University of Toronto

MAT301H1S - Groups and Symmetry

Solutions to Term Test, March 4, 2020

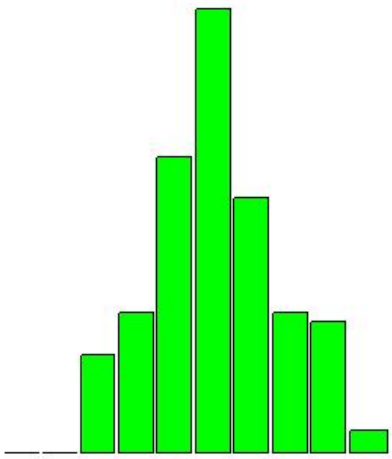
Duration: 120 minutes. Aids permitted: None.

Observations:

- Questions 1, 2, 3, 4, 9 and 10 all had passing averages. The average on these six questions was 72%.
- Questions 5, 7 and 8, which all involved proofs, had a failing average of 39%—not unexpected.
- Question 6, which was actually a computational question, was horribly done; the average was 10%.
-

Breakdown of Results: 186 students wrote this test. The marks ranged from 20% to 100%, and the average was 55.6%. There was one perfect paper. Some statistics on grade distribution are in the table on the left, and a histogram of the marks (by decade) is on the right.

Grade	%	Decade	%
		90-100%	1.6%
A	10.2%	80-89%	8.6%
B	9.1%	70-79%	9.1%
C	16.7%	60-69%	16.7%
D	29.0%	50-59%	29.0%
F	35.0%	40-49%	19.4%
		30-39%	9.1%
		20-29%	6.5%
		10-19%	0.0%
		0-9%	0.0%



1. [2 marks for each part; avg: 7.2/10] Let G be a group with operation 'multiplication' and identity element e. Define the following:

   (a) the center of G

   Solution: the center of G is $\{g \in G \mid gx = xg, \text{ for all } x \in G\}$

   (b) the order of $a \in G$

   Solution: the order of a is the least positive integer n such that $a^n = e$.

   (c) an inner automorphism of G

   Solution: for $g \in G$, the function $f_g : G \longrightarrow G$ defined by

   $$f_g(x) = gxg^{-1}$$

   is an inner automorphism of G.

   (d) the centralizer of $a \in G$

   Solution: the centralizer of a is $\{x \in G \mid xa = ax\}$

   (e) the index in G of the subgroup H.

   Solution: the index in G of H is the number of distinct (left) cosets of H.

2. [2 marks for each part; avg: 7.7/10] Find the order of the following elements in the following groups. You should put your answer in the blank to the right, but you must show your work to get full marks.

(a) 11 in $\mathbb{Z}_{99}$ **Order:** 9

Solution:

$$|11| = |11 \cdot 1| = \frac{99}{\gcd(99, 11)} = \frac{99}{11} = 9.$$

(b) 5 in $U(18)$ **Order:** 6

Solution: $|U(18)| = \phi(18) = \phi(2)\phi(9) = 1 \cdot 6 = 6$, so $|5| = 2, 3$ or 6.

$$5^2 = 25 \equiv 7 \pmod{18};\ 5^3 \equiv 35 \equiv -1 \pmod{18}.$$

So $|5|$ must be 6.

(c) $\begin{bmatrix} \cos(\pi/5) & -\sin(\pi/5) \\ \sin(\pi/5) & \cos(\pi/5) \end{bmatrix}$ in $O(2, \mathbb{R})$ **Order:** 10

Solution: a rotation of $\pi/5$ has order $2\pi/(\pi/5) = 10$.

Or in terms of degrees: a rotation of 36° has order $360^\circ/36^\circ = 10$.

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 3 & 2 & 1 \end{pmatrix}$ in S_7 **Order:** 12

Solution: write the permutation as a product of disjoint cycles.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 3 & 2 & 1 \end{pmatrix} = (147)\,(2536).$$

So the order is $\operatorname{lcm}(3, 4) = 12$.

(e) $(3, 5)$ in $\mathbb{Z}_6 \oplus \mathbb{Z}_9$ **Order:** 18

Solution: $|(3, 5)| = \operatorname{lcm}(|3|, |5|) = \operatorname{lcm}(2, 9) = 18$.

Continued...

3. [2 marks for each part; avg: 6.6/10.] Determine whether the following pairs of groups are isomorphic or not. You should circle Yes or No to the right, but you must also give a brief reason for your choice.

(a) D_4 and A_4. **Yes** **No**

Solution: $|D_4| = 8 \neq 12 = |A_4|$

(b) $U(9)$ and $\mathrm{Aut}\,(\mathbb{Z}_9)$. **Yes** **No**

Solution: specific case of the Theorem

$$\mathrm{Aut}\,(\mathbb{Z}_n) \approx U(n).$$

(c) $U(16)$ and $\mathcal{Q}$. **Yes** **No**

Solution: $\mathcal{Q}$ only has one element of order 2, namely -1, but $U(16)$ has at least two:

$$7^2 = 49 \equiv 1 \pmod{16} \text{ and } 9^2 = 81 \equiv 1 \pmod{16}.$$

(d) $\mathbb{Z}_{12}$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ **Yes** **No**

Solution: because 3 and 4 are relatively prime, $\mathbb{Z}_{12} \approx \mathbb{Z}_3 \oplus \mathbb{Z}_4$.

(e) S_4 and D_{12}. **Yes** **No**

Solution: D_{12} has (four) elements of order 12 but S_4 has no elements of order 12, since a permutation of $\{1, 2, 3, 4\}$ can only have order 1, 2, 3 or 4. (That is, S_4 consists of the identity, 2-cycles, pairs of disjoint 2-cycles, 3-cycles or 4-cycles.)

Continued...

4. [avg: 8.7/10] Let $\sigma = (123)(246)(125)(1345)$ be an element of S_6.

(a) [3 marks] Express σ as a product of disjoint cycles.

Solution:

$$\sigma = (123)(246)(125)(1345) = (1)\,(254)\,(36) = (254)\,(36)$$

(b) [2 marks] Find $|\sigma|$.

Solution: $|\sigma| = \text{lcm}(3, 2) = 6$.

(c) [3 marks] Express σ as a product of 2-cycles. Is σ even or odd?

Solution: $\sigma = (254)\,(36) = (24)\,(25)\,(36)$; so σ is odd.

(d) [2 marks] Express σ^{-1} as a product of disjoint cycles.

Solution: using answer from part (a).

$$\sigma^{-1} = ((254)\,(36))^{-1} = (36)^{-1}\,(254)^{-1} = (36)\,(245).$$

Continued...

5. [avg: 4.3/10] Prove the following:

(a) [3 marks] If G is a group such that the map $\phi : G \longrightarrow G$ defined by $\phi(g) = g^{-1}$ is a homomorphism, then G is Abelian.

Proof: let $g, h \in G$. Then

$$\phi(gh) = \phi(g)\phi(h) \Rightarrow (gh)^{-1} = g^{-1}\, h^{-1} \Rightarrow (gh)^{-1} = (hg)^{-1} \Rightarrow gh = hg,$$

so G is Abelian.

(b) [4 marks] Let G and H be finite groups and suppose $\phi : G \longrightarrow H$ is a homomorphism which is onto.[1] If H has an element of order n then G also has an element of order n.

Proof: let $h \in H$ with $|h| = n$. Since ϕ is onto, there is $g \in G$ such that $\phi(g) = h$. By a property of homomorphisms proved in class (or in the book), we know

$$|\phi(g)| \text{ divides } |g|.$$

Since $|\phi(g)| = n$, we have $|g| = k\, n$, for some integer $k \geq 1$. Then $g^k \in G$ and

$$\left|g^k\right| = \frac{kn}{\gcd(kn, k)} = \frac{kn}{k} = n.$$

(c) [3 marks] If G is a group such that $|G| = p$, for some prime number p, then G is cyclic.

Proof: pick $g \in G$ such that $g \neq e$, and consider the subgroup $\langle g \rangle$. By Lagrange's Theorem,

$$|\langle g \rangle| \text{ divides } p.$$

Since p is prime, and $|\langle g \rangle| \neq 1$,

$$|\langle g \rangle| = p \Rightarrow G = \langle g \rangle,$$

and G is cyclic.

[1] Same as surjective.

Continued...

6. [10 marks; avg: 1/10] Find the number of homomorphisms from $\mathbb{Z}_6$ to A_7. (Be careful: A_7 is not S_7.)

Solution: $\mathbb{Z}_6 = \langle 1 \rangle$, so a homomorphism $f : \mathbb{Z}_6 \longrightarrow A_7$ is completely determined by $f(1)$. Since $|f(1)|$ must divide $|1| = 6$ *and* $|f(1)|$ must divide $|A_7| = 2520$, there are four possibilities for $|f(1)|$:

Case 1: $\underline{|f(1)| = 1.}$ In this case, the only possibility is $f(1) = \epsilon$, the identity permutation.

Case 2: $\underline{|f(1)| = 2.}$ Since $f(1)$ must be of order 2, and in A_7,

$$f(1) = (ab)(cd),$$

a product of two disjoint 2-cycles. The number of such permutations is

$$\frac{7 \times 6}{2} \times \frac{5 \times 4}{2} \times \frac{1}{2} = 105.$$

Case 3: $\underline{|f(1)| = 3.}$ Since $f(1)$ must be of order 3 and in A_7,

$$f(1) = (abc) \text{ or } f(1) = (abc)(def),$$

a single 3-cycle or a product of two disjoint 3-cycles. The number of such permutations is

$$\frac{7 \times 6 \times 5}{3} + \frac{7 \times 6 \times 5}{3} \times \frac{4 \times 3 \times 2}{3} \times \frac{1}{2} = 70 + 280 = 350.$$

Case 4: $\underline{|f(1)| = 6.}$ Since $f(1)$ must be of order 6 and in A_7,

$$f(1) = (abc)(de)(fg),$$

a product of a 3-cycle and two 2-cycles, all disjoint. The number of such permutations is

$$\frac{7 \times 6 \times 5}{3} \times \frac{4 \times 3}{2} \times \frac{2 \times 1}{2} \times \frac{1}{2} = 210.$$

Conclusion: the total number of homomorphisms from $\mathbb{Z}_6$ to A_7 is $1 + 105 + 350 + 210 = 666$.

Continued...

7. [avg: 4/10] Let G be a group with identity element e. Let H and K be finite subgroups of G such that $|H| = m$ and $|K| = n$, with $\gcd(m, n) = 1$.

   (a) [4 marks] Show that $H \cap K = \{e\}$.

   Proof: let $d = |H \cap K|$. Since $H \cap K \leq H$ and $H \cap K \leq K$ we have

   $$d|m \text{ and } d|n.$$

   But m and n are relatively prime, so $d = 1$. That is, $H \cap K = \{e\}$.

   (b) [6 marks] Suppose in addition that $|G| = mn$. Show that for every $g \in G, g \neq e$, there are unique elements $h \in H$ and $k \in K$ such that $g = hk$.

   Proof: $HK = \{hk \mid h \in H, k \in K\}$ is a subset of G and

   $$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{mn}{1} = mn.$$

   If $|G| = mn$, then $G = HK$, as a set. Let $g \in G$ and suppose

   $$g = h_1k_1 \text{ and } g = h_2k_2,$$

   for some $h_1, h_2 \in H,\ k_1, k_2 \in K$. Then

   $$\begin{aligned} h_1k_1 = h_2k_2 &\Rightarrow k_1k_2^{-1} = h_1^{-1}h_2 \in H \cap K = \{e\} \\ &\Rightarrow k_1k_2^{-1} = e \text{ and } h_1^{-1}h_2 = e \\ &\Rightarrow k_1 = k_2 \text{ and } h_2 = h_1 \text{ (QED)} \end{aligned}$$

8. [avg: 3.4/10]

8.(a) [5 marks] Let G be a finite group with operation 'multiplication.' Let H be a non-empty subset of G that is closed under multiplication: $g, h \in H \Rightarrow gh \in H$. Prove $H \leq G$.

Proof: H is given to be a non-empty subset of G closed under multiplication. All we need to show is that H contains the identity, e, and that H is closed under inverses. We can do this in three steps:

1. For $g \in H$ and $h = g$ we have $g^2 \in H$. Then by taking $h = g^2$ we can conclude that $g^3 \in H$. Similarly (by induction if you will), $g^m \in H$ for all positive integers m.
2. Let $|G| = n$ and suppose $g \in H \leq G$. Then $g^n = e$, and by (1), $e \in H$.
3. Let $g \in H$. By (2), $g^n = e$. Then $g^{-1} = g^{n-1} \in H$, by (1).

So $H \leq G$.

8.(b) Let k be a positive integer.

(i) [2 marks] Let p be a prime number. Give an example of a group G with order p^k such that every non-identity element in G has order p.

Example:

$$G = \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{k \text{ times}}$$

(ii) [3 marks] Let $n \geq 2$. Show that if G is a group of order n^k such that every non-identity element of G has order n, then n must be a prime.

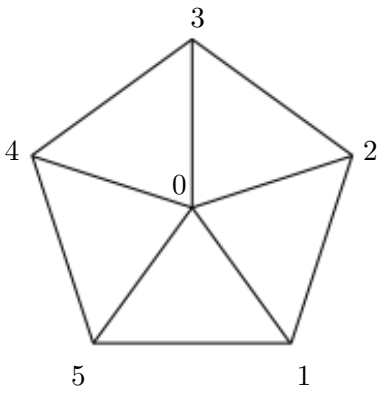
Proof: suppose $e \neq g \in G$ and $|g| = n$. Suppose n is not prime. Then n has divisors a, b such that $n = a\,b$ with $1 < a, b < n$. Then

$$|g^a| = \frac{n}{\gcd(n, a)} = \frac{n}{a} = b < n,$$

which contradicts the assumption that all non-identity elements of G have order n. Thus n must be prime.

Continued...

9. [10 marks; avg: 7.4/10] Every element in D_5 can be considered as a permutation of the five vertices of a regular pentagon. See the diagram to the right. Identify the subgroup G of ten permutations in S_5 that is isomorphic to D_5, and interpret them geometrically as rotations or reflections of the pentagon. (Be specific: Through how many degrees is each rotation? What is the axis of symmetry of each reflection?) Find $\text{stab}_G(2)$ and $\text{orbit}_G(2)$.



Solution: label the centre of the pentagon with 0.

rotation permutation: identity or 5-cycle	degrees around centre	reflection permutation: pair of disjoint 2-cycles	axis of reflection
(1)	0°	(12)(35)	line through 0 and 4
(12345)	72°	(13)(45)	line through 0 and 2
(13524)	144°	(34)(52)	line through 0 and 1
(14253)	216°	(14)(23)	line through 0 and 5
(15432)	288°	(24)(15)	line through 0 and 3

Finally

$$\text{stab}_G(2) = \{(1), (13)(45)\},\ \text{orbit}_G(2) = \{1, 2, 3, 4, 5\}.$$

Continued...

10. [avg: 5.4/10] Let $Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

(a) [4 marks] Find $C(Y)$, the centralizer of Y in $GL(2,\mathbb{R})$.

Solution: let $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R})$ such that $XY = YX$. 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

$$X = \begin{bmatrix} a & -c \\ c & a \end{bmatrix} \text{ and } C(Y) = \left\{ \begin{bmatrix} a & -c \\ c & a \end{bmatrix} \middle| \, a^2 + c^2 \neq 0, a, c \in \mathbb{R} \right\}.$$

(b) [2 marks] Explain why $H = \{A \in C(Y) \mid \det(A) = 1\}$ is a subgroup of $C(Y)$.

Solution: you can use the subgroup test OR simply observe that for $\det : GL(2,\mathbb{R}) \longrightarrow R^*$

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

and the intersection of two subgroups is itself a subgroup.

(c) [4 marks] Find a homomorphism $f : C(Y) \longrightarrow C(Y)$ such that $\ker(f) = H$, and show that your answer is correct. What is $\text{im}\,(f)$? BONUS: To which subgroup of R^* is $\text{im}\,(f)$ isomorphic?

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:

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

- $\ker(f) = H$:

$\ker(f) = \{A \in C(Y) \mid f(A) = I\} = \{A \in C(Y) \mid \det(A)\, I = I\} = \{A \in C(Y) \mid \det(A) = 1\} = H.$

Finally,

$$\text{im}\,(f) = \{f(A) \mid A \in C(Y)\} = \{(a^2 + c^2)\, I \mid a^2 + c^2 \neq 0\} = \{xI \mid x > 0\} \approx \{x \in \mathbb{R}^* \mid x > 0\}.$$

This page is for rough work or for extra space to finish a previous problem. It will not be marked unless you have indicated in a previous question to look at this page.

Continued...

This page is for rough work or for extra space to finish a previous problem. It will not be marked unless you have indicated in a previous question to look at this page.

Continued...

This page is for rough work or for extra space to finish a previous problem. It will not be marked unless you have indicated in a previous question to look at this page.

The end.