$-J$
$-J$	$-J$	K	U	$-I$	J	$-K$	$-U$	I
$-K$	$-K$	$-J$	I	U	K	J	$-I$	$-U$

one-line notation

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

rows = H

identify group elements of Q with $\{1, 2, \ldots, 8\}$
read a row of Cayley table as a permutation in S_8,
in <u>one-line notation</u>

Convert to cyclenotation to answer (b)(c).

$$H = \{(1), (1256)(3478), (1357)(2864), (1458)(2367), (15)(26)(37)(48), (1652)(3874), (1753)(2468), (1854)(2763)\}$$

(b) No. (1) is even. the 5th one is even. The rest are products of 4-cycles which ~~each~~ reduce to $2 \cdot 3 = 6$ 2-cycles each.

(c) $U \quad I \quad -U \quad -I$ $\quad \{U, I, -U, -I\} = \langle I \rangle$, so $\phi(\{U, I, -U, -I\}) = \langle \phi(I) \rangle$
$= \langle (1256)(3478) \rangle$

III. Proofs. (15 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.

Prove ***ONE*** of 9-10. Clearly indicate which proofs you want graded.

For both 9 and 10, you may assume the following corollaries, of Theorem 4.1 and Lagrange's Theorem respectively, citing usage by "(*)" or "(**)":

Let G be a group and let $a \in G$ have order r. If $a^k = e$, then r divides k. (*)

Let G be a finite group. If $H \leq G$, then $|H|$ divides $|G|$. (**)

9. Let G be a finite group of order n. Let m be a positive integer with $\gcd(m, n) = 1$. If $g \in G$ and $g^m = e$, prove that $g = e$.

10. Let G be a finite group. Prove that if $|G| = p$ with p prime, then G is cyclic.

9. Since $g^m = e$, by (*), $|g|$ divides m.
Since $|g| = |\langle g \rangle|$, by (**), $|g| \mid n$.
$|g|$ is a common divisor of m and n and thus must divide $\gcd(m,n) = 1$.
The only possibility is $|g| = 1$ and so $g = e$ $\square$

10. Let $x \in G \setminus \{e\}$.
x exists since $|G|$ prime $\Rightarrow |G| \geq 2$.
By (**), $|x| = |\langle x \rangle|$ divides $|G|$.
Since $|G| = p$ is prime, ~~and~~ the possibilities are $|x| = 1$ and $|x| = p$.
But $x \neq e$ so $|x| \neq 1$.
Therefore $|x| = |\langle x \rangle| = p$, but $\langle x \rangle \subseteq G$ by closure,
so $\langle x \rangle = G$ and G is cyclic $\square$

Prove ***ONE*** out of 11-12. Clearly indicate which proof you want graded.

11. Let $\mathbb{C}^*$ be the nonzero complex numbers under multiplication. Let

$$M^* := \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\} \setminus \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}.$$

Prove that $\mathbb{C}^*$ is isomorphic to M^* under multiplication.

12. The "special orthogonal group" $\mathrm{SO}_2(\mathbb{R})$ is the group of rotations of the plane $\mathbb{R}^2$ defined as

$$\mathrm{SO}_2(\mathbb{R}) := \left\{ \begin{bmatrix} \cos\lambda & -\sin\lambda \\ \sin\lambda & \cos\lambda \end{bmatrix} : 0 \le \lambda < 2\pi \right\},$$

under multiplication. Prove that $\mathrm{SO}_2(\mathbb{R})$ is isomorphic to

$$G := \{a + bi \in \mathbb{C} : |a + bi| = 1\},$$

that is, the complex numbers with modulus 1, under multiplication. (Hint: it will be easier to define $\phi : \mathrm{SO}_2(\mathbb{R}) \to G$.)

11. Define $\varphi : \mathbb{C}^* \to M^*$ by $\varphi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

φ 1-1: Suppose $a+bi \neq c+di$.
Then either $a \neq c$ or $b \neq d$
so $\varphi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \neq \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \varphi(c+di)$.

φ onto: Let $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in M^*$. Then $a+bi \in \mathbb{C}^*$ since not both a, b can be 0 for $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ to be in M^*. Clearly $\varphi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

φ preserves operation: Let $a+bi$, $c+di \in \mathbb{C}^*$.

$$\varphi((a+bi)(c+di)) = \varphi(ac-bd+(ad+bc)i) = \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix}$$

$$\varphi(a+bi)\varphi(c+di) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-cb \\ bc+ad & -bd+ac \end{bmatrix} = \varphi((a+bi)(c+di))$$

Therefore φ is an isomorphism and $\mathbb{C}^* \cong M^*$.