1 Mathematics 433-A Fall 2000

1.1 Key Exam 1

October 6, 2000 **Mr. Key**

____
Name

1.2 General Comments on the Examination

1. The class as a whole did quite well on this examination. This tells me most of you have at least a purple belt in "Math Fu". In particular, you have developed the intermediate level of analyzing and proving a mathematical problem. To wit,
   (a) Write down the given information.
   (b) Write down the final statement that will finalize the proof.
   (c) Fill in the details between the above two statements.
      i. The first and most important thing to do is to **write out the definitions** of all of the mathematical information given in the problem. With the partial exception of problem 6 , all of these proofs should flow nicely from this approach.
2. I suggest those of you who did not nail the induction problem should make it a point to work more of these. Mathematical induction is an important tool we will use constantly throughout the course. I will be happy to suggest problems from our text - just ask.

The Problems with solutions

1. (6 points each) Give the definitions of the following.
   (a) The **general linear** group of order n over the real numbers $GL(n, \mathbf{R})$.(Include the binary operation.)
   (b) The **center** of a group G, $Z(G)$.
   (c) The **centralizer** of an element a in a group G.
   (d) A **normal** subgroup N of a group G.
   (e) A **homomorphism** from the group G to the group G'.
2. (5 points each) Give examples of the following.
   (a) A group that is not abelian.
   (b) A finite, nontrivial, abelian group.
3. (15 points) Use one of the principles of mathematical induction to prove if a, b, c are elements in a group G for which $b = cac^{-1}$, then $b^n = ca^nc^{-1}$ is true for all positive integers n.

   Proof: Let S be the set of all positive integers n for which the statement $b^n = ca^nc^{-1}$ is true.

   $1 \in S$ since $b^1 = ca^1c^{-1}$ is given.

   As the induction hypothesis, suppose $n \in S$. That is, $b^n = ca^nc^{-1}$.

   Then, $b^{n+1} = bb^n = (cac^{-1})(ca^nc^{-1}) = caea^nc^{-1} = ca^{n+1}c^{-1}$.

   Thus, if $n \in S$, then $(n+1) \in S$ and by the First Principle of Mathematical Induction, $S = Z^+$.

4. (15 points) Given a group G, subgroup H of G and element $g \in G$,we define the **conjugate subgroup of** H in G to be the set

$$gHg^{-1} = \left\{ghg^{-1} : h \in H\right\}.$$

Prove gHg^{-1} is indeed a subgroup of G.

Proof:

(a) Let ghg^{-1} and $gh'g^{-1}$ be arbitrary elements of gHg^{-1}. Thus, $h, h' \in H$ and $hh' \in H$ since H is a sugroup and thus closed under the group operation.
Then gHg^{-1} is **closed** since the product $(ghg^{-1})(gh'g^{-1}) = gheh'g^{-1} = g(hh')g^{-1} \in gHg^{-1}$.

(b) Since the set gHg^{-1} is a subset of G and the elements of G associate under the binary operation of G, then the elements of gHg^{-1} **associate** under the same operation.

(c) The group G has an identity element e. Since $e = geg^{-1}$, we see that the set gHg^{-1} **contains the identity.**

(d) Let ghg^{-1} be any element of gHg^{-1}. Then $h \in H$ and since H is a subgroup of G, $h^{-1} \in H$.
Since $(ghg^{-1})(gh^{-1}g^{-1}) = gheh^{-1}g^{-1} = geg^{-1} = e$ and $(gh^{-1}g^{-1})(ghg^{-1}) = gheh^{-1}g^{-1} = geg^{-1} = e$,
we see that $gh^{-1}g^{-1}$ is the inverse element of ghg^{-1}. And since $h^{-1} \in H$, we have $gh^{-1}g^{-1} \in gHg^{-1}$ and the set gHg^{-1} is **closed under inverses.**

5. (15 points) Given a homomorphism $\phi : G \to G'$ and a subgroup H of G, prove

$$\ker(\phi|_H) = \ker(\phi) \cap H.$$

Proof: Note

(a) $\phi|_H : H \to G'$ is defined by $\phi|_H(h) = \phi(h)$ for all $h \in H$.

(b) $\ker(\phi|_H) = \{h \in H : \phi|_H(h) = \phi(h) = e'\}$

(c) $\ker(\phi) = \{g \in G : \phi(g) = e'\}$.

Thus, If $x \in \ker(\phi|_H)$, then $x \in H$ (the domain of $\phi|_H$) and $\phi(x) = e'$ so $x \in \ker(\phi)$. Thus, $\ker(\phi|_H) \subset (\ker(\phi) \cap H)$.

And, if $x \in (\ker(\phi) \cap H)$, then $x \in H$ (the domain of $\phi|_H$) and $e' = \phi(x) = \phi|_H(x)$ so $x \in \ker(\phi|_H)$. Thus, $(\ker(\phi) \cap H) \subset \ker(\phi|_H)$.

Hence the two sets $\ker(\phi|_H)$ and $(\ker(\phi) \cap H)$ are equal.

6. (15 points) Do any **one** of the following.

(a) Prove that, in any group, the order of the product ab is the same as the order of the product ba.

Proof: Note first that If there is an integer n for which $(ab)^n = e$ if and only if $(ba)^n = e$, then either both (ab) and (ba) have infinite order, or, if one of them has order n then so does the other.

Hence, we need only prove the following lemma.

Lemma 1 *$(ab)^n = e$ if and only if $(ba)^n = e$.*

Proof of Lemma: *Suppose $(ab)^n = e$ for some positive integer n.*
Then, $ab\,(ab)^{n-1} = e$ which implies $a^{-1}(ab)(ab)^{n-1}a = a^{-1}ea$.
This simplifies to $b\,(ab)^{n-1}a = e$ which is just $(ba)^n = e$.
Since each of the above steps is reversible, we have finished the proof of the lemma.

(b) If G contains exactly one element of order 2,prove that element is in the center of G. [Hint: consider conjugates of that element.]

Proof: Denote the special element of order 2 by a and let c be any element of G.
Then, by problem 3, $(cac^{-1})^2 = ca^2c^{-1} = cec^{-1} = e$.
Since a is the only element that equals e when squared, then $cac^{-1} = a$ or $ca = ac$. Since a commutes with every element of G , then a is in the center of G.

(c) Let G be an abelian group of odd order. Prove the map $\phi : G \to G$ defined by $\phi(x) = x^2$ is an automorphism.

Proof:

i. ϕ preserves the group operations because G is abelian. Specifically, if $a, b \in G$, then $\phi(ab) = (ab)^2 = abab = aabb = a^2b^2 = \phi(a)\phi(b)$.

ii. ϕ is one-to-one if and only if $\ker(\phi) = \{e\}$ by a result proven in class. It is also in Theorem 10.1 of the third edition of our text (I don't have a copy of the fourth edition at home to look it up - sorry.)
So suppose $x \in \ker\phi$. That is, $\phi(x) = x^2 = e$. Denote the (odd) order of G by $2n+1$. Then, since $|x|$ divides $|G|$ by Lagrange's Theorem we have

$$e = e^{n+1} = \left(x^2\right)^{n+1} = x^{2n+1}x = ex = x$$

and we conclude $\ker(\phi) = \{e\}$. Thus, ϕ is one-to-one.

iii. Any one-to-one function that maps from a finite set to the same set is automatically onto. However, to prove this about ϕ directly, let y be arbitrary in the codomain and consider $y^{n+1} \in G$ (the domain) where the order of G is $2n+1$.
Then, $\phi(y^{n+1}) = (y^{n+1})^2 = y^{2n+1}y = ey = y$ and ϕ is onto.