FIRST MIDTERM
MATH 100A, UCSD, AUTUMN 16

You have 50 minutes.

There are 5 problems, and the total number of points is 65. Show all your work. Please make your work as clear and easy to follow as possible.

Name:______________________________
Signature:__________________________

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>65</td>
<td></td>
</tr>
</tbody>
</table>
1. (15pts) Give the definition of a group.

A group is a set $G$ together with a binary operation $\ast$ such that
(1) $\ast$ is associative. That is, for all $a, b$ and $c \in G$
$$a \ast (b \ast c) = (a \ast b) \ast c.$$  
(2) There is an element $e \in G$, called the identity, with the following property. For all $a \in G$,
$$e \ast a = a \ast e = a.$$  
(3) Every element $a \in G$ has an inverse $b$, which satisfies the following property.
$$a \ast b = b \ast a = e.$$  

(ii) Let $G$ be a group and let $S$ be a subset of $G$. Give the definition of the subgroup generated by $S$.

$\langle S \rangle$ is the smallest subgroup of $G$ that contains $S$.

(iii) Let $G$ be a group and $H$ a subgroup. Give the definition of a left coset.

Let $a \in G$. The left coset of $a$ is
$$aH = \{ ah \mid h \in H \}.$$
2. (15pts) (i) Give a description of the group $D_3$ of symmetries of a triangle.

Let $I$ be the identity, $R$ rotation through $120^\circ$ and let $F_1$, $F_2$, $F_3$ be the three flips. Then $G = \{I, R, R^2, F_1, F_2, F_3\}$.

(ii) List all subgroups of $D_3$.

$\{e\}$, $\{I, F_i\}$, $i = 1, 2, 3$, $\{I, R, R^2\}$, and finally the whole of $G$.

(iii) Find the left cosets, for one subgroup of order two and one subgroup of order three.

Take $H = \{I, F_1\}$. Then there are three left cosets,

$[I] = H = \{I, F_1\} = [F_1]$
$[F_2] = F_2H = \{F_2, R\} = [R]$
$[F_3] = F_3H = \{F_3, R^2\} = [R^2]$

Take $H = \{I, R, R^2\}$. Then there are two left cosets,

$[I] = H = \{I, R, R^2\} = [R] = [R^2]$
$[F_1] = F_2H = \{F_1, F_2, F_3\} = [F_2] = [F_3]$. 
3. (10pts) Let \( G \) be a group and let \( H \) be a subgroup. Define a relation \( \sim \) by the rule \( a \sim b \) if and only if \( a^{-1}b \in H \). Prove that \( \sim \) is an equivalence relation. What are the equivalence classes?

We have to check three things. First we check reflexivity. Suppose that \( a \in G \). Then \( a^{-1}a = e \). As \( H \) is a subgroup, it certainly contains \( e \) and \( a \sim a \). Thus reflexivity holds.

Now we check symmetry. Suppose that \( a, b \in G \) and that \( a \sim b \). Then \( h = a^{-1}b \in H \). As \( H \) is a subgroup, it contains \( h^{-1} = b^{-1}a \). But then \( b \sim a \). Thus symmetry holds.

Now we check transitivity. Suppose that \( a, b, c \in G \) and that \( a \sim b \), \( b \sim c \). Then \( h = a^{-1}b \in H \) and \( k = b^{-1}c \in H \). As \( H \) is a subgroup, it contains the product \( hk = (a^{-1}b)(b^{-1}c) = a^{-1}c \). But then \( c \sim a \). Thus transitivity holds.

The equivalence classes are precisely the left cosets.
4. (10pts) If $G$ is a group and $g \in G$ is an element of $G$ show that the centraliser $C_g$ is a subgroup of $G$.

$eg = ge$ so that $e \in C_g$ and the centraliser is non-empty. Therefore it suffices to prove that $C_g$ is closed under multiplication and taking inverses. Suppose that $h$ and $k$ are two elements of $C_g$. We show that the product $hk$ is an element of $C_g$. We have to prove that $(hk)g = g(hk)$.

\[
(hk)g = h(kg) \quad \text{by associativity} \\
= h(gk) \quad \text{as } k \in C_g \\
= (hg)k \quad \text{by associativity} \\
= (gh)k \quad \text{as } h \in C_g \\
= g(hk) \quad \text{by associativity}.
\]

Thus $hk \in C_g$ and $C_g$ is closed under multiplication. Now suppose that $h \in G$. We show that the inverse of $h$ is in $G$. We have to show that $h^{-1}g = gh^{-1}$. Suppose we start with the equality $hg = gh$.

Multiply both sides by $h^{-1}$ on the left. We get $h^{-1}(hg) = h^{-1}(gh)$, so that simplifying we get $g = (h^{-1}g)h$.

Now multiply both sides of this equality by $h^{-1}$ on the right, $gh^{-1} = (h^{-1}g)(hh^{-1})$. Simplifying we get $h^{-1}g = gh^{-1}$ which is what we want. Thus $h^{-1} \in C_g$. Thus $C_g$ is closed under taking inverses and so $C_g$ is a subgroup.
5. (15pts) (i) Carefully state (but do not prove) Lagrange’s Theorem.

Let $G$ be a group and let $H$ be a subgroup. Then

$$|G| = |H||[G : H]|,$$

where $[G : H]$ counts the number of left cosets. In particular if $G$ is finite, then the order of $H$ divides the order of $G$.

(ii) Show that if $G$ is a group of order a prime $p$, then $G$ does not contain any proper subgroups.

Let $H$ be a subgroup of $G$. Then $|H|$ divides $|G| = p$. As $p$ is prime, this means that $|H| = 1$ or $p$. If the order of $H$ is 1, then $H = \{e\}$ and if the order of $H$ is $p$, then $H = G$. Thus $G$ has no proper subgroups.
6. (10pts) Prove Lagrange’s Theorem.

Let \( G \) be a group and let \( H \) be a subgroup. Then

\[
|G| = |H|[G : H].
\]

Since the left cosets of \( H \) partition \( G \) into a disjoint union of subsets, and the number of left cosets is precisely equal to \([G : H]\), it is enough to prove that each left coset has the same cardinality as \( H \).

Let \( a \in G \). Define a map

\[
f : H \rightarrow aH
\]

by setting \( f(h) = ah \). We want to show that \( f \) is bijection. The easiest way to proceed is to find the inverse \( g \) of \( f \). Define a map

\[
g : aH \rightarrow G
\]

by setting \( g(k) = a^{-1}k \). It is clear that the composition, either way, is equal to the identity, as \( a^{-1}a = aa^{-1} = e \). But then \( f \) is a bijection and \( H \) and \( gH \) have the same cardinality.
7. (10pts) Give an example of a countable group that is not finitely generated (that is a group which is not generated by any finite subset). There are two natural examples.

The first is to look at the rational numbers under addition. \( \mathbb{Q} \) is certainly countable. Suppose that \( g_1, g_2, \ldots, g_k \) were a finite set of generators. Each \( g_i \) is a rational number, say of the form \( \frac{a_i}{b_i} \). Now let \( b \) be the least common multiple of the \( b_1, b_2, \ldots, b_k \). Then any element which is a finite sum or difference of the \( g_1, g_2, \ldots, g_k \) will be of the form \( \frac{a}{b} \), for some integer \( a \). But most rationals are not of this form. Thus \( \mathbb{Q} \) is not finitely generated.

For point of reference, here is an example from latter on in the class:

The second is to look at the group \( A(\mathbb{N}) \) of permutations of the natural numbers. Now this is not countable, but consider the subgroup \( G \) consisting of all permutations that fix all but finitely many natural numbers. Note that \( A(\mathbb{N}) \) contains a nested sequence of copies of \( S_n \), for all \( n \), in an obvious way and that \( G \) is in fact the union of these finite subgroups.

In particular \( G \) is countable, as it is the countable union of countable sets. Now suppose that \( g_1, g_2, \ldots, g_k \) were a finite set of generators. Then in fact there is some \( n \) such that \( g_i \in S_n \), for all \( i \). As \( S_n \) is a subgroup of \( G \), it follows that

\[
\langle g_1, g_2, \ldots, g_k \rangle \subset S_n \neq G,
\]

a contradiction. Put differently, no finite subset generates \( G \), since any finite subset will only permute finitely many natural numbers.