UNIVERSITY OF TORONTO
Faculty of Arts and Science
FINAL EXAMINATIONS, APRIL 2020
Solutions to MAT301H1S: Groups and Symmetry
Examiners: D. Burbulla, L. Döppenschmitt
Duration - 3.5 hours Total Marks: 120

Structure of the Exam: this exam consists of five parts, Parts A through E, spread over eight Assignments on Quercus:

1. Part A: Multiple Choice, which consists of 20 multiple choice questions, worth 2 marks each. Once you start Part A: Multiple Choice you have 60 minutes to finish it. You can only attempt each question once; and once you've done a question you cannot go back to it. Total marks for Part A: Multiple Choice: 40.

2. Part B: True or False, which consists of fifteen True or False questions, worth 1 mark each. Once you start Part B: True or False, you have 30 minutes to complete it. Total marks for Part B: True or False: 15.

   You also have to submit your counterexamples for all the True or False questions you chose as False. You can do that through the Quercus Assignment Part B: Submission.

3. Part B: Submission. This is the Assignment on Quercus to which you can submit your counterexamples for all the True or False questions that you chose as False. You can also submit your work to Crowdmark. Total marks for Part B: Submission: 5.

4. Part C: Multiple Answer Questions, which consists of five questions that require you to match up to 10 statements/questions with items/answers from a tear-down menu. Each question is worth 4 marks. Once you start Part C: Multiple Answer Questions, you have 20 minutes to finish it. You can only attempt each question once; and once you've done a question you cannot go back to it. Total marks for Part C: Multiple Answer Questions: 20.

5. Part D: Three Short Proofs, which will give you three statements to prove. You have 10 minutes to view them and to write them down. You will get one mark per question for viewing it. Total marks for Part D: Three Short Proofs: 3.

   Once you have written up your proofs you should submit them in Part D: Submission.

6. Part D: Submission. This is the Assignment on Quercus to which you can submit your three short proofs. Your proofs should be hand written; you can take a picture of them to submit. You can also submit your work to Crowdmark. Each short proof will be marked out of 4. Total marks for Part D: Submission: 12.

7. Part E: Long Question, which will give you one long, involved question to solve. You can only view the question for 10 minutes. You should copy it down. You will get 1 mark for viewing the question. The Long Question will be presented in two formats: math notation using text, like G x H; and also as an inserted image which presents the whole question in proper mathematical notation, like $G \oplus H$. Total marks for Part E: Long Question: 1.

8. Part E: Submission. Once you have written up your solution to the long question—hand written please—you can upload it to Part E: Submission as a jpg, pdf or png file. Or you can submit it to Crowdmark. The long question is worth 24 marks and the part marks for each part will be indicated in the question. Total marks for Part E: Submission: 24.

Order of the Exam and Timing: you *must* complete Parts A, B and C *before* you attempt Parts D and E. You can do Parts A, B and C in any order you wish; and you can do Parts D and E in any order you wish.

1. The quizzes in Parts A, B and C have time limits, so you can spend at most 110 minutes on them. That leaves you at least 100 minutes to do the rest of the exam, including writing up your solutions and submitting them. You will probably need *at least* 30 min to do the long question from Part E.

2. Once you start the exam, you have 3.5 hours to finish the whole thing.

3. Through Quercus (and Crowdmark, for that matter) we have complete records of which time you started a quiz, when you submitted an answer or a file, when you finished a quiz, etc. Thus we will know the precise instant when you started the exam, and whether or not you completed Parts A, B and C before you started Part D or E. We will also be able to determine if anything you submitted was late—i.e. 3.5 hours after you started. Late submissions will not be graded.

Submitting Your Files: for the questions that require you to show your work, you could submit your solutions to Quercus through Part B: Submission, Part D: Submission, and Part E: Submission. But we have created a Crowdmark assignment as well, called Exam Submissions, through which you can also submit your solutions to the written questions for Parts B, D and E. We would actually **prefer** if you submitted your solutions to the written questions in Parts B, D and E via Crowdmark. If you submit something to both Quercus and Crowdmark what you submit to each must be identical. If not, we will only mark the solution that was submitted first. No corrections or alterations to previously submitted work permitted.

Showing Your Work and Not Showing Your Work: approximately two thirds of the exam does not require you to show your work. In the one third of the exam that requires you to show your work, in particular in Parts D and E, you must, must explain your work. We will mark these parts very strictly: if you do not explain what you are doing, we will not try to figure it out—you will just lose marks. What you submit must be legible and coherent, making use of correct logic and correct mathematical notation. If something doesn't make sense we will just skip it. Moreover, what you submit should be your *own* work. We will watch out for solutions that are identical, or solutions that are copied verbatim from books or websites. Any such academic offence will seriously jeopardize your exam!

Notation: typing mathematical expressions into Quercus using fancy mathematical formatting is not always reliable, so for the most part the questions on Quercus will be typed up using standard-text mathematical notation. That is,

> G x H is the external direct product of the groups G and H
>
> G / H is the factor group of G by H
>
> Subscripts are denoted by _m, e.g. D_6 is the dihedral group of order 12
>
> Superscripts are denoted by ^m, e.g. x^2 is the square of x; x^{-1} is the inverse of x
>
> Z is the set of integers
>
> R is the set of real numbers
>
> A 3 x 3 matrix is represented by [a, b, c; d, e, f; g, h, i]. So the entries in the first row of A are a, b, c; the entries in the second row are d, e, f; and the entries of the third row are g, h, i.
>
> A 2 x 2 matrix is represented by [a, b; c, d] so the entries in the row of A are a, b; the entries in the second row are c, d.

General Advice: put aside a 3.5-hour time slot in which you can focus on the exam and work without distractions or interruptions. The structure of the exam requires you to organize your time and to pay attention to one question at a time. Don't let yourself get bogged down with one question. No question in Part A, B, C or D is worth very much by itself, so skipping any one of those questions is not serious. There are no penalties for guessing in Parts A or C, so if you have narrowed a question down to two choices you can just follow your mathematical intuition and guess.

Technical Issues: there is not much we can do if technical issues should arise. There have been no technical issues during all the quizzes and assignments we have run through Quercus this year, nor have there been any technical issues in all the assignments we have run through Crowdmark this year. So with a little luck there won't be any technical issues during this Exam either. However, should some issue arise, try to document it in some way.

Questions During the Exam: since students may be writing the exam during a continuous 24-hour period, there is no way we can be available to everybody to answer any question that may arise during the exam. So we won't answer any. If there is something you are not clear about, you can always look it up in the book! If that doesn't help, then you can state any assumption you are making so that you can continue with the question.

Final Thoughts: this exam can potentially count for 60% of your final grade, so it is worth your effort to cooperate with the instructions, try to do as well as possible on this exam, and get it over with. Considering that the term test and the tutorial quizzes could count as little as 25% of your final grade, you are being given a chance to complete a math course in which as much as 75% of your final grade is based on work you do at home. Don't blow it!

PART A: Twenty multiple choice questions, selected from the following 26. (avg: 27.6/40)

1. What is the order of the group $U(18) \oplus D_3$?

   (a) 18

   (b) 54

   (c) $\boxed{36}$

   (d) 108

   (e) 72

2. What is the order of the element $(4, 5)$ in the group $\mathbb{Z}_9 \oplus U(12)$?

   (a) 2

   (b) 9

   (c) 12

   (d) $\boxed{18}$

   (e) 3

3. The following are all Abelian groups of order 900. Which two are isomorphic to each other?

   (a) $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

   (b) $\boxed{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}}$

   (c) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

   (d) $\boxed{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{75} \oplus \mathbb{Z}_3}$

   (e) $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$

4. What is the class equation of D_8?

   (a) $16 = 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2$

   (b) $\boxed{16 = 2 + 2 + 2 + 2 + 4 + 4}$

   (c) $16 = 2 + 2 + 4 + 4 + 4$

   (d) $16 = 4 + 4 + 4 + 4$

   (e) $16 = 1 + 1 + 2 + 2 + 2 + 4$

5. Let G be a finite group with operation multiplication and identity element e. Let a be a non-identity element of G with $|a| = n$. Which of the following statements is *not* true?

   (a) $C(a) \leq C(a^2)$

   (b) $C(a^n) = G$

   (c) $\boxed{\mathrm{cl}\,(a) = \mathrm{cl}\,(a^{-1})}$

   (d) $|\mathrm{cl}\,(a)| = |\mathrm{cl}\,(a^{-1})|$

   (e) $C(a) = C(a^{-1})$

6. How many homomorphisms are there from D_6 to $\mathbb{Z}_5$.

   (a) 0

   (b) $\boxed{1}$

   (c) 2

   (d) 3

   (e) 4

7. How many homomorphisms are there from $\mathbb{Z}_{10}$ to D_5.

   (a) 2

   (b) 4

   (c) 6

   (d) 8

   (e) $\boxed{10}$

8. Which of the following statements is *not* true?

   (a) If $f : G \longrightarrow H$ is a homomorphism then $\ker(f) \lhd G$.

   (b) If H is a normal subgroup of G then there is a homomorphism f defined on G such that $\ker(f) = H$.

   (c) $\boxed{\text{If } H \text{ and } K \text{ are subgroups of } G \text{ such that } H \lhd K \text{ and } K \lhd G, \text{ then } H \lhd G.}$

   (d) If $f : G \longrightarrow H$ is a homomorphism and $f(x) = f(y)$, then $xy^{-1} \in \ker(f)$.

   (e) If $f : G \longrightarrow H$ is a homomorphism then there is a subgroup K of H such that

   $$G/\ker(f) \approx K.$$

9. Which of the following groups is not isomorphic to $U(144)$?

   (a) $U(9) \oplus \mathbb{U}(16)$

   (b) $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$

   (c) $\boxed{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3}$

   (d) $\mathrm{Aut}\,(\mathbb{Z}_{144})$

   (e) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12}$

10. What is the class equation of D_5?

    (a) $10 = 1 + 1 + 2 + 2 + 2 + 2$

    (b) $10 = 5 + 5$

    (c) $10 = 1 + 4 + 5$

    (d) $10 = 2 + 2 + 2 + 2 + 2$

    (e) $\boxed{10 = 1 + 2 + 2 + 5}$

11. Which of the following permutations $\alpha \in S_5$ satisfies $\alpha\,((125)(34))\,\alpha^{-1} = (354)(12)$?

    (a) $\boxed{\alpha = (13)(254)}$

    (b) $\alpha = (1432)$

    (c) $\alpha = (42)(135)$

    (d) $\alpha = (43)(152)$

    (e) $\alpha = (15342)$

12. How many elements in S_7 are in the conjugacy class of $(1435)(257)(64)$?

    (a) $\boxed{720}$

    (b) 5040

    (c) 210

    (d) 630

    (e) 420

13. How may symmetries does the solid shown to the right have?

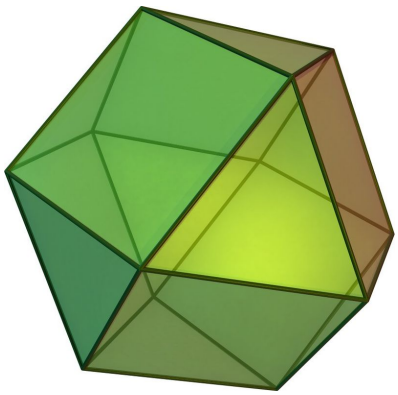
    (a) 16

    (b) 8

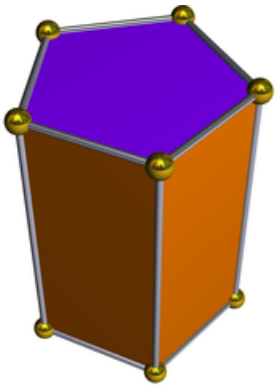
    (c) $\boxed{48}$

    (d) 20

    (e) 24



14. How may symmetries does the solid shown to the right have?



(a) 16

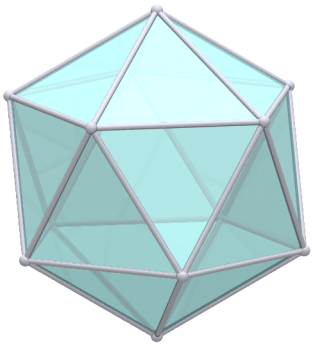
(b) 10

(c) $\boxed{20}$

(d) 40

(e) 5

15. How may symmetries does the solid shown to the right have?



(a) 20

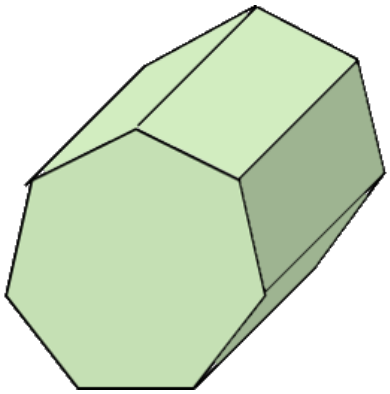
(b) $\boxed{120}$

(c) 60

(d) 40

(e) 30

16. How may symmetries does the solid shown to the right have?



(a) $\boxed{28}$

(b) 42

(c) 48

(d) 14

(e) 24

17. Suppose A and B are rotations of 180° about the points (a_1, a_2) and (b_1, b_2), respectively. Which statement best describes the combined effect of A followed by B on an arbitrary point (x_1, x_2) in the plane?

(a) A reflection in the line passing through the two points (a_1, a_2) and (b_1, b_2).

(b) A reflection in the perpendicular bisector of the line segment joining the two points (a_1, a_2) and (b_1, b_2).

(c) A rotation about the midpoint of the line segment joining the two points (a_1, a_2) and (b_1, b_2).

(d) $\boxed{\text{A translation along a line parallel to the line joining the two points } (a_1, a_2) \text{ and } (b_1, b_2).}$

(e) A translation along a line perpendicular to the line joining the two points (a_1, a_2) and (b_1, b_2).

18. What is the class equation of $S(D)$, the symmetry group of the dodecahedron?

    (a) $\boxed{120 = 2 + 20 + 12 + 12 + 15 + 20 + 12 + 12 + 15}$

    (b) $120 = 2 + 40 + 24 + 24 + 30$

    (c) $120 = 2 + 20 + 24 + 24 + 20 + 30$

    (d) $120 = 2 + 40 + 24 + 24 + 15 + 15$

    (e) $120 = 2 + 40 + 48 + 30$

19. What is the order of the group $\mathbb{Z}_3 \oplus U(15)/\langle(2, 4)\rangle$?

    (a) 2

    (b) $\boxed{4}$

    (c) 6

    (d) 8

    (e) 12

20. Which of the following is not isomorphic to $U(105)$?

    (a) $\boxed{U(7) \oplus U(16)}$

    (b) $U(3) \oplus U(5) \oplus U(7)$

    (c) $U(21) \oplus U(5)$

    (d) $U(15) \oplus U(7)$

    (e) $U(35) \oplus U(3)$

21. How many elements of order 3 are there in A_7?

    (a) 70

    (b) 105

    (c) 280

    (d) $\boxed{350}$

    (e) 560

22. What is the order of the permutation $(135)(26143)$ in S_6?

    (a) $\boxed{3}$

    (b) 6

    (c) 9

    (d) 12

    (e) 15

23. What is the inverse of the permutation (1435) in S_5?

(a) (1354)

(b) $\boxed{(1534)}$

(c) (5431)

(d) (1435)

(e) (1345)

24. What is the index of the subgroup $\{1, 7, 11\}$ in $U(19)$?

(a) $\boxed{6}$

(b) 3

(c) 7

(d) 11

(e) 9

25. Let A and B be two conjugate matrices in $GL(n, \mathbb{R})$. Which of the following statements is not true?

(a) $\boxed{AB = BA}$

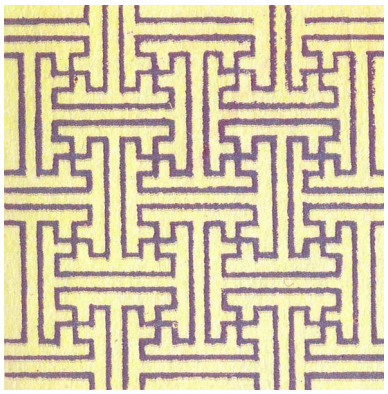
(b) $A \in \text{cl}(B)$

(c) A and B are similar matrices.

(d) The order of A is the same as the order of B.

(e) $\det(A) = \det(B)$

26. Which of the following symmetries does the wallpaper pattern to the right have? Indicate all answers that apply.



(a) $\boxed{\text{A reflection in a horizontal axis}}$

(b) $\boxed{\text{A reflection in a vertical axis}}$

(c) $\boxed{\text{A rotation of order 2}}$

(d) $\boxed{\text{A rotation of order 4}}$

(e) $\boxed{\text{A non-trivial glided reflection}}$

PART B: Fifteen True or False questions selected from the following 20 statements. If the statement is False give a counterexample to show that it is False. Students submit their counterexamples separately. True or False avg: 11.4/15; Counter examples avg: 2.4/5

1. If G is non-Abelian then $\mathrm{Aut}\,(G)$ is not cyclic. **True**

2. $D_{13} \approx \mathrm{Inn}\,(D_{13})$ **True**

3. The group of all $n \times n$ diagonal matrices with every diagonal entry ± 1 is isomorphic to

$$\underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{n \text{ times}}.$$

True

4. If G is an Abelian group of order 16 which has at least one element of order 8 and at least two elements of order 2, then $G \approx \mathbb{Z}_8 \oplus \mathbb{Z}_2$. **True**

5. Every Abelian group of order 78 is cyclic. **True**

6. If G is non-Abelian and H is a normal subgroup of G, then the factor group G/H is also non-Abelian.

   False: $S_4/A_4 \approx \mathbb{Z}_2$

7. The group G is Abelian if and only if G is cyclic.

   False: $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is Abelian but not cyclic. The other implication is True.

8. The group G is Abelian if and only if $f : G \longrightarrow G$ defined by $f(x) = x^2$ is a group homomorphism. **True**

9. The finite group G is Abelian if and only if $G/Z(G)$ is cyclic. **True**

10. The group G is Abelian if and only if the order of every non-identity element of G is 2.

    False: $\mathbb{Z}_3$ is Abelian but has elements of order 3. The other implication is True.

11. The finite group G is Abelian if and only if $|G| = p$, for some prime number p.

    False: $\mathbb{Z}_6$ is Abelian but 6 is not a prime. The other implication is True.

12. The group G is Abelian if and only if $f : G \longrightarrow G$ defined by $f(x) = x^{-1}$ is a group homomorphism. **True**

13. The group G is Abelian if and only if $Z(G) = G$. **True**

14. The group G is Abelian if and only if every subgroup of G is normal in G.

    False: in the Quaternions, $\mathcal{Q}$, the only subgroup of order 2 is the center, which is normal in $\mathcal{Q}$. The other non-trivial subgroups have order 4 and index 2, so are normal in $\mathcal{Q}$. But $\mathcal{Q}$ is not Abelian. The other implication is True.

15. The finite group G is Abelian if and only if G is an external direct product of cyclic groups. **True**

16. The finite group G is Abelian if and only if every non-identity element $a \in G$ such that a^{-1} is in $\mathrm{cl}\,(a)$ has order 2.

    False: in A_4, the conjugacy classes are

    $$\{(1)\}, \{(12)(34), (13)(24), (14)(23)\}, \{(123), (243), (142), (134)\}, \{(132), (234), (124), (143)\}.$$

    So $\alpha^{-1} \in \mathrm{cl}(\alpha)$ only if α has order 2. But A_4 is not Abelian.

    The other implication is True.

17. The group G is Abelian if and only if $C(a) = G$ for every $a \in G$. **True**

18. If G is a group with order $2p$, for some prime number p, then G is Abelian.

    False: D_3 has order $6 = 2 \cdot 3$ but D_3 is not Abelian.

19. The group G is Abelian if and only if for every $x \in G$ there is a $y \in G$ such that $x = y^2$.

    False: in $\mathbb{Z}_6$ the 'squares' y^2 are $2y$. And for $y \in Z_6$ the 'squares' are

    $$2 \cdot 0 = 0,\ 2 \cdot 1 = 2,\ 2 \cdot 2 = 4,\ 2 \cdot 3 = 0,\ 2 \cdot 4 = 2,\ 2 \cdot 5 = 4.$$

    So no odd number in $\mathbb{Z}_6$ is a square. But $\mathbb{Z}_6$ is Abelian. The other implication is True.

20. If G is a group of order p^2, for some prime number p, then G is Abelian. **True**

PART C: multiple-answer questions, from a tear-down menu. Five of the following seven questions are selected, with 10 matches to make in each question. (avg: 13.2/20)

1. For each of the following statements pick from the given list of Theorems the Theorem that best matches the statement.

   Statements:

   - If G is a finite group and H is a subgroup of G then the order of H divides the order of G. **Ans:** (a)
   - Every finite Abelian group is the direct product of cyclic groups of prime-power order. **Ans:** (b)
   - Every group is isomorphic to a group of permutations. **Ans:** (c)
   - If f is a homomorphism from the group G to the group H then the image of f is isomorphic to the factor group of G by the kernel of f. **Ans:** (d)
   - In any group the inverse of a product of two elements is the product of the inverses of the two elements, but in reverse order. **Ans:** (e)
   - Every subgroup of a finite cyclic group G is cyclic and for each divisor of the order of G there is exactly one subgroup of G with order equal to that divisor. **Ans:** (f)
   - If G is a finite group and p is a prime that divides the order of G, then G has an element of order p. **Ans:** (g)
   - If the factor group of G by its center is cyclic then G is Abelian. **Ans:** (h)
   - If G is a finite Abelian group and the prime number p divides the order of the group G, then G has an element of order p. **Ans:** (i)
   - If G is a finite group of permutations of a set and x is any element in the set, then the order of G is the product of the number of elements in the stabilizer of x and the number of elements in the orbit of x. **Ans:** (j)

   Theorems:

   (a) Lagrange's Theorem

   (b) The Fundamental Theorem of Finite Abelian Groups

   (c) Cayley's Theorem

   (d) The First Isomorphism Theorem

   (e) Socks-Shoes Property

   (f) The Fundamental Theorem of Cyclic Groups

   (g) Cauchy's Theorem

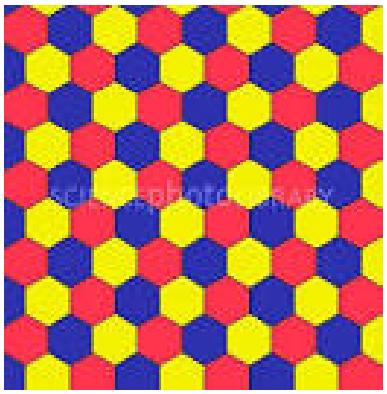
   (h) The G/Z Theorem

   (i) Cauchy's Theorem for Abelian Groups

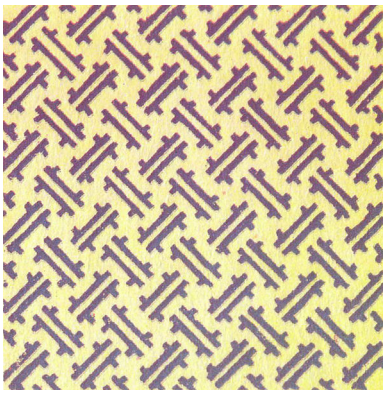
   (j) Orbit-Stabilizer Theorem

   Plus some 'distractors'

Q2.



Q3.



Q4.

Does the given wall paper pattern have a symmetry of the following type?

type of symmetry	Q2.	Q3.	Q4.
a rotation of order 2	Yes	No	Yes
a rotation of order 3	No	Yes	No
a rotation of order 4	Yes	No	Yes
a rotation of order 5	No	No	No
a rotation of order 6	No	No	No
a reflection in a horizontal axis	No	Yes	No
a reflection in a vertical axis	No	No	No
a reflection in a diagonal axis	No	Yes	Yes
a non-trivial glide reflection	No	Yes	Yes
a translation	Yes	Yes	Yes

5. How many elements of each possible order are there in the group $\mathbb{Z}_8 \oplus \mathbb{Z}_3$?

6. How many elements of each possible order are there in the group $\mathbb{Z}_{12} \oplus U(4)$?

7. How many elements of each possible order are there in the group $\mathrm{Aut}\,(\mathbb{Z}_{45})$?

order	$\mathbb{Z}_8 \oplus \mathbb{Z}_3$ $\approx \mathbb{Z}_{24}$	$\mathbb{Z}_{12} \oplus U(4)$ $\approx \mathbb{Z}_{12} \oplus \mathbb{Z}_2$	$\mathrm{Aut}\,(\mathbb{Z}_{45}) \approx U(45) \approx U(9) \oplus U(5)$ $\approx \mathbb{Z}_6 \oplus \mathbb{Z}_4 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{12}$
1	1	1	1
2	1	3	3
3	2	2	2
4	2	4	4
5	0	0	0
6	2	6	6
7	0	0	0
8	4	0	0
12	4	8	8
24	8	0	0
Total	24	24	24

PART D: Three Short Proofs. Each student is given three of the following seven statements to prove. They then submit their hand-written solutions to be marked. (avg: 9.4/15)

1. If H and K are normal subgroups of G and $H \cap K = \{e\}$, then G is isomorphic to a subgroup of $G/H \oplus G/K$.

   Proof: define $\phi : G \longrightarrow G/H \oplus G/K$ by $\phi(x) = (xH, xK)$. Then

   $\phi(xy) = (xyH, xyK) = (xH\, yH, xK\, yK) = (xH, xK)(yH, yK) = \phi(x)\phi(y)$, and

   $\ker(\phi) = \{x \in G \mid xH = H \text{ and } xK = K\} = \{x \in G \mid x \in H, x \in K\} = H \cap K = \{e\}$.

   Thus ϕ is a one-to-one homomorphism. Then by the First Isomorphism Theorem,

   $$G \approx G/\ker(\phi) \approx \text{im}\,(\phi) \leq G/H \oplus G/K.$$

2. If m and n are positive positive integers then the mapping $f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_n$ defined by $f(x) = x \mod n$ is a homomorphism if and only if n divides m.

   Proof: let $f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_n$ be defined by $f(x) = x$.

   Note that in $\mathbb{Z}_m$, $\underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} = m \equiv 0 \bmod m$. If ϕ is a homomorphism, then

   $$0 = f(0) = \phi(\underbrace{1 + 1 + \cdots + 1}_{m \text{ times}}) = m\,\phi(1) = m \cdot 1 = m;$$

   that is, $m \equiv 0 \bmod n$; so n divides m. Conversely, if n divides m, then $m = kn$, for some positive integer k. Then

   $$x + y \equiv q \bmod m \Rightarrow kn \text{ divides } x + y - q \Rightarrow n \text{ divides } x + y - q.$$

   Thus $x + y \equiv q \bmod m \Rightarrow x + y \equiv q \bmod n$, and so $f(x + y) = f(x) + f(y)$, which means that f is a homomorphism.

3. Every subgroup of D_n of odd order is cyclic.

   Proof: D_n consists of n rotations, which form a cyclic subgroup of D_n of order n; and n reflections, which all have order 2. Thus any subgroup G of D_n that has odd order contains no reflections, else 2 divides an odd number. Thus the subgroup G consists solely of rotations. That means G is a subgroup of a cyclic group, so is cyclic.

4. If H is a subgroup of S_n and the order of H is an odd number, then $H \leq A_n$.

   Proof: let $h \in H$. Since $|H|$ is odd, the order of h is also odd. If h is written as a product of disjoint cycles in S_n, then each cycle must have odd order, since only the lowest common multiple of odd numbers can be odd. But each cycle of length an odd number is an even permutation. Thus $h \in A_n$.

5. If G is a group of order n and k is an integer relatively prime to n, then the mapping $\phi : G \longrightarrow G$ defined by $\phi(g) = g^k$ is one-to-one.

   Proof: since $\gcd(n, k) = 1$ there are integers a and b such that

$$1 = ak + bn \Leftrightarrow ak = 1 - bn.$$

$$\begin{aligned} \text{Thus, for } x, y \in G: \ \phi(x) = \phi(y) &\Rightarrow x^k = y^k \\ &\Rightarrow (x^k)^a = (y^k)^a \\ &\Rightarrow x^{ak} = y^{ak} \\ &\Rightarrow x^{1-bn} = y^{1-bn} \\ &\Rightarrow x\, x^{-bn} = y\, y^{-bn} \\ &\Rightarrow x\, (x^n)^{-b} = y\, (y^n)^{-b} \\ (\text{since } |G| = n) &\Rightarrow x\, e^{-b} = y\, e^{-b} \\ &\Rightarrow x\, e = y\, e \\ &\Rightarrow x = y, \end{aligned}$$

   and ϕ is one-to-one. **Note:** ϕ is not necessarily a homomorphism.

6. For $n \geq 3$, $Z(S_n) = \{\epsilon\}$.

   Proof: suppose $\sigma \in S_n$ and $\sigma \neq \epsilon$. Then $\sigma(i) \neq i$, for some i. Let $\sigma(i) = j \neq i$. Pick $k \leq n$ such that $k \neq i, k \neq j$. (Possible since $n \geq 3$.) Let $\tau = (ik)$. Then

$$(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \tau(j) = k \text{ but } (\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(k) \neq j,$$

   since σ is one-to-one and $\sigma(i) = j$. Thus $\tau \circ \sigma \neq \sigma \circ \tau$ and σ can't be in $Z(S_n)$.

7. Let $A \in GL(3, \mathbb{R})$. Show that $\mathrm{cl}\,(A) \neq \mathrm{cl}\,(-A)$ but that $|\mathrm{cl}\,(A)| = |\mathrm{cl}\,(-A)|$.

   Proof: if $-A = XAX^{-1}$ for some $X \in GL(3, \mathbb{R})$, then

$$-\det(A) = \det(-A) = \det(XAX^{-1}) = \det(X)\det(A)\det(X^{-1}) = \det(A),$$

   and consequently $\det(A) = 0$, which means A is not in $GL(3, \mathbb{R})$. Thus $-A$ can't be in $\mathrm{cl}\,(A)$, and so $\mathrm{cl}\,(A) \neq \mathrm{cl}\,(-A)$.

   For the other part:

$$\begin{aligned} Y \in \mathrm{cl}(A) &\Leftrightarrow Y = XAX^{-1}, \text{ for some } X \in GL(3, \mathbb{R}) \\ &\Leftrightarrow -Y = X(-A)X^{-1}, \text{ for some } X \in GL(3, \mathbb{R}) \\ &\Leftrightarrow -Y \in \mathrm{cl}(-A). \end{aligned}$$

   That is, multiplicaton by $-I$ gives a one-to-one correspondence between $\mathrm{cl}(A)$ and $\mathrm{cl}(-A)$, so they have the same order.

PART E: Long Written Question. Each student is assigned one of these four questions. They then submit their hand-written solution to be marked. (avg: 9.5/25)

1. Let G be a finite group with operation multiplication. For $x \in G$ define $f_x : \mathbb{Z} \longrightarrow G$ by $f_x(m) = x^m$. Prove the following:

   (a) [2 marks] f_x is a group homomorphism.
   Proof: $f_x(m+n) = x^{m+n} = x^m x^n = f_x(m) f_y(m)$.

   (b) [4 marks] $\ker(f_x) = \langle |x| \rangle$
   Proof: to show $\ker(f_x) = \langle |x| \rangle$ show $\ker(f_x) \subset \langle |x| \rangle$ and $\langle |x| \rangle \subset \ker(f_x)$:
   $m \in \ker(f_x) \Rightarrow f(m) = e \Rightarrow x^m = e \Rightarrow |x| \big| m \Rightarrow m \in \langle |x| \rangle \Rightarrow \ker(f_x) \subset \langle |x| \rangle$,
   and
   $m \in \langle |x| \rangle \Rightarrow m = k|x| \Rightarrow f_x(m) = x^{k|x|} = (x^{|x|})^k = e^k = e \Rightarrow \langle |x| \rangle \subset \ker(f_x)$.

   (c) [2 marks] $\mathrm{im}\,(f_x) = \langle x \rangle$
   Proof: $\mathrm{im}\,(f_x) = \{f_x(m) \mid m \in \mathbb{Z}\} = \{x^m \mid m \in \mathbb{Z}\} = \langle x \rangle$.

   (d) [6 marks] If G is Abelian then the set $H = \{f_x \mid x \in G\}$ with the operation $*$ defined by
   $$(f_x * f_y)(m) = f_x(m)\, f_y(m), \text{ for all } m \in \mathbb{Z},$$
   is an Abelian group.
   Proof: in five steps.
   Step 1: for $x, y \in G$ show $f_x * f_y$ is in H. Let $m \in \mathbb{Z}$. Then
   $$(f_x * f_y)(m) = f_x(m)\, f_y(m) = \underbrace{x^m\, y^m = (xy)^m}_{\textit{since } G \textit{ is Abelian}} = f_{xy}(m).$$
   This shows that $f_x * f_y = f_{xy}$. Since $xy \in G$, $f_x * f_y \in H$.
   Step 2: existence of identity. The identity function is f_e since
   $$f_x * f_e = f_{xe} = f_x = f_{ex} = f_e * f_x.$$
   Step 3: H has inverses. Let $f_x \in H$. Then $f_x^{-1} = f_{x^{-1}}$ since
   $$f_x * f_{x^{-1}} = f_{xx^{-1}} = f_e = f_{x^{-1}x} = f_{x^{-1}} * f_x.$$
   Step 4: $*$ is associative. Let $x, y, z \in G$. Then
   $$(f_x * f_y) * f_z = f_{xy} * f_z = f_{xyz} = f_x * f_{yz} = f_x * (f_y * f_z).$$
   Steps 1 through 4 show that H together with the operation $*$ is a group. Finally,
   Step 5: H is Abelian. Let $x, y \in G$. Then
   $$f_x * f_y = \underbrace{f_{xy} = f_{yx}}_{\textit{since } G \textit{ is Abelian}} = f_y * f_x.$$

(e) [5 marks] If G is Abelian, then $H \approx G$, with H as in part (d).

Proof: define $\phi : G \longrightarrow H$ by $\phi(x) = f_x$. Then, making use of the results proved in part (d),

- ϕ is a homomorphism: $\phi(xy) = f_{xy} = f_x * f_y = \phi(x) * \phi(y)$.
- ϕ is one-to-one:

$$\phi(x) = f_e \Rightarrow f_x = f_e \Rightarrow f_x(1) = f_e(1) \Rightarrow x = e \Rightarrow \ker(\phi) = \{f_e\}.$$

- ϕ is onto: for $f_x \in H$ we have $\phi(x) = f_x$, so $\mathrm{im}\,(\phi) = H$.

So ϕ is an isomorphism and thus $G \approx H$.

(f) [5 marks] If G is Abelian, then $\mathrm{Aut}\,(H) \approx \mathrm{Aut}\,(G)$, with H as in part (d).

Proof: it's true in general that isomorphic groups have isomorphic automorphism groups. The proof of *that* is as follows. Let $\phi : G \longrightarrow H$ be the isomorphism from part (e); let $\alpha \in \mathrm{Aut}\,(G)$. Define $f : \mathrm{Aut}\,(G) \longrightarrow \mathrm{Aut}\,(H)$ by

$$f(\alpha) = \phi \circ \alpha \circ \phi^{-1}.$$

Then check the following:

1. $f(\alpha)$ is in $\mathrm{Aut}\,(H)$: i.e. $f(\alpha) : H \longrightarrow H$ and $f(\alpha)$ is an isomorphism. Let $x, y \in H$.
   $f(\alpha)$ is a homomorphism:
   $(f(\alpha))(xy) = (\phi\circ\alpha\circ\phi^{-1})(xy) = \phi(\alpha(\phi^{-1}(xy))) = \phi(\alpha(\phi^{-1}(x)\,\phi^{-1}(y)))$
   $= \phi(\alpha(\phi^{-1}(x))\,\alpha(\phi^{-1}(y))) = \phi(\alpha(\phi^{-1}(x))\,\phi(\alpha(\phi^{-1}(y))) = (f(\alpha))(x)(f(\alpha))(y).$
   $f(\alpha)$ is one-to-one:
   $f(\alpha)(x) = e_H \Rightarrow \phi(\alpha(\phi^{-1}(x))) = e_H \Rightarrow \alpha(\phi^{-1}(x)) = \phi^{-1}(e_H) = e_G$
   $\Rightarrow \phi^{-1}(x) = \alpha^{-1}(e_G) = e_G \Rightarrow x = \phi(e_G) = e_H$
   $f(\alpha)$ is onto: for any $y \in H$,
   $(f(\alpha))(\phi(\alpha^{-1}(\phi^{-1}(y)))) = (\phi \circ \alpha \circ \phi^{-1})(\phi(\alpha^{-1}(\phi^{-1}(y)))) = y$
2. $f : \mathrm{Aut}\,(G) \longrightarrow \mathrm{Aut}\,(H)$ is a homomorphism:
   Let $\alpha, \beta \in \mathrm{Aut}\,(G)$. Then

$$f(\alpha \circ \beta) = \phi \circ \alpha \circ \beta \circ \phi^{-1} = \phi \circ \alpha \circ \phi^{-1} \circ \phi \circ \beta \circ \phi^{-1} = f(\alpha) \circ f(\beta)$$

3. f is one-to-one: let $i_G : G \longrightarrow G$ and $i_H : H \longrightarrow H$ be the identity automorphisms on G and H, respectively. Then
   $f(\alpha) = i_H \Rightarrow \phi\circ\alpha\circ\phi^{-1} = i_H \Rightarrow \phi\circ\alpha = \phi\circ i_H = \phi \Rightarrow \alpha = \phi^{-1}\circ\phi = i_G$
4. f is onto: let $\beta \in \mathrm{Aut}\,(H)$. Then
   $f(\phi^{-1} \circ \beta \circ \phi) = \phi \circ \phi^{-1} \circ \beta \circ \phi \circ \phi^{-1} = i_G \circ \beta \circ i_H = \beta.$

Thus f is an isomorphism and so $\mathrm{Aut}\,(H) \approx \mathrm{Aut}\,(G)$.

2. Let p be a prime.

(a) [6 marks] How many subgroups does $\mathbb{Z}_p \oplus \mathbb{Z}_p$ have?

Solution: we know that $|\mathbb{Z}_p \oplus \mathbb{Z}_p| = p^2$ and that every non-identity element in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has order p. If $G \leq \mathbb{Z}_p \oplus \mathbb{Z}_p$ then by Lagrange's Theorem $|G| = 1, p$ or p^2.

1. If $|G| = 1$ then G is the trivial subgroup.
2. If $|G| = p^2$ then $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$, the whole group.
3. If $|G| = p$, then $G \approx \mathbb{Z}_p$ and $G = \langle x \rangle$ for some $x \in \mathbb{Z}_p \oplus \mathbb{Z}_p$, with $|x| = p$. There are $p^2 - 1$ elements of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ but $p - 1$ of them are in the same subgroup: that is, if $G = \langle x \rangle$, then G is generated by all of $x, x^2, x^3, \ldots, x^{p-1}$. Thus the number of distinct subgoups of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is

$$\frac{p^2 - 1}{p - 1} = p + 1.$$

So in total, $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has $p + 3$ subgroups.

(b) [7 marks] How many homomorphisms are there from $\mathbb{Z}_p \oplus \mathbb{Z}_p$ to $\mathbb{Z}_p$?

Solution: let $f : \mathbb{Z}_p \oplus \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ be a homomorphism. Since $|\mathrm{im}\,(f)| \big| p$, there are only two possibilities:

1. $|\mathrm{im}\,(f)| = 1$, in which case f is the zero map: $f(x) = 0$, for all $x \in \mathbb{Z}_p \oplus \mathbb{Z}_p$.
2. $|\mathrm{im}\,(f)| = p$, in which case $|\ker(f)| = p$. Hence $\mathrm{im}\,(f) = \mathbb{Z}_p$ and $\ker(f) \approx \mathbb{Z}_p$. Suppose $\ker(f) = \langle x \rangle$, one of the $p+1$ subgroups of $\mathbb{Z}_p \oplus \mathbb{Z}_p$ of order p. Then $\mathbb{Z}_p \oplus \mathbb{Z}_p / \ker(f) \approx \mathbb{Z}_p$, so there is a $y \in \mathbb{Z}_p \oplus \mathbb{Z}_p$ such that

$$\mathbb{Z}_p \oplus \mathbb{Z}_p / \ker(f) = \langle y \ker(f) \rangle,$$

and in terms of cosets,

$$\mathbb{Z}_p \oplus \mathbb{Z}_p = \ker(f) \cup y \ker(f) \cup y^2 \ker(f) \cup \cdots \cup y^{p-1} \ker(f).$$

Then the homomorphism f is completely determined by the value of $f(y)$: if $f(y) = m \in \mathbb{Z}_p$, then for any $z \in y^i \ker(f)$ we have $z = y^i x^k$, for some x^k in $\ker(f)$, and so

$$f(z) = f(y^i x^k) = f(y^i) + f(x^k) = i\,m + 0 = i\,m.$$

Since there are $p + 1$ choices for $\ker(f)$ and $p - 1$ choices for m, in this case the total number of homomorphisms is $(p + 1)(p - 1) = p^2 - 1$.

In total there are $1 + p^2 - 1 = p^2$ possible homomorphisms from $\mathbb{Z}_p \oplus \mathbb{Z}_p$ to $\mathbb{Z}_p$.

Alternate Solution: this approach uses techniques of Linear Algebra, but if you use this approach you must justify everything. First observe that if $a, b \in \mathbb{Z}_p, a, b \neq 0$, and $f : \mathbb{Z}_p \oplus \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ is a homomorphism, then

$$\begin{aligned} f((a,b)) &= f((a,0)+(0,b)) \\ &= f((a,0)) + f((0,b)) \\ &= f(\underbrace{(1,0)+(1,0)+\cdots+(1,0)}_{a \text{ times}}) + f(\underbrace{(0,1)+(0,1)+\cdots+(0,1)}_{b \text{ times}}) \\ &= \underbrace{f((1,0))+f((1,0))+\cdots+f((1,0))}_{a \text{ times}} + \underbrace{f((0,1))+f((0,1))+\cdots f((0,1))}_{b \text{ times}} \\ &= a\, f((1,0)) + b\, f((0,1)). \end{aligned}$$

Similarly,

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

This shows that the homomorphism f is completely determined by the two values, $f((1,0))$ and $f((0,1))$.

Now, if $f : \mathbb{Z}_p \oplus \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ is a homomorphism, then $|\mathrm{im}\,(f)| \,\big|\, p$, so there are only two possibilities:

1. $|\mathrm{im}\,(f)| = 1$, in which case f is the zero map: $f((a,b)) = 0$.
2. $|\mathrm{im}\,(f)| = p$, in which case $\mathrm{im}\,(f) = \mathbb{Z}_p$ and $\mathrm{im}\,(f)$ must contain an element of order p. Since f is not the zero map, at least one of $f((1,0))$ and $f((0,1))$ is not 0.

   (a) If $f((1,0)) = 0$, then $f((0,1)) \in \{1, 2, \ldots, p-1\}$, giving $p-1$ possibilities.
   (b) If $f((0,1)) = 0$, then $f((1,0)) \in \{1, 2, \ldots, p-1\}$, giving $p-1$ possibilities.
   (c) If neither $f((1,0)) = 0$ nor $f((0,1)) = 0$, then there are

   $$(p-1)(p-1) = p^2 - 2p + 1$$

   ways to pick $f((1,0))$ and $f((0,1))$, giving $p^2 - 2p + 1$ possibilities for f.

   Thus the total number of homomorphisms in this case is

   $$p - 1 + p - 1 + p^2 - 2p + 1 = p^2 - 1.$$

And so, in total, there are $1 + p^2 - 1 = p^2$ homomorphisms from $\mathbb{Z}_p \oplus \mathbb{Z}_p$ to $\mathbb{Z}_p$.

(c) [6 marks] Let G be the set of all homomorphisms from $\mathbb{Z}_p \oplus \mathbb{Z}_p$ to $\mathbb{Z}_p$. Show that G together with the operation of function addition, $+$, defined by

$$(f+g)(x) = f(x) + g(x), \text{ for all } x \in \mathbb{Z}_p \oplus \mathbb{Z}_p,$$

for $f, g \in G$, is an Abelian group.

Proof: in five steps.

Step 1: for $f, g \in G$ show $f+g$ is in G. Let $f, g \in G, x, y \in \mathbb{Z}_p \oplus \mathbb{Z}_p$. Then

$$\begin{aligned}(f+g)(x+y) &= f(x+y) + g(x+y) \\ &= f(x) + f(y) + g(x) + g(y) \\ &= f(x) + g(x) + f(y) + g(y), \text{ since } \mathbb{Z}_p \text{ is Abelian} \\ &= (f+g)(x) + (f+g)(y),\end{aligned}$$

which means $f + g \in G$.

Step 2: existence of identity. The zero map, $e(x) = 0$ for all $x \in \mathbb{Z}_p \oplus \mathbb{Z}_p$, is the identity, since for any $f \in G$, and every $x \in \mathbb{Z}_p \oplus \mathbb{Z}_p$,

$$(e+f)(x) = e(x)+f(x) = 0+f(x) = f(x) = f(x)+0 = f(x)+e(x) = (f+e)(x).$$

That is $e + f = f = f + e$.

Step 3: G has inverses. For $f \in G$ define $-f : \mathbb{Z}_p \oplus \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ by

$$(-f)(x) = -f(x), \text{ the additive inverse of } f(x) \in \mathbb{Z}_p.$$

Then $-f \in G$ since for all $x, y \in \mathbb{Z}_p \oplus \mathbb{Z}_p$,

$$(-f)(x+y) = -(x+y) = -x - y = (-f)(x) + (-f)(y);$$

and $-f$ is the inverse of f, since

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0.$$

That is, $f + (-f) = e$, the zero map.

Step 4: functional addition is associative. Let $f, g, h \in G, x \in \mathbb{Z}_p \oplus \mathbb{Z}_p$. Then

$$(f+(g+h))(x) = f(x)+(g+h)(x) = f(x)+g(x)+h(x) = (f+g)(x)+h(x) = ((f+g)+h)(x).$$

Since this is true for any x, we have $f + (g + h) = (f + g) + h$.

Step 5: Show G is Abelian. Let $f, g \in G, x \in \mathbb{Z}_p \oplus \mathbb{Z}_p$. Then

$$(f+g)(x) = \underbrace{f(x) + g(x) = g(x) + f(x)}_{\textit{since } \mathbb{Z}_p \textit{ is Abelian}} = (g+f)(x),$$

so $f + g = g + f$.

(d) [3 marks] Show that $G \approx \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Proof: $|G| = p^2$ and there are only two Abelian groups up to isomorphism of order p^2 : $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Let $g \in G$ with order n and let x be any element in $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Then

$$(\underbrace{g + g + \cdots + g}_{p \text{ times}})(x) = p\, g(x) = 0 \text{ in } \mathbb{Z}_p.$$

Thus $n \big| p$, which means $n = 1$ or p. So G has no element of order p^2, and by default $G \approx \mathbb{Z}_p \oplus \mathbb{Z}_p$.

(e) [1 mark] For $x \in \mathbb{Z}_p \oplus \mathbb{Z}_p$, define $x^* : G \longrightarrow \mathbb{Z}_p$ by

$$x^*(g) = g(x).$$

Show that x^* is a homomorphism.

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

$$x^*(f + g) = (f + g)(x) = f(x) + g(x) = x^*(f) + x^*(g).$$

(f) [1 mark] Assume that $H = \{x^* \mid x \in \mathbb{Z}_p \oplus \mathbb{Z}_p\}$ together with function addition, $+$, defined by

$$(x^* + y^*)(g) = x^*(g) + y^*(g), \text{ for } g \in G,$$

for $x^*, y^* \in H$, is a group. Suggest a homomorphism $\phi : \mathbb{Z}_p \oplus \mathbb{Z}_p \longrightarrow H$ that you could use to show $H \approx \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Suggestion: $\phi(x) = x^*$.

3. Define the following six matrices in $O(3,\mathbb{R})$:

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ P_{132} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix},\ P_{123} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

$$P_{23} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},\ P_{13} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},\ P_{12} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

(a) [5 marks] Show that $\{I, P_{132}, P_{123}, P_{23}, P_{13}, P_{12}\}$ is a subgroup of $O(3,\mathbb{R})$ isomorphic to S_3.

Proof: let $P = \{I, P_{132}, P_{123}, P_{23}, P_{13}, P_{12}\}$. All we need to show is that P is a non-Abelian group, since we proved in class that there are only two possible groups of order 6, namely $\mathbb{Z}_6$ and D_3. Then D_3 must be isomorphic to S_3, since they are both non-Abelian groups of order 6. The easiest way to prove P is a group, and the most useful way in terms of what is to come, is to write out it's Cayley table, or multiplication table:

	I	P_{132}	P_{123}	P_{23}	P_{13}	P_{12}
I	I	P_{132}	P_{123}	P_{23}	P_{13}	P_{12}
P_{132}	P_{132}	P_{123}	I	P_{13}	P_{12}	P_{23}
P_{123}	P_{123}	I	P_{132}	P_{12}	P_{23}	P_{13}
P_{23}	P_{23}	P_{12}	P_{13}	I	P_{123}	P_{132}
P_{13}	P_{13}	P_{23}	P_{12}	P_{132}	I	P_{123}
P_{12}	P_{12}	P_{13}	P_{23}	P_{123}	P_{132}	I

Alternate Solution: observe that the effect of left-multiplying I by the matrix P_σ is to permute the rows of I, one matrix for each possible permutation of the three rows. So $\sigma \mapsto P_\sigma$ defines an isomorphism from S_3 to P.

(b) [6 marks] Let H be the set of all invertible matrices of the form

$$aI + cP_{132} + bP_{123} = \begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix},\ \text{with } a, b, c \in \mathbb{R}.$$

Show that H is a subgroup of $GL(3,\mathbb{R})$.

Proof: H is obviously non-empty so we need only check closure under multiplication and inverses. Let $A = aI + cP_{132} + bP_{123}$ and $B = xI + yP_{132} + zP_{123}$ be two matrices in H. Then

$$AB = (aI + cP_{132} + bP_{123})(xI + yP_{132} + zP_{123})$$

$$= (ax + by + cz)I + (ay + bz + cx)P_{132} + (az + bx + cy)P_{123} \in H.$$

Checking that H is closed under inverses is a little trickier. If you use the adjoint formula for A^{-1} you find

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} a^2 - bc & b^2 - ac & c^2 - ab \\ c^2 - ab & a^2 - bc & b^2 - ac \\ b^2 - ac & c^2 - ab & a^2 - bc \end{bmatrix} \in H.$$

(c) [2 marks] Let K be the set of all invertible matrices of the form

$$aP_{23} + bP_{12} + cP_{13} = \begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix}, \text{ with } a, b, c \in \mathbb{R}.$$

Show that if $A \in K$ then $A^{-1} \in K$.

Proof: similar calculation to (b). Let $A = aP_{23} + bP_{12} + cP_{13}$. Then

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} cb - a^2 & ac - b^2 & ab - c^2 \\ ac - b^2 & ab - c^2 & cb - a^2 \\ ab - c^2 & cb - a^2 & ac - b^2 \end{bmatrix} \in K.$$

(d) [4 marks] Show that

(i) if $A, B \in K$ then $AB \in H$.

Proof: let $A = aP_{23} + bP_{12} + cP_{13}$ and $B = xP_{23} + yP_{12} + zP_{13}$ be matrices in K. Then

$$AB = (aP_{23} + bP_{12} + cP_{13})(xP_{23} + yP_{12} + zP_{13})$$

$$= (ax + by + cz)I + (ay + bz + cx)P_{132} + (az + bx + cy)P_{123} \in H.$$

(ii) if $A \in H$ and $B \in K$ then both AB and BA are in K.

Proof: let $A = aI + cP_{132} + bP_{123}$ be in H, let $B = xP_{23} + yP_{12} + zP_{13}$ be in K. Then

$$AB = (aI + cP_{132} + bP_{123})(xP_{23} + yP_{12} + zP_{13})$$

$$= (ax + bz + cy)P_{23} + (ay + bx + cz)P_{12} + (az + by + cx)P_{13} \in K.$$

A similar calculation shows that $BA \in K$ as well.

(e) [3 marks] Let $G = H \cup K$. Show that G is a subgroup of $GL(3, \mathbb{R})$.

Proof: note that if $A \in H \cap K$ then A is of the form

$$A = \begin{bmatrix} a & a & a \\ a & a & a \\ a & a & a \end{bmatrix},$$

which is not invertible. Thus $H \cap K = \emptyset$. Therfore to show G is closed under multiplication we only have to consider products of the four types

1. A_1A_2 with $A_1, A_2 \in H$
2. B_1B_2 with $B_1, B_2 \in K$
3. A_1B_1 with $A_1 \in H, B_1 \in K$
4. B_1A_1 with $A_1 \in H, B_1 \in K$

By part (b), products of type 1 are in H; by part (d)(i), products of type 2 are in H; and by part (d)(ii), products of type 3 and 4 are in K. Thus G is closed under multiplication.

Finally, if $A \in G$ then it is in H or K. And by parts (b) and (c), $A^{-1} \in H$ or K, respectively. So $A^{-1} \in G$. Thus G is a subgroup of $GL(3, \mathbb{R})$.

(f) [4 marks] Let $A \in G$. Find conditions on a, b, c such that A is orthogonal.

Proof: observe that for any $A \in G$ the vector

$$\vec{v} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

is an eigenvector of A with corresponding eigenvalue $\lambda = a + b + c$. If A is orthogonal then $\lambda = \pm 1$ and the columns of A form an orthonormal basis for $\mathbb{R}^3$. In particular each column of A must be a unit vector. Thus we require

$$a + b + c = \pm 1 \text{ and } a^2 + b^2 + c^2 = 1.$$

Observe that

$$(a + b + c)^2 = 1 \text{ and } a^2 + b^2 + c^2 = 1 \text{ together imply } 2ab + 2ac + 2bc = 0,$$

and so the columns of A form an orthogonormal set! Thus $A \in G$ is orthogonal if and only if

$$a + b + c = \pm 1 \text{ and } a^2 + b^2 + c^2 = 1.$$

4. Let G be the set of all 2×2 invertible matrices, with entries in $\mathbb{Z}$.

(a) [2 marks] Is G together with matrix multiplication a group? If not, why not?

Solution: No. G is not closed under inverses. For example,

$$A = \begin{bmatrix} 1 & 5 \\ 2 & 3 \end{bmatrix} \in G \text{ but } A^{-1} = \frac{1}{7}\begin{bmatrix} -3 & 5 \\ 2 & -1 \end{bmatrix} \text{ is not in } G.$$

(b) [5 marks] Prove that if both A and A^{-1} are in G then $\det(A) = \pm 1$.

Proof: let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be in G, for which

$$A^{-1} = \frac{1}{\det(A)}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

If $A^{-1} \in G$, then $\det(A)$ must divide all of a, b, c, d. Suppose p is a prime such that p^k divides $\det(A)$ but p^{k+1} doesn't. Then p^k divides all of a, b, c, d but p^{k+1} does not. Then there are integers a', b', c', d' such that

$$A = \begin{bmatrix} p^k a' & p^k b' \\ p^k c' & p^k d' \end{bmatrix}$$

and

$$A^{-1} = \frac{1}{p^{2k}\det(a'd' - b'c')}\begin{bmatrix} p^k d' & -p^k b' \\ -p^k c' & p^k a' \end{bmatrix} = \frac{1}{p^k \det(a'd' - b'c')}\begin{bmatrix} d' & -b' \\ -c' & a' \end{bmatrix}.$$

But p does not divide at least one of a', b', c' or d', so the matrix A^{-1} is not in G. Thus there is no prime p that divides $\det(A)$, which means $\det(A) = \pm 1$.

(c) [3 marks] Explain why $H = \{A \in G \mid \det(A) = \pm 1\}$, together with matrix multiplication, is a group.

Solution: H contains the identity matrix I, since $\det(I) = 1$. H is closed under multiplication: if $A, B \in H$ then $\det(A) = \pm 1, \det(B) = \pm 1$, so

$$\det(AB) = \det(A)\det(B) = \pm 1$$

as well. By part (b), H is closed under inverses. Finally, matrix multiplication is always associative. Conclusion: H is a group.

(d) [2 marks] Prove that $K = \{A \in H \mid \det(A) = 1\}$ is a normal subgroup of H. To which group is H/K isomorphic?

Proof: consider the homomorphism $\det : H \longrightarrow \{1, -1\}$, with operation multiplication. Then $K = \ker(\det)$ and thus $K \lhd H$. By the First Isomorphism Theorem,

$$H/K \approx \operatorname{im}(\det) = \{1, -1\} \approx \mathbb{Z}_2.$$

(e) [4 marks] Find the order of each of the following matrices in H :

$$A = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, D = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix},$$
$$X = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, Z = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}.$$

Solution: A, B, C, D have order 2, since

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; B^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix};$$

$$C^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; D^2 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

X, Y, Z have order 4, 3 and 6, respectively:

$$X^4 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix};$$

$$Y^3 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix};$$

$$Z^6 = \left(\begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}^2\right)^3 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

(f) [8 marks] It is known that all the non-trivial finite subgroups of H are isomorphic to

$$\mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_6, D_3, D_4 \text{ or } D_6.$$

Find examples of subgroups in H for each of these eight possibilities.

Solution: from part (e) we know $|A| = |B| = |C| = |D| = 2, |X| = 4, |Y| = 3$ and $|Z| = 6$.

For the cyclic groups:

1. $\mathbb{Z}_2 \approx \langle A \rangle$ or $\langle B \rangle$ or $\langle C \rangle$ or $\langle D \rangle$.
2. $\mathbb{Z}_3 \approx \langle Y \rangle$.
3. $\mathbb{Z}_4 \approx \langle X \rangle$.
4. $\mathbb{Z}_6 \approx \langle Z \rangle$.

As for the Dihedral groups:

1. D_2 aka $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \approx \{I, C, D, -I\}$, since $D = -C$ and $CD = DC = -I$.
2. $D_3 \approx \langle Y, C \rangle$, since $Y^3 = C^2 = I$ and $CYC = Y^2$.
3. $D_4 \approx \langle X, B \rangle$, since $X^4 = B^2 = I$ and $BXB = X^3$.
4. $D_6 \approx \langle Z, C \rangle$, since $Z^6 = C^2 = I$ and $CZC = Z^5$.