MA 361 - 04/03/2003 SECOND MIDTERM	Spring 2003 A. Corso	Name: Answer Key

PLEASE, BE NEAT AND SHOW ALL YOUR WORK; JUSTIFY YOUR ANSWER.

Problem Number	Possible Points	Points Earned
1	10	
2	10	
3	10	
4	10	
5	10	
6	10	
7	10	
8	10	
9	20	
TOTAL	100	

1. Describe all the elements in the cyclic subgroup H of the group of all 2×2 invertible matrices with real entries $\mathrm{GL}(2, \mathbb{R})$ generated by the matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = A$.
Which group is H isomorphic to?

Notice that $A^2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ and this gives us the idea that $A^n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$. (Here is the inductive step $A^{n+1} = A^n A = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ n+1 & 1 \end{bmatrix}$ for $n \geq 0$. But it works for $n \in \mathbb{Z}$, $n < 0$).

Thus $\left\langle \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^n \,\middle|\, n \in \mathbb{Z} \right\} = \left\{ \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} \,\middle|\, n \in \mathbb{Z} \right\}$

$\cong \mathbb{Z}$

pts: /10

2. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$. Justify your answer.

Read the explanation in the HW set for Section 6, problem #51 (see my handwritten online solutions)

pts: /10

$$(xax^{-1})^2 = (xax^{-1})(xax^{-1}) = xa^2x^{-1} =$$

$$= xex^{-1} = e$$

$\therefore$ xax^{-1} has order 2.

Because a is given to be the unique element of G of order 2, we see that

$$xax^{-1} = a \quad \text{for all } x \in G.$$

Thus $xa = ax$ for all $x \in G$. $\blacksquare$

#51. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.

Answer: The positive integers less than pq and relatively prime to pq are those that are not multiples of p and are not multiples of q. There are $p-1$ multiples of q and $q-1$ multiples of p that are less than pq. Thus there are

$$(pq-1) - (p-1) - (q-1) = (p-1)(q-1)$$

positive integers less than pq and relatively prime to pq.

I use the fact that if G is a cyclic group of order n generated by g. Then $\langle g^t \rangle = \langle g^{\gcd(t,n)} \rangle$

3. Find all subgroups of the group $\mathbb{Z}_{20}$, and draw the subgroup diagram for the subgroups.

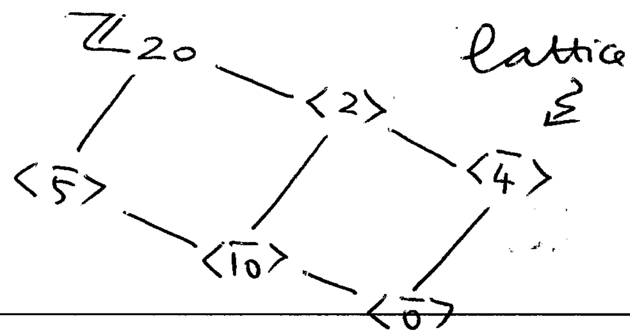
$\mathbb{Z}_{20} = \langle \bar{1} \rangle = \langle \bar{3} \rangle = \langle \bar{7} \rangle = \langle \bar{9} \rangle = \langle \overline{11} \rangle = \langle \overline{13} \rangle = \langle \overline{17} \rangle = \langle \overline{19} \rangle$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}\} = \langle \bar{6} \rangle = \langle \overline{14} \rangle = \langle \overline{18} \rangle$

$\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}, \overline{12}, \overline{16}\} = \langle \bar{8} \rangle = \langle \overline{12} \rangle = \langle \overline{16} \rangle$

$\langle \bar{5} \rangle = \{\bar{0}, \bar{5}, \overline{10}, \overline{15}\} = \langle \overline{15} \rangle$

$\langle \bar{0} \rangle = \{\bar{0}\}$ $\quad \langle \overline{10} \rangle = \{\bar{0}, \overline{10}\}$



pts: /10

4. List the elements of the subgroup generated by the subset $\{\bar{8}, \overline{10}\}$ of $\mathbb{Z}_{18}$.

We know that $\mathbb{Z}_{18}$ is a cyclic group generated say by $\bar{1}$. Any subgroup of a cyclic group is cyclic.

$\langle \bar{8}, \overline{10} \rangle =$ subgroup generated by the class of the gcd of 8 and 10

$= \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}\}$

pts: /10

5. (*a*) If G is an abelian group written multiplicatively, with identity e, prove that the set

$$H = \{g \in G \mid g^2 = e\}$$

is a subgroup of G.

(*b*) Is the above statement true if G is not abelian? Give an example.

(a)

H is non-empty as $e^2 = e$, so $e \in H$

For $a, b \in H$, i.e. $a^2 = e$ and $b^2 = e$, then $a^{-1}b \in H$ as $(a^{-1}b)^2 = a^{-1}ba^{-1}b = (a^{-1})^2 b^2 = (a^2)^{-1}(b^2) = e^{-1}e = e$. We used that G is abelian

(b) No : Consider S_3 and $H = \{id, (12), (13), (23)\}$

H can't be a subgroup as $|H| = 4$ But $4 \nmid |S_3| = 6$ (Lagrange theorem).

pts: /10

6. Let a non-empty finite subset H of a group G be closed under the binary operation of G. Show that H is a subgroup of G.

Read the explanation in the HW set for Section 5, problem # 50

(see my handwritten online solutions)

pts: /10

Identity e is in H : in fact $e^2 = e \cdot e = e$.

Inverse: if $a \in H$ then $a^2 = a \cdot a = e$.

Thus $a^{-1} = a$. So $a^{-1} \in H$.

This shows that H is a subgroup of G. ∎

#50. Let a non-empty finite subset H of a group G be closed under the binary operation of G. Show that H is a subgroup of G.

Ans: Let $a \in H$ and let H have n elements. Then the elements

$a, a^2, a^3, \ldots, a^{n+1}$ are all in H

(because H is closed under the operation), and cannot all be different.

$\therefore$ $a^i = a^j$ for some $i < j$.

Then multiplication by a^{-i} shows

$e = a^{j-i} \in H$

Also $a^{-1} = a^{j-i-1} \in H$. Thus H is a subgroup of G. $\blacksquare$

#51. Let G be a group and let a be one fixed element of G. Show that

$$H_a = \{ x \in G \mid xa = ax \}$$

is a subgroup of G.

<u>Ans</u>. Let $x, y \in H_a$, i.e. $xa = ax$ and $ya = ay$. We want to show that $xy \in H_a$. But

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y$$

$$\overset{!}{=} a(xy) \quad \therefore \quad xy \in H_a.$$

Obviously, $ea = a = ae$ so that $e \in H_a$.

Finally, from $xa = ax$ we get

$$xax^{-1} = a\underbrace{xx^{-1}}_{e} = a \quad \text{so} \quad xax^{-1} = a.$$

But then $\underbrace{x^{-1}x}_{e}ax^{-1} = x^{-1}a$ so that

$$ax^{-1} = x^{-1}a \quad \therefore \quad x^{-1} \in H_a.$$

$\therefore$ H_a is a subgroup of G.

7. (*i*) Let G be a group and let g be a fixed element of G. Show that the map $\lambda_g\colon G \longrightarrow G$, given by $\lambda_g(x) = xg$ for $x \in G$, is a permutation of the set G, that is $\lambda_g \in S_G$.
   (*ii*) Show that $H = \{\lambda_g \mid g \in G\}$ is a subgroup of S_G.

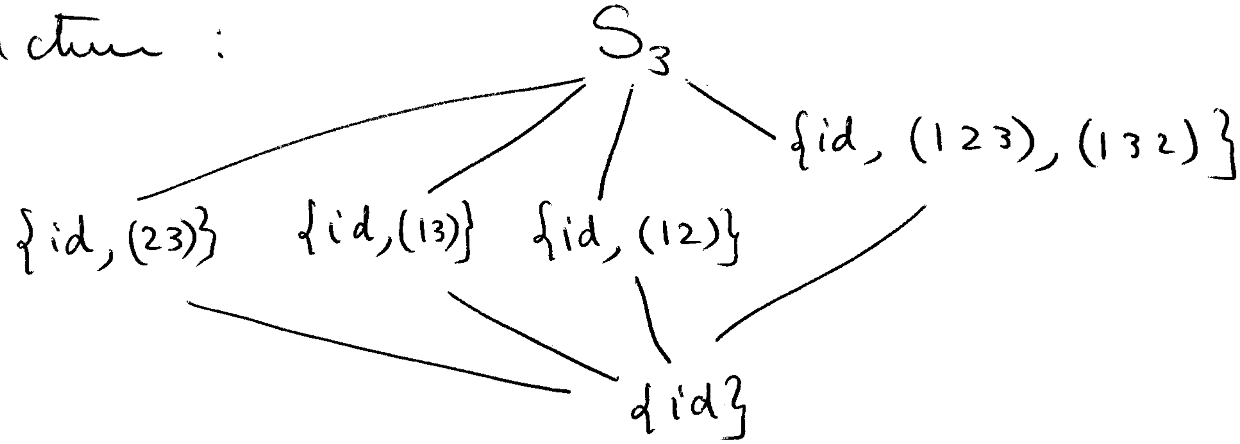
(i) This is embedded in the proof of Cayley's Theorem: λ_g <u>injective</u>: $\lambda_g(x) = \lambda_g(y)$ means $gx = gy \Rightarrow x = y$ by left cancellation.
λ_g is <u>surjective</u>: given $y \in G$, $y = \lambda_g(g^{-1}y)$.

(ii) Conceptual explanation: by Cayley's theorem $\varphi: G \longrightarrow S_G$, $\varphi(g) = \lambda_g$ is an homomorphism of groups and $H = \text{image of } \varphi$ ~~Use now HW~~ #41 page 58

pts: /10

8. (*i*) Show that for every subgroup H of S_n for $n \geq 2$, either all permutations in H are even or exactly half of them are even.
   (*ii*) Produce two subgroups of S_3 that illustrate each occurrence described in the above statement.

For (ii) we know that S_3 has the following structure:



$\boxed{\{id\}, \{id, (123), (132)\}}$ all elements are even permut.

pts: /10

$\boxed{\{id, (23)\}, \{id, (13)\}, \{id, (12)\}}$ half-and-half

even odd even odd even odd

$\boxed{\#7, (ii)}$ More concreate explanation

$H = \{\lambda_g \mid g \in G\}$ is a subgroup of S_G.

- H is non-empty as $\lambda_e = id$ $[\,: \lambda_e(x) = x\,]$ is an element of H.
- $\lambda_g, \lambda_{g'} \in S_G \Longrightarrow (\lambda_g \circ \lambda_{g'})(x) =$

$$= \lambda_g(g'x) = g(g'x) = (gg')(x) = \lambda_{gg'}(x)$$

i.e. $\lambda_g \circ \lambda_{g'} = \lambda_{gg'} \in H$ as $gg' \in G$.

- If $\lambda_g \in H$ then $(\lambda_g)^{-1} = \lambda_{g^{-1}} \in H$

So H is a subgroup by the subgroup criterion.

$\boxed{\#8, (i)}$ If H consists of all even permutations we are done. Otherwise H has an odd permutation, call it τ.

Let $\mathcal{A} = \{\text{all even permutations of } H\}$
$\mathcal{B} = \{\text{all odd permutations of } H\}$

Then $H = \mathcal{A} \cup \mathcal{B}$ (disjoint union) and

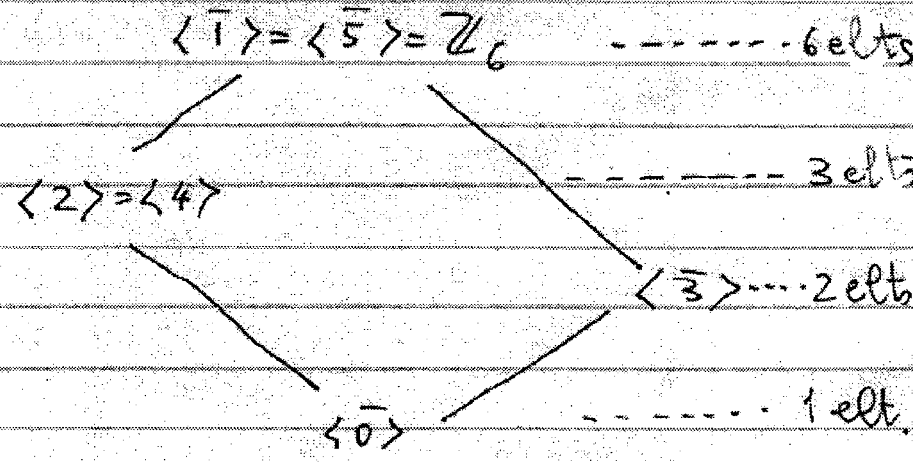
$$\psi : \mathcal{A} \longrightarrow \mathcal{B} \quad \text{is a bijection.}$$
$$\sigma \longmapsto \tau\sigma$$

even permut

~~odd~~ odd permutation

So $|\mathcal{A}| = |\mathcal{B}|$

(d) Moreover, the lattice subgroup of $\mathbb{Z}_6$ is



#41. Let $\varphi : G \longrightarrow G'$ be an isomorphism of a group $(G, *)$ with a group $(G', *')$. Show that if H is a subgroup of G then $\varphi(H) = \{ \varphi(h) \mid h \in H \}$ is a subgroup of G'.
<u>That is</u>, an isomorphism carries subgroups into subgroups.

<u>Ans</u>: Let $\varphi(a), \varphi(b) \in \varphi(H)$. Now $a * b \in H$ as H is a subgroup of G.
Thus $\varphi(a) *' \varphi(b) \underset{\text{as } \varphi \text{ is a homomorphism.}}{=} \varphi(a * b) \in \varphi(H)$

This shows that $\varphi(H)$ is closed under product.

Observe that $e' = \varphi(e) \in \varphi(H)$, where e is the identity of G and H.

Finally, let $a \in H$ so that $\varphi(a) \in \varphi(H)$. Since H is a subgroup of G we also have that $a^{-1} \in H$. Thus

$$e' = \varphi(e) = \varphi(a * a^{-1}) = \varphi(a) *' \varphi(a^{-1})$$

shows that $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H)$.

Thus $\varphi(H)$ is a subgroup of G'.

#42. Let $\varphi : G \longrightarrow G'$ be an isomorphism of a group $(G, *)$ with a group $(G', *')$. Show that if G is cyclic then G' is also cyclic.

<u>Ans.</u> Let a be a generator of G.
We <u>claim</u> that $\varphi(a)$ is a generator of G'.

Since $\varphi(a) \in G'$ we clearly have that $\langle \varphi(a) \rangle$ is contained in G'. Thus we need to show that

$$G' \subseteq \langle \varphi(a) \rangle$$

Pick $b' \in G'$. Since φ is onto there exists $b \in G$ such that

$$\varphi(b) = b'.$$

9. (i) Compute the indicated product of cycles that are permutations of S_8.

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

   (ii) Express the following permutations of S_8

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 1 & 3 & 6 & 8 & 4 & 7 \end{pmatrix} \qquad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 1 & 3 & 7 & 2 & 8 & 5 \end{pmatrix}$$

   as product of disjoint cycles and then as product of transpositions.

   (iii) Compute: $\sigma^{-1}\mu\sigma$, $|\langle\mu\rangle|$, $|\langle\sigma\rangle|$, σ^{-9}.

   (iv) Is $\langle\mu\rangle$ isomorphic to S_3?

(i)

$$(1\ 2)(7\ 8\ 4)(2\ 1)(8\ 1\ 5\ 7\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 3 & 7 & 8 & 6 & 2 & 1 \end{pmatrix}$$

$$= (1\ 5\ 8)(2\ 4\ 7)$$

$(8\ 6\ 4)(3\ 2\ 7\ 1)$ nothing to do as it is product of disjoint cycles.

(ii)

$$\sigma = (1\ 2\ 5\ 6\ 8\ 7\ 4\ 3) = (1\ 3)(1\ 4)(1\ 7)(1\ 8)(1\ 6)(1\ 5)(1\ 2)$$

$$\mu = (1\ 4\ 3)(2\ 6)(5\ 7\ 8)$$

$$= (1\ 3)(1\ 4)(2\ 6)(5\ 8)(5\ 7)$$

(iii) $\sigma^{-1}\mu\sigma = (3\ 7\ 4)(1\ 5)(2\ 8\ 6)$

$|\langle\mu\rangle| = 6 \qquad |\langle\sigma\rangle| = 8$

$$\sigma^{-9} = \sigma^{-1}\sigma^{-8} = \sigma^{-1}\underbrace{(\sigma^{8})^{-1}}_{\text{identity}} = \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$$

pts: /20

(iv) $\langle\mu\rangle$ has order 6 <u>but</u> it abelian as it is cyclic. Hence it can't be isomorphic to S_3