FIRST MIDTERM
MATH 100A, UCSD, AUTUMN 23

You have 80 minutes.

There are 5 problems, and the total number of points is 70. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:______________________________

Signature:___________________________

Student ID #:_________________________

Section instructor:____________________

Section Time:________________________

Problem	Points	Score
1	15	
2	20	
3	10	
4	10	
5	15	
6	10	
7	10	
Total	70	

1. (15pts) *Give the definition of a group.*

A group is a set G together with a binary operation $*$ such that

(1) $*$ is associative. That is, for all a, b and $c \in G$

$$a * (b * c) = (a * b) * c.$$

(2) There is an element $e \in G$, called the identity, with the following property. For all $a \in G$,

$$e * a = a * e = a.$$

(3) Every element $a \in G$ has an inverse b, which satisfies the following property.

$$a * b = b * a = e.$$

(ii) *Give the definition of the centre $Z(G)$ of a group G.*

$$Z(G) = \{\, a \in G \mid \text{for every } b \in G,\ ab = ba \,\}..$$

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

Let $a \in G$. The right coset of a is

$$Ha = \{\, ha \mid h \in H \,\}.$$

2. (20pts) (i) *Give a description of the group D_4 of symmetries of a square.*

Label the vertices A, B, C and D, going clockwise from the top left. We have

$$D_4 = \{ I, R, R^2, R^3, R^4, D_1, D_2, F_1, F_2 \},$$

where R is rotation through $\pi/2$, D_1 is the diagonal flip about AC, D_2 is the diagonal flip about BD, F_1 is the horizontal flip, switch A and D, B and C and F_2 is the vertical flip, switch A and B, C and D.
This gives 8 symmetries. I claim this is all of them.
In fact any symmetry is determined by its action on the fours vertices A, B, C and D. Now there are $24 = 4!$ possible such permutations. But any symmetry of a square must fix opposite corners. Thus once we have decided where to send A, for which there are four possibilities, the position of C is determined, it is opposite to A. There are then two possible positions for B. So there are at most eight symmetries and we have listed all of them.

(ii) *List all subgroups of D_4.*

The order of D_4 is 8 and so the order of a subgroup H of D_4 is 1, 2, 4 or 8.
If it is 1 then $H = \{I\}$ and if it is 8 then $H = D_4$. If the order of H is two then H has two elements, one is the identity and the other is its own inverse. There are five such elements, F_1, F_2, D_1, D_2 and R^2. Thus the two element subgroups are

$$\{I, F_1\}, \qquad \{I, F_2\}, \qquad \{I, D_1\}, \qquad \{I, D_2\}, \qquad \text{and} \qquad \{I, R^2\}.$$

We start looking for subgroups. Two trivial examples are
A non-trivial example is afforded by the set of all rotations $\{I, R, R^2, R^3\}$. Clearly closed under products and inverses. Note that rotation through π radians R^2 generates the subgroup
Simliarly, since any flip is its own inverse, the following are all subgroups,
Now try combining side flips and diagonal flips. Now $F_1D_1 = R^3$. So any subgroup that contains F_1 and D_1 must contain R^3 and hence all rotations. From there it is easy to see we will get the whole of G. So we cannot combine side flips with diagonal flips.
Now consider combining rotations and flips. Note that $F_1F_2 = R^2$ and $D_1D_2 = R^2$ by direct computation. We then try to see if

$$\{I, F_1, F_2, R^2\}$$

is a subgroup. As this is finite, it suffices to check that it is closed under products. We look at pairwise products. If one of the terms is I this is clear. We already checked F_1F_2. It remains to check F_1R^2 and F_2R^2. Consider the equation $F_1F_2 = R^2$. Multiplying by F_1 on the left, and using the fact that it is its own inverse, we get $F_2 = F_1R^2$. Similarly all other products, of any two of F_1, F_2 and R^2, gives the third. Thus

$$\{I, F_1, F_2, R^2\}$$

is a subgroup.
Similarly

$$\{I, D_1, D_2, R^2\}$$

is a subgroup.

(iii) Find the left cosets (up to the obvious symmetries of the subgroups).

In the notation of the first question from homework 2, there are eight subgroups of D_4, up to symmetries.

$\{I\}, \{I, R^2\}, \{I, F_1\}, \{I, D_1\}, \{I, R, R^2, R^3\}, \{I, D_1, D_2, R^2\}, \{I, F_1, F_2, R^2\}, D_4$.

D_4 has one left and one right coset, D_4 itself. At the other extreme the left and right cosets of $\{I\}$ are the eight one element subsets of D_4,

$$\{\{I\}, \{R\}, \{R^2\}, \{R^3\}, \{D_1\}, \{D_2\}, \{F_1\}, \{F_2\}\}.$$

The three subgroups of order 4 have one other coset (both left and right), the complement of the subgroup:

$$\{\{I, R, R^2, R^3\}, \{D_1, D_2, F_1, F_2\}\},$$
$$\{\{I, D_1, D_2, R^2\}, \{R, R^3, F_1, F_2\}\},$$
$$\{\{I, F_1, F_2, R^2\}, \{R, R^3, D_1, D_2\}\}.$$

Now we attack the three subgroups of order 2. We are looking for four subsets of order 2.

If we start with $H = \{I, R^2\}$ then we get the partition

$$\{\{I, R^2\}, \{R, R^3\}, \{D_1, D_2\}, \{F_1, F_2\}\},$$

regardless of whether we look at left or right cosets.

If we start with $H = \{I, F_1\}$ then we get the two partitions

$\{\{I, F_1\}, \{R, D_1\}, \{R^2, F_2\}, \{R^3, D_2\}\}$ and $\{\{I, F_1\}, \{R, D_2\}, \{R^2, F_2\}, \{R^3, D_1\}\}$.

Finally, if we start with $H = \{I, D_1\}$ then we get the two partitions

$\{\{I, D_1\}, \{R, F_2\}, \{R^2, D_2\}, \{R^3, F_1\}\}$ and $\{\{I, D_1\}, \{R, F_1\}, \{R^2, D_2\}, \{R^3, F_2\}\}$.

4. (10pts) *True or False? If true then prove the result and if false then give a counterexample.*
(i) *The union of two subgroups of a group is a subgroup.*

False. Let $G = D_3$, $H = \{I, F_1\}$ and $K = \{I, F_2\}$. Then H and K are both subgroups of G but the union

$$H \cup K = \{I, F_1, F_2\},$$

is not.

(ii) *The intersection of two subgroups of a group is a subgroup.*

True. Suppose that H and K are subgroups of G. The intersection is non-empty as it contains e. We check that $H \cap K$ is closed under products and inverses.
Suppose that a and $b \in H \cap K$. Then a and $b \in H$ and a and $b \in K$. As H is a subgroup, $ab \in H$ and as K is a subgroup, $ab \in K$. But then $ab \in H \cap K$ and $H \cap K$ is closed under products.
Suppose that $a \in H \cap K$. Then $a \in H$ and $a \in K$. As H is a subgroup, $a^{-1} \in H$ and as K is a subgroup, $a^{-1} \in K$. But then $a^{-1} \in H \cap K$ and $H \cap K$ is closed under inverses.
As $H \cap K$ is closed under products and inverses it is a subgroup.

4. (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.

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 finite group with identity e and there is an element $a \in G$ such that $a^2 = e$ then either $a = e$ or G has even order.*

As $a^2 = e$ the order of a is either 1 or 2. If the order of G is odd it cannot be 2 by Lagrange. Thus the order of a is one. But then $x = e$.

Bonus Challenge Problems

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

$$f \colon H \longrightarrow aH$$

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

$$g \colon aH \longrightarrow G$$

by setting $f(k) = a^{-1}k$. 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) *Find the centre $Z(D_n)$ of the dihedral group D_n of order $2n$.*

The dihedral group is the group of symmetries of a regular n-gon. One obvious symmetry is rotation R through $2\pi/n$. The powers of R give n distinct rotations, including I. One can also write down a flip F. If n is odd then F flips about a vertex and the centre of the opposite side; if n is even then F flips about two opposite vertices.
Consider the subgroup $H = \langle R, F\rangle$ generated by R and F. H contains the subgroup of all rotations $\langle R\rangle$ which has order n. Thus the order of H is a multiple of n by Lagrange. It contains more than n elements and so it must contain at least $2n$ elements.
On the other hand if A and B are adjacent vertices then any symmetry of an n-gon is determined by where it sends A and B. There are n possible places to send A. The image of B is then adjacent to A and so there are two choices for the image of B.
Thus there are at most $2n$ symmetries. It follows that $H = D_n$. In fact

$$R^i \qquad \text{and} \qquad FR^i \qquad \text{where } 0 \leq i < n.$$

are $2n$ distinct elements of D_n, so that these are the elements of D_n.
Note that h commutes with g if and only if

$$hgh^{-1} = g.$$

Thus $g \notin Z(G)$ if

$$hgh^{-1} \neq g$$

for some $h \in G$.
h belongs to the centre if and only if h commutes with every $g \in G$. It is enough to check h commutes with every generator. So it suffices to check that h commutes with F and R.
We may suppose that the rotation R sends A to B and that F fixes A and sends B to the other vertex Z adjacent to A.
Note that

$$FRF^{-1} = FRF = R^{-1}.$$

We check that both sides have the same effect on the vertices A and B. F sends A to A, R sends A to B and F sends B to Z. On the other hand F sends B to Z, R sends Z to A and F sends A to A. Thus FRF sends A to Z and B to A. This is precisely what R^{-1} does.
Thus

$$FR^iF = R^{-i} = R^{n-i}.$$

This is not equal to R^i unless

$$i = n - i \qquad \text{that is} \qquad 2i = n.$$

This is only possible if $n = 2m$ is even.
If R^m is in the centre as it commutes with R and F.
On the other hand

$$\begin{aligned} F(FR^i)F^{-1} &= F(FR^iF^{-1}) \\ &= FR^{-i}. \end{aligned}$$

Thus FR^i is not in the centre, unless n is even and $i = m$. We argue that FR^m is not in the centre.
There are two ways to proceed. For the first note that FR^m is a flip. Flips come in families, up to symmetries, and so it is not possible for only one member of the family to be in the centre. Thus FR^m is not in the centre.
For the second, we simply compute. Note that

$$RFR^{-1} = FR^{-2}.$$

We check that both sides have the same effect on the vertices A and B. R^{-1} sends A to Z, F sends Z to B and R sends B to C. On the other hand R^{-1} sends B to A, F sends A to A and R sends A to B. Thus RFR^{-1} sends A to C and fixes B. This is precisely what R^{-2} does.
It follows that

$$\begin{aligned} R(FR^m)R^{-1} &= (RFR^{-1})R^m \\ &= FR^{-2}R^m \\ &= FR^{m-2}. \end{aligned}$$

This is not equal to R^m as $n > 2$.
Finally F is not in the centre.
Thus the centre depends on the parity of n

$$Z(D_n) = \begin{cases} \{I, R^m\} & \text{if } n = 2m \text{ is even} \\ \{I\} & \text{if } n \text{ is odd.} \end{cases}$$