SECOND MIDTERM
MATH 100A, UCSD, AUTUMN 23

You have 80 minutes.

There are 6 problems, and the total number of points is 85. 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	15	
3	15	
4	10	
5	10	
6	20	
7	10	
8	10	
Total	85	

1. (15pts) *Give the definition of the commutator subgroup.*

The subgroup generated by all elements of the form $a^{-1}b^{-1}ab$, where a and $b \in G$.

(ii) *Give the definition of an automorphism.*

An isomorphism $\phi\colon G \longrightarrow G$.

(iii) *The kernel of a group homomorphism.*

The kernel of the group homomorphism $\phi\colon G \longrightarrow H$ is the inverse image of the identity.

2. (15pts)
(i) *Find the cycle decomposition of the following element of* S_9,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 6 & 2 & 1 & 3 & 9 & 5 & 8 \end{pmatrix}.$$

$$(1,7,9,8,5)(2,4)(3,6)$$

(ii) *Compute the conjugate of* σ *by* τ, *where* $\sigma = (1,5)(6,3,2)$ *and* $\tau = (1,5,6)(4,3,7,2)$.

$$(5,6)(1,7,4).$$

(iii) *Is it possible to conjugate* σ *to* σ', *where* $\sigma = (1,5)(2,3)(4,7,6)$ *and* $\sigma' = (1,4)(3,5,2)(6,7)$? *If so, find an element* τ *so that* σ' *is the conjugate of* σ *by* τ. *Otherwise explain why it is impossible.*

As σ and σ' have the same cycle type, this is possible. One possibility is

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 3 & 4 & 2 & 5 \end{pmatrix}$$

3. (15pts) *Let H be a subgroup of G and let*

$$N(H) = \{\, a \in G \,|\, aHa^{-1} \subset H \,\}.$$

Show that
(i) *$N(H)$ is a subgroup of G and $H \subset N(H)$.*

We have to check that $N(H)$ is non-empty and that it is closed under products and inverses. Suppose that $a \in H$ and let $h \in H$. Then $aha^{-1} \in H$ as H is a subgroup. Thus $a \in N(H)$ and so $H \subset N(H)$. In particular $N(H)$ is non-empty as H is non-empty.
Suppose that a and $b \in N(H)$. We check $ab \in N(H)$. If $h \in H$ then we have

$$(ab)h(ab)^{-1} = a(bhb^{-1})a^{-1}$$

Note that $bhb^{-1} \in H$ as $b \in N(H)$. It follows that $a(bhb^{-1})a^{-1} \in H$, as $a \in N(H)$. Thus $ab \in N(H)$ and H is closed under products.
Now suppose that $a \in N(H)$. We check $a^{-1} \in N(H)$. Unfortunately this fails. Here is an example where it fails. Let $G = A(\mathbb{Z})$ the permutations of the integers. Let H be the subgroup that fixes all of the negative integers

$$H = \{\, \sigma \in A(\mathbb{Z}) \,|\, \sigma(n) = n, \forall n < 0 \,\}.$$

Consider

$$\tau\colon \mathbb{Z} \longrightarrow \mathbb{Z} \qquad \text{given by} \qquad \tau(n) = n + 1.$$

Then $\tau \in G$ is a permutation of the integers. It shifts everything to the right by one. In particular if $\sigma \in H$ then $\tau\sigma\tau^{-1}$ fixes all integers $n < 1$. Thus

$$\tau\sigma\tau^{-1} \in N(H).$$

However τ^{-1} shifts by one to the left. So we only know that $\tau^{-1}\sigma\tau$ fixes all integers $n < -1$. For example if we define σ to be the tranposition that switches 0 and 1 and fixes everything else then $\sigma \in H$. But $\tau^{-1}\sigma\tau$ is the transposition that switches -1 and 0, so that $\tau^{-1}\sigma\tau \notin N(H)$.
For the record the correct definition of $N(H)$ is

$$N(H) = \{\, a \in G \,|\, aHa^{-1} = H \,\}.$$

In this case if $a \in N(H)$ then

$$aHa^{-1} = H \qquad \text{so that} \qquad H = a^{-1}Ha$$

so that $a^{-1} \in N(H)$ and $N(H)$ is closed under taking inverses.
It follows that $N(H)$ is a subgroup of G and $H \subset N(H)$.

(ii)

$$H \lhd N(H).$$

Suppose that $h \in H$ and $a \in N(H)$. Then $aha^{-1} \in H$. Thus

$$H \lhd N(H).$$

(iii) *If* K *is a subgroup of* G *such that*

$$H \lhd K$$

then

$$K \subset N(H).$$

Let $a \in K$. Let $h \in H$. As H is normal in K we have $aha^{-1} \in H$. Thus $a \in N(H)$. But then

$$K \subset N(H).$$

4. (10pts) *Let G be a group and let H be a normal subgroup. Show that G/N is abelian if and only if N contains $a^{-1}b^{-1}ab$ for every a and $b \in G$.*

Suppose that G contains the commutator $a^{-1}b^{-1}ab$ of every pair of elements a and b of G. Suppose that aH and bH are two left cosets Then

$$\begin{aligned}(bH)(aH) &= baH \\ &= ba(a^{-1}b^{-1}ab)H \\ &= abH \\ &= (aH)(bH).\end{aligned}$$

Thus G/H is abelian.
Now suppose that G/H is abelian. Suppose that a and $b \in H$. We have

$$\begin{aligned}abH &= (aH)(bH) \\ &= (bH)(aH) \\ &= baH.\end{aligned}$$

It follows that $ab = bah$, for some $h \in H$. But then

$$a^{-1}b^{-1}ab = h \in H.$$

Thus H contains the commutator of a and b.

5. (10pts) *Let G be a group and let Z be its centre. Prove that if G/Z is cyclic, then G is abelian.*

Suppose that G/Z is generated by aZ. Then the elements of G/Z are of the form a^iZ, for $i \in \mathbb{Z}$.
Suppose that x and $y \in G$. Then xZ and yZ are two left cosets, so that $xZ = a^iZ$ and $yZ = a^jZ$, for some i and j. It follows that we may find z_1 and $z_2 \in Z$ so that $x = a^iz_1$ and $y = a^jz_2$.
We have

$$\begin{aligned} xy &= (a^iz_1)(a^jz_2) \\ &= a^i(z_1a^j)z_2 \\ &= a^i(a^jz_1)z_2 \\ &= a^ia^j(z_1z_2) \\ &= a^{i+j}(z_1z_2). \end{aligned}$$

Similarly $yx = a^{j+i}z_2z_1 = a^{i+j}z_1z_2 = xy$. Thus G is abelian.

6. (20pts) (i) L*et* $a \in G$. *Prove that the map*

$$\sigma = \sigma_a \colon G \longrightarrow G \qquad \text{given as} \qquad \sigma(g) = aga^{-1},$$

is an automorphism of G.

Suppose that g and h are elements of G. We have

$$\begin{aligned}
\sigma(g)\sigma(h) &= (aga^{-1})(aha^{-1}) \\
&= ag(a^{-1}a)ha^{-1} \\
&= agha^{-1} \\
&= \sigma(gh).
\end{aligned}$$

Thus σ is a group homomorphism.

(ii) *Let* $\phi \colon G \longrightarrow A(G)$ *be the map which sends* a *to* $\phi(a) = \sigma_a$. *Show that* ϕ *is a group homomorphism.*

Let a and $b \in G$. Let $\sigma = \sigma_a$, $\tau = \sigma_b$ and $\rho = \sigma_{ab}$. We want to check that $\rho = \sigma\tau$. Both sides of this equation are functions from G to G, so we just need to check that they have the same effect on an element $g \in G$:

$$\begin{aligned}
(\sigma\tau)(g) &= \sigma(\tau(g)) \\
&= \sigma(bgb^{-1}) \\
&= a(bgb^{-1})a^{-1} \\
&= (ab)g(b^{-1}a^{-1}) \\
&= (ab)g(ab)^{-1} \\
&= \rho(g).
\end{aligned}$$

Thus ϕ is a group homomorphism.

(iii) *Show that the image $H = \phi(G)$ is isomorphic to G/Z, where Z is the centre of G.*

We check that Z is the kernel of ϕ. Suppose that $a \in Z$ and let $\sigma = \sigma_a = \phi(a)$. If $g \in G$ then

$$\sigma(g) = aga^{-1} = gaa^{-1} = g.$$

Thus σ is the identity map and so $a \in \operatorname{Ker}\phi$.
Now suppose that $a \in \operatorname{Ker}\phi$. Then σ is the identity map and so

$$g = \sigma(g) = aga^{-1}.$$

Multiplying on the right by a we get

$$ga = ag,$$

so that $a \in Z$. Thus $Z = \operatorname{Ker}\phi$ and the result follows by the first isomorphism theorem.

(iv) *Show that H is normal in* $\operatorname{Aut}(G)$.

Suppose that τ is an automorphism of G and let $\sigma = \sigma_a = \phi(a)$. Let $b = \tau(a)$ and let $\rho = \sigma_b = \phi(b)$. We check that

$$\tau\sigma\tau^{-1} = \rho.$$

Since both sides of this equation are functions from G to G we just need to check they have the same effect on elements g of G. As τ is a bijection we may find $h \in G$ such that $\tau(h) = g$. We have

$$\begin{aligned}
\tau\sigma\tau^{-1}(g) &= \tau\sigma\tau^{-1}(\tau(g)) \\
&= \tau(\sigma(h)) \\
&= \tau(aha^{-1}) \\
&= \tau(a)\tau(h)\tau(a^{-1}) \\
&= b\tau(h)b^{-1} \\
&= \rho(g).
\end{aligned}$$

As τ is arbitrary and $\rho \in H$ it follows that H is normal in $\operatorname{Aut}(G)$.

Bonus Challenge Problems
7. (10pts) *Prove the Second isomorphism theorem.*

Theorem 0.1 (Second Isomorphism Theorem)**.** *Let G be a group, let H be a subgroup and let N be a normal subgroup. Then*

$$H \vee N = HN = \{\, hn \,|\, h \in H, n \in N \,\}.$$

Furthermore $H \cap N$ is a normal subgroup of H and the two groups $H/H \cap N$ and HN/N are isomorphic.

Proof. The pairwise products of the elements of H and N are certainly elements of $H \vee N$. Thus the RHS of the equality above is a subset of the LHS. The RHS is clearly non-empty, it contains H and N and so it suffices to prove that the RHS is closed under products and inverses. Suppose that x and y are elements of the RHS. Then $x = h_1 n_1$ and $y = h_2 n_2$, where $h_i \in H$ and $n_i \in N$. Now $h_2^{-1} n_1 h_2 = n_3 \in N$, as N is normal in G. So $n_1 h_2 = h_2 n_3$. In this case

$$\begin{aligned} xy &= (h_1 n_1)(h_2 n_2) \\ &= h_1(n_1 h_2) n_2 \\ &= h_1(h_2 n_3) n_2 \\ &= (h_1 h_2)(n_3 n_2), \end{aligned}$$

which shows that xy has the correct form. On the other hand, suppose $x = hn$. Then $hnh^{-1} = m \in N$ as N is normal and so $hn^{-1}h^{-1} = m^{-1}$. In this case

$$\begin{aligned} x^{-1} &= n^{-1} h^{-1} \\ &= hm^{-1}, \end{aligned}$$

so that x^{-1} is of the correct form.
Hence the first statement. Let $H \longrightarrow HN$ be the natural inclusion. As N is normal in G, it is certainly normal in HN, so that we may compose the inclusion with the natural projection map to get a homomorphism

$$H \longrightarrow HN/N.$$

This map sends h to hN.
Suppose that $x \in HN/N$. Then $x = hnN = hN$, where $h \in H$. Thus the homorphism above is clearly surjective. Suppose that $h \in H$ belongs to the kernel. Then $hN = N$, the identity coset, so that $h \in N$. Thus $h \in H \cap N$. The result then follows by the First Isomorphism Theorem applied to the map above. □

8. (10pts) *Prove that if G is an abelian group that contains an element of order m and an element of order n then it contains an element of order l, where l is the least common multiple of m and n.*

We are given a and $b \in G$ of orders m and n. It is tempting to believe that ab is an element of order l.
However this not true. For example suppose that $b = a^{-1}$. Then a and b have the same order, so that $l = m = n$. However $ab = e$ is an element of order one, not l.
Let d be the greatest common divisor of m and n. Then $b' = b^d$ is an element of order $n' = n/d$. The lowest common multiple of m and n' is still l.
Replacing b by b^d and n by n/d we may therefore assume that m and n are coprime. Consider the order k of $c = ab$. On the one hand

$$\begin{aligned} c^l &= (ab)^l \\ &= a^l b^l \\ &= e. \end{aligned}$$

Thus k divides l.
On the other hand, we have

$$\begin{aligned} c^m &= (ab)^m \\ &= a^m b^m \\ &= b^m. \end{aligned}$$

As m is coprime to n the order of b^m is n. Thus $l \leq k$. It follows that $l = k$. Thus G contains an element of order l.
In fact, going back to the original setup, it follows that ab^d is an element of order l.