

PRINT Last name: _____ First name: _____

Signature: _____ Student ID: _____

Math 430 Final, Fall 2006

I. Examples, Counterexamples and short answer. (4 pts ea.) Do not give proofs, but clearly indicate your proposed example or counterexample, or short answer where appropriate.

1. Define what makes a group cyclic. Give an example of a cyclic group with order > 1 .

Cyclic: $\exists g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\} = \langle g \rangle$

Ex. $G = \mathbb{Z}_2$

2. Define what makes a group Abelian. Give an example of an Abelian group which is not cyclic.

Abelian: $\forall g, h \in G, gh = hg$

Ex. $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$

3. Define the center of a group. Give an example of a non-Abelian group G such that its center $Z(G)$ has more than one element.

Center $Z(G) := \{g \in G : gx = xg \ \forall x \in G\}$

Ex. $G = D_4$

4. At least two types of groups we have studied have order > 1 and trivial center, i.e., $|Z(G)| = 1$. Give an example of such a group. (We could say that examples 1-4 represent a decreasing hierarchy of "Abelian-ness." The next step might be *simple groups*, which have no normal subgroups other than $\{e\}$ and the group itself.)

Ex. $G = D_5$

Prove **ONE** of 18-19. Clearly indicate which proof you want graded.

18. The elements of the Quaternion Q group are $\{\pm U, \pm I, \pm J, \pm K\}$ with identity U , where $I^2 = J^2 = K^2 = -U$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$, $IK = -J$, and $-$'s can be factored through; i.e., $(-G)(-H) = GH$ and $-(-G) = G$. Classify the possible homomorphic images of Q up to isomorphism.
19. Let $S = \left\{ \frac{m}{n} : m, n \in \mathbb{Z} \text{ and } n \text{ is odd} \right\}$. Prove or disprove that S is a subring of \mathbb{Q} , the rationals under addition and multiplication.

18. The normal subgroups of Q are $\{U\}$, $\langle -U \rangle$, $\langle I \rangle$, $\langle J \rangle$, $\langle K \rangle$, and Q .

The homomorphic images are Q/N for $N \triangleleft Q$.

$$Q/\{U\} \cong Q,$$

$$Q/\langle I \rangle \cong Q/\langle J \rangle \cong Q/\langle K \rangle \cong \mathbb{Z}_2$$

$$Q/Q \cong \{e\}.$$

For $Q/\langle U \rangle$: note $(I + \langle -U \rangle)^2 = (J + \langle -U \rangle)^2 = (K + \langle -U \rangle)^2 = \langle -U \rangle$
so no order 4 elts.

$$\text{Thus } Q/\langle -U \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

19. Subgroup: $0 \in S$ since $0 = \frac{0}{1}$, 1 odd.

Let $g, h \in S$. $g = \frac{m_1}{n_1}$, $h = \frac{m_2}{n_2}$, $m_1, m_2, n_1, n_2 \in \mathbb{Z}$, n_1, n_2 odd.

$$g-h = \frac{m_1}{n_1} - \frac{m_2}{n_2} = \frac{m_1 n_2 - m_2 n_1}{n_1 n_2}, \quad n_1 n_2 \text{ odd} \Rightarrow g-h \in S.$$

By 1-step subgroup test, $S \leq \mathbb{Q}$.

Closure under mult:

Let $g, h \in S$ with form above.

$$gh = \frac{m_1 m_2}{n_1 n_2}, \quad \text{where } n_1 n_2 \text{ odd} \Rightarrow gh \in S.$$

$\therefore S$ is a subring of \mathbb{Q} .

III. Proofs. (12 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 13-14. Clearly indicate which proof you want graded.

13. Assume that whenever a, b, c belong to the group G , if $ab = ca$, then $b = c$. Prove as a result that G is Abelian.
14. Prove that if a_1, \dots, a_n are distinct elements of the group G , and $b \in G$, then ba_1, \dots, ba_n are distinct elements of G .

13. Let $g, h \in G$.

$$g(h) = (ghg^{-1})g$$

$$\Rightarrow h = ghg^{-1} \text{ by assumption}$$

$$hg = gh \quad \therefore G \text{ Abelian.}$$

14. Assume ~~to~~ a_1, \dots, a_n distinct and assume to the contrary that

$$ba_i = ba_j \quad \text{for } i \neq j.$$

by cancellation, $a_i = a_j$ ~~✗✗~~

II. Constructions and Algorithms. (12 pts ea.) Do not write proofs, but do give clear, concise answers, including steps to algorithms where applicable.

11. (a) On the left side, list all Abelian groups of order 180 up to isomorphism, by expressing them as external direct products of cyclic groups of prime power order.
 (b) On the right side, for each group in your list on the left, re-express it in the form $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ where $n_i | n_{i-1}$ for all $1 < i \leq k$.

$$180 = 18 \cdot 10 = \cancel{2 \cdot 2} \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$$

| | |
|--|---------------------------------------|
| $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$ | \mathbb{Z}_{180} |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$ | $\mathbb{Z}_{90} \oplus \mathbb{Z}_2$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ | $\mathbb{Z}_{30} \oplus \mathbb{Z}_6$ |
| $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ | $\mathbb{Z}_{60} \oplus \mathbb{Z}_3$ |

5. What is the order of the element $6 + \langle 8 \rangle$ in the factor group $\mathbb{Z}_{48}/\langle 8 \rangle$?

$$(6 + \langle 8 \rangle)(6 + \langle 8 \rangle) = 4 + \langle 8 \rangle \neq \langle 8 \rangle$$

$$(6 + \langle 8 \rangle)(4 + \langle 8 \rangle) = 2 + \langle 8 \rangle \neq \langle 8 \rangle$$

$$(6 + \langle 8 \rangle)(2 + \langle 8 \rangle) = \langle 8 \rangle$$

$$\therefore |6 + \langle 8 \rangle| = 4$$

6. Find all elements $g \in U(9)$ such that $\langle g \rangle = U(9)$.

$$U(9) = \{1, 2, 4, 5, 7, 8\}$$

$$2 \cdot 2 = 4 \quad 4 \cdot 2 = 8 \quad 8 \cdot 2 = 7 \quad \dots \Rightarrow U(9) = \langle 2 \rangle$$

$$4 \cdot 4 = 7 \quad 7 \cdot 4 = 1$$

$$8 \cdot 5 = 7 \quad 7 \cdot 5 = 8 \quad 8 \cdot 5 = 4 \quad 4 \cdot 5 = 2 \dots \quad U(9) = \langle 5 \rangle$$

$$7 \cdot 7 = 4 \quad 4 \cdot 7 = 1$$

$$8 \cdot 8 = 1$$

$$\left(\text{since } U(9) \cong \mathbb{Z}_6, \varphi(6) = 2 = |\{2, 5\}| \right)$$

7. Find a homomorphism ϕ from \mathbb{Z} to some other group G such that $\mathbb{Z}/\text{Ker}\phi \cong \mathbb{Z}_6$.

$$\text{define } \varphi: \mathbb{Z} \rightarrow \mathbb{Z}_6$$

$$\text{by } \varphi(n) = n \pmod{6}$$

8. Find the number of order 2 elements in $D_6 \oplus D_4$. For partial credit, it is necessary to describe each element you find, or at least explain the combinatorial enumeration.

in D_6 : R_{180}, F_1, \dots, F_6
 in D_4 : R_{180}, E_1, \dots, E_4
 counting R_0 except (R_0, R_0) , ^{tuples} products are
 $8 \cdot 6 - 1 = 47$

9. Write the permutation (12345) as a product of 2-cycles.

$$(12345) = (15)(14)(13)(12)$$

10. Write 1 as an integer combination of 11 and 19.

$$\begin{aligned}
 19 &= 1 \cdot 11 + 8 \\
 11 &= 1 \cdot 8 + 3 \\
 8 &= 2 \cdot 3 + 2 \\
 3 &= 1 \cdot 2 + 1 \\
 2 &= 2 \cdot 1 + 0
 \end{aligned}
 \quad \rightarrow \quad
 \begin{aligned}
 1 &= 3 - 1 \cdot 2 \\
 &= 3 - 1 \cdot (8 - 2 \cdot 3) \\
 &= 3 \cdot 3 - 1 \cdot 8 \\
 &= 3 \cdot (11 - 1 \cdot 8) - 1 \cdot 8 \\
 &= 3 \cdot 11 - 4 \cdot 8 \\
 &= 3 \cdot 11 - 4 \cdot (19 - 1 \cdot 11) \\
 1 &= 7 \cdot 11 - 4 \cdot 19
 \end{aligned}$$

12. A certain group of order 6 is generated by the elements a and b , where $|a| = 3$, $|b| = 2$ and $ab = ba^2$. Complete the Cayley table for the group, expressing each group element in the form $a^n b^m$ or $b^m a^n$ with $n, m \geq 0$.

| | e | a | b | a^2 | ab | ba |
|-------|-------|-------|-------|-------|-------|-------|
| e | e | a | b | a^2 | ab | ba |
| a | a | a^2 | ab | e | ba | b |
| b | b | ba | e | ab | a^2 | a |
| a^2 | a^2 | e | ba | a | b | ab |
| ab | ab | b | a | ba | e | a^2 |
| ba | ba | ab | a^2 | b | a | e |

for ab :

$$aab = aba^2 = ba^4 = ba$$

take ba as a new element.

$$ba = e \Rightarrow a = b^{-1} = b \quad \#$$

$$ba = a \Rightarrow b = e \quad \#$$

$$ba = b \Rightarrow a = e \quad \#$$

$$ba = a^2 \Rightarrow b = a \quad \#$$

$$ba = ab = ba^2 \Rightarrow a = e \quad \#$$

Now complete the table.

$$aab = ba$$

$$aba = ba^3$$

$$bab = bba^2 = a^2$$

$$|a| = 3 \Rightarrow a^2 \neq a, e$$

$$|b| = 2 \Rightarrow b^{-1} = b.$$

$$|a| = 3 \Rightarrow |a^2| = 3 \Rightarrow a^2 \neq b.$$

take ab as a new element:

$$ab = e \Rightarrow a = b^{-1} = b \quad \#$$

$$ab = a \Rightarrow b = e \quad \#$$

$$ab = b \Rightarrow a = e \quad \#$$

$$ab = a^2 \Rightarrow a = b \quad \#$$

Prove **ONE** of 15-17. Clearly indicate which proof you want graded.

15. Let \mathbb{C}^* be the nonzero complex numbers under multiplication, and let $U = \{a + bi \in \mathbb{C} : \sqrt{a^2 + b^2} = 1\}$. Assuming that \mathbb{C}^* is a group, prove that U is a subgroup of \mathbb{C}^* .
16. Prove that there is no largest finite subgroup of the nonzero complex numbers \mathbb{C}^* under multiplication.
17. Let $G = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z} \right\}$. Prove that G under multiplication is isomorphic to \mathbb{Z} under addition. (Don't skimp on the steps!)

15. U nonempty: $1+0i \in U$ since $\sqrt{1^2+0^2} = 1$.

Let $g, h \in U$; $g = a+bi$ $h = c+di$.

$$gh^{-1} = \frac{a+bi}{c+di} \frac{(c-di)}{(c-di)} = \frac{(ac+bd) + i(bc-ad)}{c^2+d^2} = \frac{(ac+bd)}{c^2+d^2} + i \frac{(bc-ad)}{c^2+d^2}$$

$$\begin{aligned} \text{with modulus } \sqrt{(ac+bd)^2 + (bc-ad)^2} &= \sqrt{(ac)^2 + 2abcd + (bd)^2 + (bc)^2 - 2abcd + (ad)^2} \\ &= \sqrt{a^2(c^2+d^2) + b^2(c^2+d^2)} = \sqrt{(a^2+b^2)(c^2+d^2)} = 1 \Rightarrow gh^{-1} \in U \end{aligned}$$

By 1-step subgroup test, $U \leq \mathbb{C}^*$.

16. Let $n \in \mathbb{Z}_{>0}$, $g = e^{i2\pi/n} \in \mathbb{C}^*$. $\langle g \rangle \leq \mathbb{C}^*$, and
 $1 = (e^{i2\pi/n})^n$, $(e^{i2\pi/n})^j \neq 1$ for $1 \leq j < n$
 so $|\langle g \rangle| = n$. Let $n \rightarrow \infty$ for the claim.

17. Define $\psi: G \rightarrow \mathbb{Z}$ by $\psi\left(\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\right) = n$.

1-1: suppose $\psi(g) = \psi(h)$, where
 $g = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, $h = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ for some $n, m \in \mathbb{Z}$.
 then $n = m$, and so $g = h$.

onto: let $n \in \mathbb{Z}$, then $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \in G$ and $\psi\left(\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\right) = n$.

op. prop.: $\psi\left(\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\right) = \psi\left(\begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix}\right) = m+n = \psi\left(\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}\right) + \psi\left(\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\right)$

$\therefore \psi$ is an isomorphism.