FINAL EXAM
MATH 100A, UCSD, AUTUMN 23

You have three hours.

There are 8 problems, and the total number of points is 95. 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	10	
3	15	
4	15	
5	10	
6	10	
7	10	
8	10	
9	10	
10	10	
11	10	
12	10	
13	10	
Total	95	

1. (15pts) *Give the definition of the centre $Z(G)$ of a group G.*

$$Z(G) = \{\, z \in G \mid zg = gz \text{ for all } g \in G \,\}.$$

(ii) *Give the definition of the kernel of a homomorphism.*

If

$$\phi\colon G \longrightarrow G'$$

is a homomorphism then

$$\operatorname{Ker}(\phi) = \{\, g \in G \mid \phi(g) = g \,\}.$$

(iii) *Give the definition of S_n.*

The group of permutations of the first n integers.

2. (10pts) *Compute* $(23)^{37} \mod 17$.

First note that 23 is congruent to 6 modulo 17. So it is enough to calculate 6^{37} modulo 17. 17 is prime and so by Fermat's little theorem we have 6^{16} is congruent to one modulo 17. Putting all of this together and working modulo 17 we have

$$\begin{aligned}(23)^{37} &= 6^{37} \\ &= 6^{32} \cdot 6^5 \\ &= (6^{16})^2 \cdot 6^5 \\ &= 6^5 \\ &= 6 \cdot (36)^2 \\ &= 6 \cdot 2^2 \\ &= 24 \\ &= 7.\end{aligned}$$

3. (15pts) (i) *Exhibit a proper normal subgroup H of D_6. To which group is H isomorphic to?*

Let

$$H = \{ I, R, R^2, R^3, R^4, R^5 \}$$

be the subgroup of rotations. H is normal in D_6 as it has index 2. $H = \langle R \rangle \simeq \mathbb{Z}_6$.

(ii) *Give the left cosets of H inside D_6.*

$H = [I] = \{ I, R, R^2, R^3, R^4, R^5 \}$ and $H = [F_1] = \{ F_1, F_2, F_3, D_1, D_2.D_3 \}$, where F_1, F_2 and F_3 are all of the side flips and D_1, D_2 and D_3 are all of the diagonal flips.

(iii) *To which group is D_6/H isomorphic to?*

This has order two, so it is isomorphic to $\mathbb{Z}_2$.

4. (15pts) *True of false? If true then give a proof and if false then give a counterexample. Let G be a group.*
(i) *The centre $Z(G)$ of G is normal in G.*

True. If $z \in Z$ and $g \in G$ then

$$\begin{aligned} gzg^{-1} &= zgg^{-1} \\ &= ze \\ &= z \in Z. \end{aligned}$$

Thus Z is normal in G.

(ii) *The centraliser $C(a)$ of an element is normal in G.*

False. Let $G = S_3$ and let $a = (1, 2)$. Then

$$C(a) = \{e, (1, 2)\}.$$

If $g = (2, 3)$ then

$$gag^{-1} = (1, 3) \notin C(a).$$

Thus $C(a)$ is not normal in G.

(iii) *The kernel* $\operatorname{Ker}\phi$ *of a homomorphism $\phi\colon G \longrightarrow G'$ is normal in G.*

True. Let K be the kernel of ϕ and let $e' \in G'$ be the identity. If $k \in K$ and $g \in G$ then

$$\begin{aligned} \phi(gkg^{-1}) &= \phi(g)\phi(k)\phi(g^{-1}) \\ &= \phi(g)e'\phi(g)^{-1} \\ &= \phi(g)\phi(g)^{-1} \\ &= e' \end{aligned}$$

Thus $gkg^{-1} \in K$ and so K is normal in G.

5. (10pts) *Let G be a group and let H be a subgroup. Prove that the following are equivalent.*

(1) H is normal in G.
(2) For every $g \in G$, $gHg^{-1} = H$.
(3) For every $a \in G$, $aH = Ha$.
(4) The set of left cosets is equal to the set of right cosets.

Suppose that H is normal in G. Then for all $a \in G$,

$$aHa^{-1} \subset H.$$

Taking $a = g$ and $a = g^{-1}$ we get

$$gHg^{-1} \subset H \qquad \text{and} \qquad g^{-1}Hg \subset H.$$

Multiplying the second inclusion on the left by g and on the right by g^{-1} we get,

$$H \subset gHg^{-1}.$$

Hence (2) holds. Now suppose that (2) holds. Multiplying

$$aHa^{-1} = H,$$

on the right by a, we get

$$aH = Ha.$$

Hence (3) holds. Now suppose that (3) holds. Then (4) certainly holds. Finally suppose (4) holds. Pick $g \in G$. Then $g \in gH$ and $g \in Hg$. As the set of left cosets equals the set of right cosets, it follows that $gH = Hg$. Multiplying on the right by g^{-1} we get

$$gHg^{-1} = H.$$

As g is arbitrary, it follows that H is normal in G. Hence (1). Thus the four conditions are certainly equivalent.

6. (10pts) *True of false? If true then give a proof and if false then give a counterexample.*
Let G be a group and define the function

$$\phi\colon G \longrightarrow G \qquad \text{by} \qquad \phi(g) = g^{-1}.$$

(i) *ϕ is a homomorphism.*

False. Let $G = S_3$ and let $a = (1, 2)$, $b = (2, 3)$. Then

$$\begin{aligned}\phi(ab) &= (ab)^{-1} \\ &= b^{-1}a^{-1} \\ &= ba \\ &= (1, 2, 3) \\ &\neq (1, 3, 2) \\ &= ab \\ &= a^{-1}b^{-1} \\ &= \phi(a)\phi(b).\end{aligned}$$

(ii) *If G is abelian then ϕ is a homomorphism.*

True.

$$\begin{aligned}\phi(ab) &= (ab)^{-1} \\ &= b^{-1}a^{-1} \\ &= a^{-1}b^{-1} \\ &= \phi(a)\phi(b).\end{aligned}$$

7. (10pts) *Prove that the transpositions* $\tau_1, \tau_2, \dots, \tau_{n-1}$*, given by*

$$\tau_i = (i, i+1) \qquad \text{for} \qquad 1 \leq i \leq n-1,$$

generate S_n.

Let σ be a permutation. Then σ defines an ordering of the integers from one to n,

$$a_1, a_2, \dots, a_n \qquad \text{where} \qquad a_i = \sigma(i).$$

We first write down a product of $\tau_1, \tau_2, \dots, \tau_{n-1}$ that puts these integers into the usual order

$$1, 2, 3, \dots, n.$$

It is convenient to imagine that we have cards numbered from 1 to n and we are trying to put the cards into the usual order by switching adjacent cards.

Suppose that the first i cards have been put into the correct order. Consider the position of the $i+1$th card. If it is in the $i+1$th position then there is nothing to do. Otherwise it must be in a higher position j, $j > i+1$. It we switch the card in the jth position with the card in the $j-1$th position then now the $i+1$th card is in position $j-1$. Continuing in this way we can put the $i+1$th card into the $i+1$th position. By induction on i it then follows we can put all of the cards into the correct order.

Therefore we have found a product of $\tau_1, \tau_2, \dots, \tau_{n-1}$ that undoes the action of σ, that is, we have written σ^{-1} as a product of $\tau_1, \tau_2, \dots, \tau_{n-1}$. Since the inverse of a transposition is a transposition and the inverse of a product is the product of the inverses in the reverse order, it follows that σ is the product of the same transpositions but in the reverse order.

Thus $\tau_1, \tau_2, \dots, \tau_{n-1}$ generate S_n.

8. (10pts) *State and prove one of the Isomorphism Theorems.*

Bonus Challenge Problems

9. (10pts) *Prove the rest of the Isomorphism Theorems.*

10. (10pts) *Classify all groups of order* 22.

First suppose that G is abelian. Then

$$G \simeq \mathbb{Z}_{22}$$

is cyclic, by the classification of finitely generated abelian groups.
Now suppose that G is not abelian. Consider the possible order of an element of G. As this divides 22, it must be one of 1, 2, 11 and 22.
If there is an element of order 22 then G is cyclic. But this is not possible as we are assuming that G is not abelian. There is only one element of order 1, the identity. If every other element has order 2 then G is abelian.
So there must be an element a of order 11. Let $H = \langle a \rangle$. H has index 2 and so H is normal in G. Pick $b \in G$ not belonging to H. Then

$$\begin{aligned} b^2H &= (bH)^2 \\ &= h. \end{aligned}$$

Thus $b^2 \in H$. If $b^2 \neq e$ then b^2 has order 11 and so b has order 22, contrary to our assumptions.
Thus b has order 2. Consider

$$\mathrm{Aut}(\mathbb{Z}_{11}) \simeq U_{11}.$$

$2^2 = 4$, $4^2 = 16 = 5$ and $4^5 = 2 \cdot 5 \neq 1$. Thus $2 \in U_{11}$ has order 10 and U_{11} is cyclic of order 10. But then $10 = -1$ is the only element of order 2.
Conjugation by b defines an element of $\mathrm{Aut}(\mathbb{Z}_{11})$ of order 2. By what we proved this means

$$bab^{-1} = a^{-1}.$$

But then G is isomorphic to the Dihedral group D_{11} of order 22.

11. (10pts) *Let G be a simple group of order n, where $1 < n < 60$. Show that n is* prime.

12. (10pts) *If G is a finitely generated group whose automorphism group is trivial then prove that G has order at most 2.*

In fact this result is true without the hypothesis that G is finitely generated.
Suppose that a does not belong to the centre of G, so that $ab \neq ba$ for some $b \in G$. Let ϕ be the inner automorphism of G defined by a,

$$\phi\colon G \longrightarrow G \qquad \text{given by} \qquad \phi(g) = aga^{-1}.$$

Then

$$\begin{aligned} \phi(b) &= aba^{-1} \\ &\neq b. \end{aligned}$$

Thus ϕ is not the identity in $\mathrm{Aut}(G)$.
It follows that we may assume that G is abelian. In this case

$$\phi\colon G \longrightarrow G \qquad \text{given by} \qquad \phi(g) = g^{-1},$$

is an automorphism of G. If $g \neq g^{-1}$ then

$$\begin{aligned} \phi(g) &= g^{-1} \\ &\neq g. \end{aligned}$$

Thus we may assume that every element of G has order 2.
By the classification of finitely generated abelian groups, we know that G is isomorphic to a product of cyclic groups (this is the only place we use the hypothesis that G is finitely generated). If every element has order two then each term in the product must be $\mathbb{Z}_2$. So G is isomorphic to a product

$$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2.$$

Suppose that there is more than one term in the product. Let

$$\phi\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$$

be the function which switches the entries in the first two factors. Then ϕ is a non-trivial automorphism of G.
Thus we may assume that there is at most one factor. But then G has order at most two.

13. (10pts) *Let G be a simple group of order* 168. *Show that G is isomorphic to a subgroup of A_7.*

First note that if G is simple and $G \subset S_n$ then $G \subset A_n$, since otherwise $G \cap A_n$ is a subgroup of G of index 2 and any such is automatically normal in G.
Thus it is enough to show that G is isomorphic to a subgroup of S_7. Suppose that there is a non-trivial representation

$$\phi\colon G \longrightarrow S_k.$$

The kernel of ϕ must be trivial as it is a normal subgroup and so G is isomorphic to a subgroup of S_k. As the order of G divisible by 7, it follows that $k \geq 7$ and if $k = 7$ then we are done.
In particular it is enough to exhibit a subgroup of index $k \leq 7$ (for example, to show that there are $1 < k \leq 7$ Sylow p-subgroups).

$$168 = 2^3 \cdot 3 \cdot 7.$$

We count the number of Sylow p-subgroups for $p = 2$, 3 and 7.
Let x be the number of Sylow 7-subgroups. Then x is congruent to 1 modulo 7, so that

$$x = 1, 8, 15, 22, \dots.$$

$x \neq 1$ as G is simple. As x divides $2^3 \cdot 3$ the only possibility is that $x = 8$. It follows that G is isomorphic to a subgroup of S_8.
This almost gives us what we want. We need to count the other Sylow p-subgroups. Observe that 8 Sylow 7-subgroups gives us $8 \cdot 6 = 48$ elements of order 7. Note also that if the order of an element of G is divisible by 7 then it is seven. Indeed, consider the cycle type of the corresponding permutation in S_8. There must be a 7-cycle and there is not room for anything else.
Let y be the number of Sylow 3-subgroups. Then y is congruent to 1 modulo 3, so that

$$y = 1, 4, 7, 10, \dots.$$

$y \neq 1$ as G is simple. As y divides $2^3 \cdot 7$ the only possibility is that $y = 4$, $y = 7$, or $y = 28$. As above, we may assume that $y = 28$. Then there are $28 \cdot 2 = 56$ elements of order 3.
Let z be the number of Sylow 2-subgroups. Then z is congruent to 1 modulo 2, so that

$$z = 1, 3, 5, 7, \dots.$$

$z \neq 1$ as G is simple.

We may suppose that $z = 21$. Let P and Q be two Sylow 2-subgroups. Consider their intersection $H = P \cap Q$. Suppose that this is always trivial. Then there would be $21 \cdot 7 = 147$ elements of G whose order is a power of two. This gives us

$$168 < 48 + 56 + 147$$

distinct elements of G, clearly asburd.
Thus H sometimes has order at least two. Let N be the normaliser of H in G and let n be the order of N.
Suppose that H has order 4. Then H is normal in P, as the index of H in P is two, and so P is contained in N. It follows that 8 divides n and that $n > 8$ (as Q is also contained in N). But then $n \geq 24$ so that the index of N is at most 7. We are done in this case.
Suppose that $H = \{e, h\}$ has order 2. If $g \in N$ then $ghg^{-1} \in H$ and $ghg^{-1} \neq e$. But then $ghg^{-1} = h$ so that $gh = hg$. Thus $N = C(h)$.
Suppose that 7 divides n. Then we may find $g \in N$ of order 7. In this case gh is an element of order 14, which we already decided is not possible. Thus 7 does not divide n.
Let K be a subgroup of P of order 4 containing H. As the index of H in K is two it follows that H is normal in K. Therefore K is contained in N. It follows that 4 divides n and that $n > 4$. Thus n is divisible by 12.
Let w be the number of Sylow 3-subgroups of N. Then w is congruent to 1 modulo 3, so that

$$w = 1, 4, 7, 10, \dots.$$

Suppose that $w = 1$. Then there is a unique Sylow 3-subgroup R contained in N. Thus N is contained in the normaliser M of R in G and M has index e, a divisor of $2 \cdot 7$. But $e = y = 28$.
Thus $w \geq 4$ and N contains at least $8 = 4 \cdot 2$ elements of order 3. On the other hand N contains K and least one more element of Q. Thus $n \geq 24 > 12$ and the index of N is at most 7.