UNIVERSITY OF TORONTO
Faculty of Arts and Science
Solutions to **FINAL EXAMINATIONS, DECEMBER 2017**
**MAT301H1F: Groups and Symmetry**
Examiner: D. Burbulla

Duration - 3 hours

NAME: _____ STUDENT NUMBER: _____

**INSTRUCTIONS:** Present your solutions to the following questions in the space provided. You can use the backs of the pages if you need more space. No aids of any kind permitted. Do not tear any pages from this exam. The marks for each question are indicated in parentheses beside the question number. **TOTAL MARKS:** 100

**Notation:**

- $\mathbb{Q}^*$ is the multiplicative group of non-zero rational numbers.
- $\mathbb{R}^*$ is the multiplicative group of non-zero real numbers.
- If $n \geq 2$, $\mathbb{Z}_n$ is the additive group of integers modulo $n$.
- If $n \geq 2$, $U(n)$ is the multiplicative group of units modulo $n$ consisting of all positive integers less than $n$ and relatively prime to $n$.
- $C_n$ is the cyclic group of order $n$.
- $S_n$ is the symmetric group of degree $n$.
- $A_n$ is the alternating group of degree $n$.
- $GL(n, \mathbb{R})$ is the group of $n \times n$ invertible matrices with real entries.
- If $n \geq 3$, $D_n$ is the dihedral group of order $2n$.
- If $G_1, G_2, \ldots, G_k$ are groups, $G_1 \oplus G_2 \oplus \cdots \oplus G_k$ is the external direct product of $G_1, G_2, \ldots, G_k$.
- If $G$ is a group, $\mathrm{Inn}\,(G)$ is the group of inner automorphisms of $G$.
- If $G$ is a group, $\mathrm{Aut}\,(G)$ is the group of automorphisms of $G$.

1. [10 marks] Define the following:

   (a) [2 marks] $H$ is a **normal subgroup** of the group $G$, given that $H \leq G$.

   **Definition:** $H$ is a normal subgroup of $G$ if for all $g \in G$, $gH = Hg$.

   (b) [2 marks] the **kernel** of $f$, if $f : G \longrightarrow H$ is a group homomorphism.

   **Definition:** if $e_H$ is the identity element of $H$, $\ker(f) = \{x \in G \mid f(x) = e_H\}$.

   (c) [2 marks] two elements $a$ and $b$ are **conjugate** in the group $G$.

   **Definition:** two element $a, b \in G$ are conjugate if there is an element $x \in G$ such that

   $$b = xax^{-1}.$$

   (d) [2 marks] an **automorphism** $f$ of a group $G$.

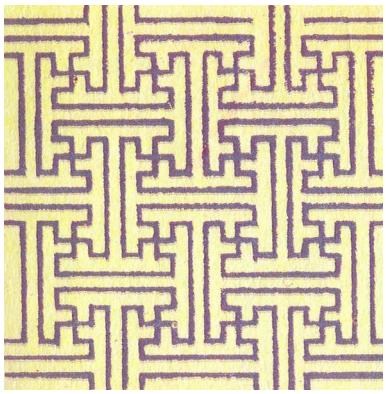
   **Definition:** $f : G \longrightarrow G$ is an automorphism of $G$ if it is a homomorphism that is also one-to-one and onto.

   (e) [2 marks] a **cyclic** group $G$.

   **Definition:** $G$ is a cyclic group if there is an element $a \in G$ such that $G = \langle a \rangle$.

2. [20 marks] No justifications for your answers to the following questions are required:

(a) [5 marks] Consider the wall paper pattern exhibited to the right. Which of the following symmetries does the pattern have?



| | |
|---|---|
| (*i*) a rotation of order 2 | Yes |
| (*ii*) a rotation of order 3 | No |
| (*iii*) a rotation of order 4 | Yes |
| (*iv*) a rotation of order 5 | No |
| (*v*) a rotation of order 6 | No |
| (*vi*) a horizontal reflection | Yes |
| (*vii*) a vertical reflection | Yes |
| (*viii*) a diagonal reflection | No |
| (*ix*) a glide reflection | Yes |

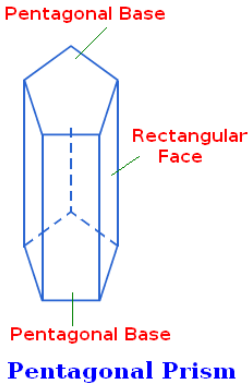
(b) [8 marks] List all possible non-isomorphic Abelian groups of order $900 = 4 \times 9 \times 25$.

**Solution:** the part of order 4 is $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_4$; the part of order 9 is $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_9$; the part of order 25 is $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ or $\mathbb{Z}_{25}$. So the eight possible non-isomorphic Abelian groups of order 900 are:

$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$, and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}$.

(c) [1 mark] How many symmetries of a regular 5-prism are there? See the figure to the right.

**Solution:** $2\,|D_5| = 20$



**Pentagonal Prism**

(d) [6 marks] How many elements of each order are there in $\mathbb{Z}_{12}$?

**Solution:** the divisors of 12 are $d = 1, 2, 3, 4, 6$ or 12 and the number of elements of order $d$ in $\mathbb{Z}_{12}$ is $\phi(d)$. So there are

- 1 element of order 1,
- 1 element of order 2,
- 2 elements of order 3,
- 2 elements of order 4,
- 2 elements of order 6,
- 4 elements of order 12.

3. [12 marks] How many elements of each possible order are there in the following groups?

(a) [6 marks] $\mathbb{Z}_4 \oplus U(8)$.

**Solution:** to begin wth, $U(8) = \{1, 3, 5, 7\}$ and elements 3, 5, 7 all have order 2. Then $|\mathbb{Z}_4 \oplus U(8)| = 4 \times 4 = 16$, and the only possible orders of $(m, n) \in \mathbb{Z}_4 \oplus U(8)$ are

$$\text{lcm}(|a|, |b|) = \begin{cases} 1 & \text{if } a = 0, b = 1 \\ 2 & \text{if } a = 0 \text{ and } b = 3, 5 \text{ or } 7 \\ 2 & \text{if } a = 2 \text{ and } b \in U(8) \\ 4 & \text{if } a = 1 \text{ or } 3 \text{ and } b \in U(8) \end{cases}$$

Thus in $\mathbb{Z}_4 \oplus U(8)$ there are

- 1 element of order 1,
- 7 elements of order 2,
- 8 elements of order 4.

(b) [6 marks] $\mathbb{Z}_8 \oplus \mathbb{Z}_3/\langle(4, 2)\rangle$.

**Solution:** observe that $|(4, 2)| = \text{lcm}(|4|, |2|) = \text{lcm}(2, 3) = 6$, or that

$$\langle(4, 2)\rangle = \{(4, 2), (0, 1), (4, 0), (0, 2), (4, 1), (0, 0)\},$$

Either way, $|\langle(4, 2)\rangle| = 6$ and $|\mathbb{Z}_8 \oplus \mathbb{Z}_3/\langle(4, 2)\rangle| = 24/6 = 4$. Then $\mathbb{Z}_8 \oplus \mathbb{Z}_3/\langle(4, 2)\rangle$ consists of the four cosets

$$\langle(4, 2)\rangle, (1, 0) + \langle(4, 2)\rangle, (2, 0) + \langle(4, 2)\rangle, 1, 0) + \langle(4, 2)\rangle \text{ and } (3, 0) + \langle(4, 2)\rangle,$$

the orders of which in $\mathbb{Z}_8 \oplus \mathbb{Z}_3/\langle(4, 2)\rangle$ are, respectively, 1, 4, 2 and 4. That is,

$$\mathbb{Z}_8 \oplus \mathbb{Z}_3/\langle(4, 2)\rangle \approx \mathbb{Z}_4,$$

so it has 1 element of order 1, 2 elements of order 4, and 1 element of order 2.

4. [18 marks] Let $Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$; let $GL(2,\mathbb{R})$ be the group of $2 \times 2$ invertible matrices with real entries.

   (a) [5 marks] Find $C(Y)$, the centralizer of $Y$ in $GL(2,\mathbb{R})$.

   **Solution:** let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R})$ such that $AY = YA$. Then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Leftrightarrow \begin{bmatrix} b & -a \\ d & -c \end{bmatrix} = \begin{bmatrix} -c & -d \\ a & b \end{bmatrix},$$

   so we must have $d = a$ and $b = -c$. Thus

$$C(Y) = \left\{ \begin{bmatrix} a & -c \\ c & a \end{bmatrix} \mid a^2 + c^2 \neq 0 \right\}.$$

   Note: some observations that could be useful:

   1. $C(Y)$ is Abelian,
   2. and for $A \in C(Y)$, $A\,A^T = A^T\,A = \det(A)$.

   (b) [4 marks] Let $H = \{A \in C(Y) \mid \det(A) = 1\}$. Prove: $H$ is a subgroup of $C(Y)$. To which subgroup of $GL(2,\mathbb{R})$ is $H$ isomorphic?

   **Solution:** you can use the subgroup test, but it is easier to observe that

$$H = C(Y) \cap \ker(\det),$$

   and the intersection of two subgroups is itself a subgroup. Finally, if $A \in C(Y)$ and $a^2 + c^2 = 1$, then

$$A = \begin{bmatrix} a & -c \\ c & a \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = R_\theta,$$

   for some $\theta$. So $H \approx SO(2,\mathbb{R})$; that is, $H$ is isomorphic to the group of $2 \times 2$ rotation matrices.

   **Using the Subgroup Test:** to show $H$ is a subgroup of $C(Y)$, suppose $A, B$ are in $C(Y)$ with $\det(A) = \det(B) = 1$. Then

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = 1 \times 1^{-1} = 1$$

   and $AB^{-1} \in C(Y)$, because $C(Y)$ is a subgroup of $GL(2,\mathbb{R}^2)$. So $AB^{-1} \in C(Y)$.

(c) [4 marks] Find a homomorphism $f : C(Y) \longrightarrow C(Y)$ such that $\ker(f) = H$, and show that your answer is correct.

**Solution:** define $f : C(Y) \longrightarrow C(Y)$ by $f(A) = \det(A)\, I$. Then:

- $f(A)$ *is* in $C(Y)$, since $kI$ commutes with *every* matrix in $GL(2, \mathbb{R})$.
- $f$ is a homomorphism:

$$f(AB) = \det(AB)\, I = \det(A)\det(B)\, I = \det(A)\, I\, \det(B)\, I = f(A)f(B),$$

- $\ker(f) = H$: let $A \in \ker(f)$. Then $A \in C(Y)$ and

$$f(A) = I \Rightarrow \det(A)\, I = I \Rightarrow \det(A) = 1 \Rightarrow A \in H.$$

(d) [5 marks] Find to which group the factor group $C(Y)/H$ is isomorphic. Express your answer as s subgroup of $\mathbb{R}^*$.

**Solution:** by the First Isomorphism Theorem,

$$C(Y)/H = C(Y)/\ker(f) \approx \mathrm{im}\,(f) = \{(a^2 + c^2)\, I \mid a^2 + c^2 \neq 0\} = \{xI \mid x > 0\}.$$

We claim

$$\{xI \mid k > 0\} \approx \{x \in \mathbb{R}^* \mid x > 0\}.$$

(Aside: the set of positive real numbers *is* a subgroup of $\mathbb{R}^*$ since 1 is positive, the product of positive numbers is positive, and the inverse (reciprocal) of a positive number is also positive.) The isomorphism is the 'obvious' one: $\phi(xI) = x$ :

- $\phi$ is a homomorphism: $\phi(xI\, yI) = \phi(xyI) = x\, y = \phi(xI)\phi(yI)$
- $\phi$ is one-to-one: $\phi(xI) = 1 \Rightarrow x = 1 \Rightarrow xI = I$
- $\phi$ is onto: for $x > 0$, $\phi(xI) = x$.

5.(a) [5 marks] Let $G$ be a group. Assume that $\mathrm{Inn}\,(G) \leq \mathrm{Aut}\,(G)$. Prove that

$$\mathrm{Inn}\,(G) \lhd \mathrm{Aut}\,(G).$$

**Solution:** let $\phi_g \in \mathrm{Inn}\,(G)$ and let $h \in \mathrm{Aut}\,(G))$. Then, for $x \in G$,

$$\begin{aligned}(h \circ \phi_g \circ h^{-1})(x) &= h(\phi_g(h^{-1}(x))) \\ &= h(g\,h^{-1}(x)\,g^{-1}) \\ &= h(g)\,h(h^{-1}(x))\,h(g^{-1}) \\ &= h(g)\,x\,(h(g))^{-1} \\ &= \phi_{h(g)}(x)\end{aligned}$$

Thus $h \circ \phi_g \circ h^{-1} = \phi_{h(g)} \in \mathrm{Inn}\,(G)$ and $\mathrm{Inn}\,(G) \lhd \mathrm{Aut}\,(G)$.

5.(b) [5 marks] Prove that the mapping $f : GL(n,\mathbb{R}) \longrightarrow GL(n,\mathbb{R})$ defined by

$$f(A) = (A^{-1})^T$$

is an automorphism.

**Solution:** we use the facts that for $A, B \in GL(n,\mathbb{R})$,

$$(AB)^{-1} = B^{-1}A^{-1},\ (AB)^T = B^T A^T \text{ and } (A^{-1})^T = (A^T)^{-1}.$$

Then

1. $f$ is a homomorphism:

$$f(AB) = ((AB)^{-1})^T = (B^{-1}A^{-1})^T = (A^{-1})^T\,(B^{-1})^T = f(A)\,f(B)$$

2. $f$ is one-to-one. Show that $\ker(f) = \{I\}$:

$$f(A) = I \Rightarrow (A^{-1})^T = I \Rightarrow A^{-1} = I^T = I \Rightarrow A = I^{-1} = I.$$

3. $f$ is onto. If $A \in GL(n,\mathbb{R})$, then

$$f\left((A^{-1})^T\right) = \left(\left((A^{-1})^T\right)^{-1}\right)^T = \left(\left((A^{-1})^{-1}\right)^T\right)^T = (A^T)^T = A$$

That is, $f$ has order 2. This can also be used to prove that $f$ is one-to-one:

$$f(A) = I \Rightarrow f(f(A)) = f(I) \Rightarrow A = I.$$

6. [15 marks] For the group $S_5$ find the following:

   (a) [8 marks] the number of elements in $S_5$ of each possible order, and indicate whether the elements are even or odd.

   **Solution:** for parts (a) and (b) we use the fact that in $S_n$ elements of the same cycle structure have the same order **and** that elements are conjugate if and only if they have the same cycle structure. For $S_5$:

| Cycle structure | Number of conjugates | Order | Parity |
|---|---|---|---|
| $(1)$ | $1$ | $1$ | even |
| $(ab)$ | $(5 \times 4)/2 = 10$ | $2$ | odd |
| $(abc)$ | $(5 \times 4 \times 3)/3 = 20$ | $3$ | even |
| $(abcd)$ | $(5 \times 4 \times 3 \times 2)/4 = 30$ | $4$ | odd |
| $(abcde)$ | $(5 \times 4 \times 3 \times 2 \times 1)/5 = 24$ | $5$ | even |
| $(ab)(cd)$ | $\frac{1}{2}\left(\frac{5\times4}{2} \times \frac{3\times2}{2}\right) = 15$ | $2$ | even |
| $(abc)(de)$ | $\frac{5\times4\times3}{3} \times \frac{2\times1}{2} = 20$ | $6$ | odd |

   So $S_5$ has

   - 1 even element of order 1,
   - 10 odd elements of order 2,
   - 20 even elements of order 3,
   - 30 odd elements of order 4,
   - 24 even elements of order 5,
   - 15 even elements of order 2,
   - 20 odd elements of order 6.

(b) [5 marks] the number of elements in each conjugacy class of $S_5$ and the class equation of $S_5$.

**Solution:** reading off the number of elements in each conjugacy class from the chart in part (a), and observing that $Z(S_4) = \{(1)\}$, we have

$$|S_5| = 1+|\mathrm{cl}\left((12)\right)|+|\mathrm{cl}\left((123)\right)|+|\mathrm{cl}\left((1234)\right)|+|\mathrm{cl}\left((12345)\right)+|\mathrm{cl}\left((12)(34)\right)|+|\mathrm{cl}\left((123)(45)\right|$$

$$\Leftrightarrow 120 = 1 + 10 + 20 + 30 + 24 + 15 + 20.$$

(c) [2 marks] an element $\alpha \in S_5$ such that $\alpha\left((123)(45)\right)\alpha^{-1} = (451)(32)$.

**Solution:** $\alpha$ can be determined by the correspondence between the two elements:

$$(123)(45)$$

and

$$(451)(32).$$

That is, take $\alpha = (143)(25)$. Then $\alpha^{-1} = (134)(25)$ and for

$$\alpha\left((123)(45)\right)\alpha^{-1} = (143)(25)\left((123)(45)\right)(134)(25)$$

we have

- $1 \to 3 \to 1 \to 4$,
- $2 \to 5 \to 4 \to 3$,
- $3 \to 4 \to 5 \to 2$
- $4 \to 1 \to 2 \to 5$,
- $5 \to 2 \to 3 \to 1$,

as required.

Other correct choices of $\alpha$ that were found on the exam:

1. $\alpha = (35)(24)$
2. $\alpha = (152)(34)$
3. $\alpha = (2435)$
4. $\alpha = (54321)$

7. [15 marks] Recall that the dihedral group of order 10 can be described as

$$D_5 = \langle a, b \mid a^5 = b^2 = e, bab = a^{-1} \rangle.$$

Determine how many homomorphisms there are

(a) [4 marks] from $D_5$ to $\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$

**Solution:** let $f : D_5 \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$ be a homomorphism. Then $|\mathrm{im}\,(f)|$ divides both 10 and 4, so there are only two possibilities:

1. $|\mathrm{im}\,(f)| = 2$ : then $|\ker(f)| = 5$, so $\ker(f) = \langle a \rangle$ and $f(a) = (0,0)$. As for $f(b)$, its order must be 2, otherwise $\mathrm{im}\,(f) = \{(0,0)\}$, so there are three possibilities for $f(b)$, namely

$$f(b) = (0,1), (1,0) \text{ or } (1,1).$$

   Hence in this case there are three homomorphisms.
2. $|\mathrm{im}\,(f)| = 1$ : there is only one homomorphism in this case, the zero homomorphism defined by $f(x) = (0,0)$.

Thus there are **four** homomorphisms from $D_5$ to $\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

(b) [4 marks] from $D_5$ to $\mathbb{Q}^*$

**Solution:** suppose $f : D_5 \longrightarrow Q^*$ is a homomorphism. Since $|f(x)|$ must divide $|x|$, and there are only two elements in $Q^*$ with finite order, namely 1 (with order 1) and $-1$ (with order 2), we must have

$$f(a) = \pm 1 \text{ and } f(b) = \pm 1.$$

But $|a| = 5$, so in fact $f(a) = 1$. That leaves only two possibilities left,

$$f(b) = 1 \text{ or } f(b) = -1.$$

Thus there are **two** homomorphisms from $D_5$ to $\mathbb{Q}^*$.

**Aside:** as it says on the front page, $\mathbb{Q}^*$ is the multiplicative group of non-zero rational numbers, *not* the quaternions.

(c) [3 marks] from $\mathbb{Z}$ to $D_5$.

**Solution:** suppose $f : \mathbb{Z} \longrightarrow D_5$ is a homomorphism. Since $\mathbb{Z} = \langle 1 \rangle$, $f$ is completely determined by $f(1)$. Let $f(1) = x$, for any $x \in D_5$. Then $f(0) = e = x^0$, by convention. For $n > 0$,

$$f(n) = f(n \cdot 1) = (f(1))^n = x^n$$

and

$$f(-n) = f(n(-1)) = (f(-1))^n = (x^{-1})^n = x^{-n}.$$

Thus for $m, n \in \mathbb{Z}$,

$$f(m+n) = x^{m+n} = x^m x^n = f(m)f(n);$$

that is, $f$ is a homomorphism for each $x \in D_5$. Thus there are **ten** homomorphisms from $\mathbb{Z}$ to $D_5$.

**Aside:** the homomorphism $f : \mathbb{Z} \longrightarrow D_5$ defined by $f(1) = x$, for $x \in D_5$ is interesting for two reasons:

1. $\text{im}\,(f) = \langle x \rangle$
2. $\ker(f) = \langle n \rangle$, where the order of $x \in D_5$ is $n$.

(d) [4 marks] from $D_5$ to $\mathbb{Z}_{10}$.

**Solution:** suppose $f : D_5 \longrightarrow \mathbb{Z}_{10}$ is a homomorphism. Since $|D_5| = |\mathbb{Z}_{10}|$ there are at most four possibilities:

1. $|\text{im}\,(f)| = 10$ and $|\ker(f)| = 1$ : in this case, $f$ would be an isomorphism. But $D_5$ and $\mathbb{Z}_{10}$ are *not* isomorphic: one is Abelian, the other isn't. So there are no homomorphisms in this case.
2. $|\text{im}\,(f)| = 5$ and $|\ker(f)| = 2$ : in this case, $\ker(f) = \{e, r\}$, for some reflection $r \in D_5$. Since $\ker(f) \lhd D_5$, the reflection $r$ commutes with all $x \in D_5$. That implies that $r \in Z(D_5)$; but this is impossible because $Z(D_n) = \{e\}$ if $n$ is odd. So there are also no homomorphisms in this case.
3. $|\text{im}\,(f)| = 2$ and $|\ker(f)| = 5$ : in this case, $\ker(f) = \langle a \rangle$, so $f(a) = 0$. What about $f(b)$? $f(b)$ must have order 2, and there is only one element of order 2 in $\mathbb{Z}_{10}$ : $f(b) = 5$. So there is one homomorphism in this case.
4. $|\text{im}\,(f)| = 1$ and $|\ker(f)| = 10$ : in this case there is one homomorphism, namely $f(x) = 0$ for all $x \in D_5$.

Thus there are **two** homomorphisms from $D_5$ to $\mathbb{Z}_{10}$.