Main Examination period 2024 – January – Semester A

MTH6106: Group Theory

Duration: 2 hours

The exam is intended to be completed within **2 hours**. However, you will have a period of **4 hours** to complete the exam and submit your solutions.

You should attempt ALL questions. Marks available are shown next to the questions.

All work should be **handwritten** and should **include your student number**. Only one attempt is allowed – **once you have submitted your work, it is final**.

In completing this assessment:

- You may use books and notes.
- You may use calculators and computers, but you must show your working for any calculations you do.
- You may use the Internet as a resource, but not to ask for the solution to an exam question or to copy any solution you find.
- You must not seek or obtain help from anyone else.

When you have finished:

- scan your work, convert it to a **single PDF file**, and submit this file using the tool below the link to the exam;
- e-mail a copy to **maths@qmul.ac.uk** with your student number and the module code in the subject line;

Examiners: I.D. Morris, F. Rincón

Question 1 [25 marks].

(a) For the following, either give an example or explain why no example can exist:

(i) A group with at least four elements in which every element has order either 1 or 2. [**2**]

[Seen similar.] The Klein group $\mathcal{V}_4 \simeq \mathcal{C}_2 \times \mathcal{C}_2$ is the example most likely to be familiar to students.

(ii) A group with at least four elements in which every element has order either 1 or 4. [**2**]

[Unseen.] If G is such a group, and $g \in G$ is an element of order 4, then g^2 has order 2, so this is impossible.

(iii) Two groups of order 24 which are not isomorphic to one another. [**2**]

[Seen similar.] An easy example is $\mathcal{S}_4$ and $\mathcal{C}_{24}$, which are not isomorphic because the latter is abelian and the former is not.

(iv) Two countably infinite groups which are not isomorphic to each other. [**2**]

[Unseen.] The additive group of rationals and the multiplicative group of nonzero rationals are both examples. (One has an element of order 2 and the other does not.) Alternatives could include $\mathbb{Z}$ and $\mathbb{Q}$, since the former is finitely generated and the latter is not.

(b) Let $G = \{x \in \mathbb{R} \colon x \geq 0\}$ and define a binary operation $\circ$ on G by $x \circ y := |x - y|$. Decide which of the four group axioms is satisfied by $(G, \circ)$ and which is not. For each axiom, give a brief justification for your answer. [**5**]

[Unseen.] This clearly satisfies the closure axiom (students might call this “G1”) since if x and y are non-negative reals then so is $|x - y|$. (1 mark.) It does **not** satisfy associativity (“G2”) since for example $||2-1|-1| = 0 \neq 2 = |2 - |1-1||$. (2 marks.) The identity axiom G3 is satisfied since $|x - 0| = |0 - x| = |x| = x$ for every $x \in G$ (1 mark) and the inverse axiom G4 is satisfied since $|x - x| = 0$ for every $x \in G$ (1 mark).

(c) Using Lagrange's theorem, or otherwise, show that if g is an element of a group G such that $|G| = n$, then g^n is the identity element of G. [**3**]

[Unseen.] The order of g equals the order of the the group generated by g, which must divide n by Lagrange's theorem, so $g^k = 1$ for some k which divides g. Hence $g^{k(n/k)} = 1$ as needed. (3 marks)

(d) Using the result of (c) above, show that if p is a prime number and n is an integer in the range $1 \leq n \leq p$, then $n^{p-1} \equiv 1 \mod p$. (Hint: consider the group $\mathcal{U}_p$.) [**3**]

[Unseen.] Since p is prime, n is coprime to p, hence is an element of $\mathcal{U}_p$ (1 mark). The number of elements in $\mathcal{U}_p$ is $p - 1$ (1 mark) so we have $n^{p-1} \equiv 1$ by the previous result (1 mark).

(e) List all subgroups of the dihedral group $\mathcal{D}_{10}$ and indicate briefly why your list is complete. [**6**]

[Unseen.] Subgroups must have order 1, 2, 5 or 10, and the subgroups with these respective orders are: $\{1\}$; $\langle s\rangle = \{1, s\}$, $\langle rs\rangle = \{1, rs\}$, $\langle r^2s\rangle = \{1, r^2s\}$, $\langle r^3s\rangle = \{1, r^3s\}$ and $\langle r^4s\rangle = \{1, r^4s\}$, $\langle r\rangle = \{1, r, r^2, r^3, r^4\}$; and $\mathcal{D}_{10}$. (4 marks for complete list). To see that this list is complete, note that any group containing both a reflection r^is and a rotation r^j must include the identity, all four nontrivial rotations, and a reflection, hence has order at least six, hence has order ten by Lagrange's theorem (2 marks any correct justification).

 Continue to next page

Question 2 [25 marks].

(a) Consider the two permutations $f, g \in S_5$ given by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}.$$

(i) Write each of f, g, and fg in disjoint cycle notation. **[5]**

We have $f = (14325)$ and $g = (13)(25)$ (1 mark each), and $fg = (12)(34)$ (3 marks).

(ii) State the **order** of each of f, g, and fg. Briefly justify your answer with reference to a result from the course. **[3]**

The orders are respectively 5, 2, 2, and students should be aware that the order of a permutation is the least common multiple of the lengths of its component (disjoint) cycles. (3 marks)

(iii) State the **cycle type** of each of f, g and fg. **[3]**

The cycle types are respectively (5), $(2, 2, 1)$, $(2, 2, 1)$ (1 mark each).

(iv) Which of f, g and fg are **conjugate** to one another? Briefly justify your answer with reference to a result from the course. **[3]**

g and fg are conjugate to one another because they have the same cycle type, but no others are conjugate. Students should be aware that cycle type is a complete invariant for conjugacy in S_n.

(v) Which of f, g and fg are elements of the **alternating group** A_5? Briefly justify your answer with reference to a result from the course. **[3]**

All three belong to A_5 since a permutation (written in disjoint cycle notation) belongs to the alternating group iff it has an even number of cycles of even length (and any number of odd cycles). (1 mark each)

(b) (i) Consider the element r^3 of the dihedral group $\mathcal{D}_{10}$. Find the **centraliser** of r^3 in $\mathcal{D}_{10}$. **[3]**

All rotations commute with r^3 so the centraliser contains all five rotations (including the identity). It follows by Lagrange's theorem that the centraliser either consists only of rotations, or consists of all elements of $\mathcal{D}_{10}$. Since $r^3 s = sr^{-3} = sr^2 \neq sr^3$, r^3 does not commute with s, so the centraliser is not the whole of $\mathcal{D}_{10}$ and therefore must be $\{1, r, r^2, r^3, r^4\}$. (3 marks any valid argument).

(ii) Now instead consider the element r^3 of the dihedral group $\mathcal{D}_{12}$. Find the **centraliser** of r^3 in $\mathcal{D}_{12}$. **[3]**

All rotations commute with r^3, so the centraliser has cardinality at least six. Since in this group $r^3 s = sr^{-3} = sr^3$, r^3 commutes with s and therefore commutes with all elements of $\mathcal{D}_{12}$. (3 marks any valid argument)

(iii) Write down the **centre** of the group $\mathcal{D}_{10}$. **[2]**

All rotations (except the identity) fail to commute with s, so the centraliser is just $\{1\}$. (2 marks)

Question 3 [25 marks].

(a) Give an example of a group G and subgroup $H \leq G$ such that H is **not** normal in G. [**2**]

The simplest example is any 2-element subgroup of S_3. (2 marks.)

(b) Show that:

(i) If N is a normal subgroup of an abelian group G, then G/N is also abelian. [**3**]
We have $(g_1N)(g_2N) = (g_1g_2)N = (g_2g_1)N = (g_2N)(g_1N)$ using (in the middle step) the fact that G is abelian. (3 marks)

(ii) If $\phi\colon G \to H$ is a group homomorphism and G is abelian, then $\operatorname{im}\phi$ is abelian. [**3**]
This can be argued directly using surjectivity; or, by the first isomorphism theorem, the image is isomorphic to $G/\ker\phi$ which is abelian by the result of the previous question (3 marks).

(c) Using the Third Isomorphism Theorem, or otherwise, prove that if H_1 and H_2 are subgroups of an abelian group G, then

$$|H_1H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}.$$

Indicate clearly in your answer where, and how, you make use of the fact that G is abelian.

Since G is abelian, both H_1 and H_2 are normal in G, so the third isomorphism theorem is applicable (1 and a half marks). By the third isomorphism theorem $(H_1H_2)/H_2 \simeq H_1/(H_1 \cap H_2)$, so in particular $|H_1H_2|/|H_2| = |H_1|/|H_1 \cap H_2|$ and the result follows by rearrangement (2 and a half marks).

[**4**]

(d) Define

$$G := \mathcal{U}_{56,}, \qquad H_1 := \{1, 5, 9, 13, 25, 45\}, \qquad H_2 := \{1, 3, 9, 19, 25, 17\}.$$

Calculate $|H_1H_2|$. [**4**]

Using the previous result, since $|H_1| = 6$ and $|H_2| = 6$ and $|H_1 \cap H_2| = 3$, we have $|H_1H_2| = 36/3 = 12$ (4 marks any correct argument).

(e) Let $\mathbb{F}_4$ denote the field with four elements, let $\mathbb{F}_4^2$ denote the set of all two-dimensional vectors with entries in $\mathbb{F}_4$, and recall that $\mathrm{GL}_2(\mathbb{F}_4)$ denotes the group of invertible 2×2 matrices with entries in $\mathbb{F}_4$. In this question we consider the action π of $\mathrm{GL}_2(\mathbb{F}_4)$ on $\mathbb{F}_4^2$ defined by $\pi(A, v) := Av$.

(i) How many elements of $\mathrm{GL}_2(\mathbb{F}_4)$ belong to the stabiliser of the vector $\binom{1}{0}$? [**3**]
Every matrix whose upper-left entry is 1 and whose lower left entry is 0 fixes this vector, and such a matrix is invertible iff if the lower-right entry is nonzero, so there are 12 such matrices (4 options for the upper right entry, 3 for the lower-right, 0 options for other entries). (3 marks)

(ii) How many vectors belong to the orbit of the vector $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$? **[3]**

All nonzero vectors belong to this orbit. To see this form the matrix which has the desired vector as its first column, and fill in the second column with any vector which is not a scalar multiple of the first vector. So 15 vectors total. (3 marks)

(iii) Using an appropriate result from the course, calculate the order of $\mathrm{GL}_2(\mathbb{F}_4)$. **[3]**

By the orbit-stabiliser theorem this equals the cardinality of the orbit of the vector defined above, multiplied by the cardinality of its stabiliser, so 12×15, i.e. 180. (3 marks)

Question 4 [25 marks].

(a) Suppose that G is a group of order 117. Prove that G cannot be simple. State carefully any additional results from the course which you require in your answer. [**5**]

If G is a group of order $p^a q$ where p is prime, q is coprime to p, and $a \geq 1$, write $n_p(G)$ for the number of subgroups of G with order p^a. Then $n_p(G)|q$ and $n_p(G) \equiv 1 \mod p$. (2 marks for stating this; it's in the notes, but students should still explain clearly what they're doing here.) Since $117 = 9 \times 13$, $n_3(G)$ is congruent to 1 mod 3 and divides 13, hence must be 1. So G has a unique subgroup of order 9. This subgroup must be normal since all subgroups conjugate to it also have order 9 and hence are equal to it. So G has a nontrivial normal subgroup and is not simple. (3 marks any correct argument)

(b) Suppose that G is a group of order 168, and let n_7 denote the number of Sylow 7-subgroups of G. List all possible values that n_7 could take which are consistent with Sylow's theorems. Is it possible to decide, using this list of values, whether or not G is simple? Why, or why not? [**4**]

We have $n_7(G) \equiv 1 \mod 7$ and $n_7(G)|24$ by the previous argument, so n_7 could be either 1 or 8. This does not preclude the possibility that G is simple, because it might in principle have 8 subgroups of order 7 and be simple.

(c) Without proof, write down:

(i) A composition series for the group $\mathcal{C}_{27}$. [**2**]
$1 \lhd \mathcal{C}_3 \lhd \mathcal{C}_9 \lhd \mathcal{C}_{27}$ is the only valid answer.

(ii) A composition series for the group $\mathcal{D}_{12}$. [**2**]
$1 \lhd \{1, r, r^2, \ldots, r^5\} \lhd \mathcal{D}_{12}$ and $1 \lhd \{1, s\} \lhd \mathcal{D}_{12}$ are valid answers. These could be written respectively as $1 \lhd \mathcal{C}_6 \lhd \mathcal{D}_{12}$ and $1 \lhd \mathcal{C}_2 \lhd \mathcal{D}_{12}$.

(iii) A composition series for the group $\mathcal{S}_4$. [**3**]
The only correct answer is $1 \lhd \mathcal{C}_2 \lhd \mathcal{V}_4 \lhd \mathcal{A}_4 \lhd \mathcal{S}_4$. The group $\mathcal{V}_4$ could alternatively be written as $\mathcal{C}_2 \times \mathcal{C}_2$ or as $\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$.

(iv) A composition series for one of the three groups listed in (i)–(iii) above which is **different** to the composition series which you stated in your earlier answer. [**2**]
As noted above there are two distinct options for (ii) and the student should give whichever of these was not given previously.

(v) Show that if a group is abelian then all of its inner automorphisms are trivial. [**2**]
An inner automorphism $\phi \colon G \to G$ is an automorphism of the form $\phi(g) = hgh^{-1}$ for some $h \in G$, so $\phi(g) = hgh^{-1} = hh^{-1}g = 1g = g$ when G is abelian. (3 marks)

(vi) Let p be a prime number and let G be the group of integers $\{0, 1, \ldots, p-1\}$ equipped with the binary operation of addition modulo p. By considering the effect of each automorphism on the element 1, show that the outer automorphism group of G has exactly $p-1$ elements. [**5**]

For every $k = 1, 2, \ldots, p-1$ we may define a homomorphism $\phi_k \colon G \to G$ by $\phi_k(n) = kn \mod p$. Since $\mathcal{U}_p$ is a group with respect to multiplication modulo p, every such homomorphism ϕ_k has an inverse $\phi_{k^{-1}}$, so all such homomorphisms are automorphisms and the number of automorphisms of G is at least $p-1$. (2 marks any correct argument). On the other hand if two automorphisms ϕ, ψ take the same value at $1 \in G$ then they must be identical, so the number of automorphisms of G is also at **most** $p-1$. (2 marks.) Since by the previous question the inner automorphism group is trivial, the outer automorphism group has cardinality exactly $p-1$. (1 mark)

End of Paper.