Queen Mary University of London

Main Examination period 2022 – January – Semester A

MTH6106: Group Theory

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

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.**

All work should be **handwritten** and should **include your student number**.

The exam is available for a period of **24 hours**. Upon accessing the exam, you will have **3 hours** in which to complete and submit this assessment.

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;
- with your e-mail, include a photograph of the first page of your work together with either yourself or your student ID card.

Please try to upload your work well before the end of the submission window, in case you experience computer problems. **Only one attempt is allowed – once you have submitted your work, it is final**.

Examiners: I.Morris, R. Johnson

Question 1 [25 marks].

(a) Give examples of:

(i) A group of order 24 which is not abelian. **[2]**

Solution. (Unseen) Probably the easiest answer is the dihedral group $D_{24} = \{1, r, r^2, \ldots, r^{11}, s, sr, \ldots, sr^{11}\}$ which is the group of symmetries of a regular dodecagon. Another option is S_4.

(ii) A group of infinite order which is not abelian. **[2]**

Solution. (Unseen) The general linear group of dimension 2 over $\mathbb{R}$, or any of a large range of matrix groups, or the group of bijections from a particular infinite set to itself, or the infinite dihedral group D_∞, all work here.

(iii) A pair of abelian groups of the same order which are not isomorphic to one another. (You do not need to give a proof that the two groups are not isomorphic.) **[2]**

Solution. (Unseen) Probably the easiest example is the cyclic group of order 4 and the Klein 4-group.

(iv) A group G and a two subgroups $H_1, H_2 \leq G$ such that $H_1 \cup H_2$ is not a subgroup of G. **[3]**

Solution. (Unseen) Let G be any group which has two distinct elements of order 2 and let H_1, H_2 be the subgroups generated by those two elements. Then $H_1 \cup H_2$ contains three elements but cannot be a subgroup because it has cardinality 3 but contains an element of order 2, which contradicts Lagrange's theorem.

A more concrete example would be the Klein 4-group $\langle a, b, c | ab = c,\ a^2 = b^2 = c^2 = 1\rangle$ with $H_1 = \{1, a\}$ and $H_2 = \{1, b\}$.

(b) Complete the following table in a way which results in the Cayley table of a group.

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	1
b					
c					
d					

[5]

Solution. (Seen similar) The only solution is

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	1
b	b	c	d	1	a
c	c	d	1	a	b
d	d	1	a	b	c

.

(c) The following table is **not** the Cayley table of a group. Indicate which group axioms are inconsistent with this table. For each group axiom which is inconsistent with the table, give an example of where in the table the inconsistency occurs.

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	d	1	c
b	b	1	c	d	a
c	c	d	a	b	1
d	d	c	1	a	b

[5]

Solution. (Seen similar) The axiom of inverses is violated, because while every element has a left inverse and a right inverse, the left and right inverses are not equal. So for example $ac = 1$ but $ca = d \neq 1$, contradicting the inverse axiom. (2 marks). Associativity is also violated because for example $(aa)a = ba = 1$ but $a(aa) = ab = d$. (3 marks.) In this question 2 marks are available for identifying which axioms are violated and 3 marks are available for the reasoning.

Recall that $\mathrm{GL}_n(\mathbb{R})$ denotes the group of invertible $n \times n$ matrices with real entries. Let $\mathrm{O}(n)$ denote the set

$$\mathrm{O}(n) := \left\{A \in \mathrm{GL}_n(\mathbb{R})\colon A^T A = I\right\}$$

where I denotes the $n \times n$ identity matrix and A^T denotes the transpose of the matrix A. Show that $\mathrm{O}(n)$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. [6]

Solution. (Unseen) Using the subgroup test, we would need to show that $\mathrm{O}(n)$ is nonempty and that for every $A, B \in \mathrm{O}(n)$ the product $A^{-1}B$ is an element of $\mathrm{O}(n)$. (Or, we could show that AB^{-1} is an element of $\mathrm{O}(n)$: either is fine if used consistently.) To see that $\mathrm{O}(n)$ is nonempty we notice that it contains the identity. (2 marks). If $A, B \in \mathrm{O}(n)$ then $(AB^{-1})^T AB^{-1} = (B^{-1})^T A^T AB^{-1} = (B^{-1})^T B^{-1} = (BB^T)^{-1}$. But if $B \in \mathrm{O}(n)$ then $B^T = B^{-1}$ (2 marks for this observation in some form) so BB^T is the identity and therefore this expression is the identity as required. (2 marks).
Note that there are 2 marks for explaining why the identity $BB^T = I$ is true, since it is not immediately obvious a priori.

Question 2 [25 marks].

(a) Let G be a group and let $f, g \in G$. Suppose that f and g have finite order and that $fg = gf$. Show that the order of fg is **less than or equal to** the least common multiple of the orders of f and g. [3]

Solution. (Seen similar.) Let n be the least common multiple of the order of f and the order of g, so that $n = k\,\mathrm{ord}(f) = \ell\,\mathrm{ord}(g)$, say. We have $(fg)^n = f^n g^n = (f^{\mathrm{ord}(f)})^k (g^{\mathrm{ord}(g)})^\ell = 1$, which implies that the order of fg is not greater than n. (3 marks.)

(b) Give an example of two permutations $f, g \in S_3$ such that the order of $\mathrm{ord}(fg)$ is **not equal to** the least common multiple of the orders of f and g. **[3]**

Solution. (Unseen.) There are various options: if $f = g^{-1}$ then $\mathrm{ord}(fg) = 1$, so we could take $f = g = (12)$, say, or $f = (123)$ and $g = (132)$. Alternatively we could take f and g non-commuting with orders 2 and 3, and then the least common multiple of the orders would be 6, but there are no elements of order 6 in S_3.

(c) Consider the permutations $f, g \in S_8$ given by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 4 & 3 & 1 & 8 & 7 & 2 \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 8 & 1 & 4 & 7 & 5 & 2 & 6 \end{pmatrix}$$

Write f, g and fg in disjoint cycle notation and state the order of each of f, g and fg. **[9]**

Solution. (Seen similar.) We have $f = (15)(34)(268)$ and $g = (13)(28657)$ and $fg = (143576)$ (for 1.5, 1.5 and 3 marks respectively) so the orders of f, g and fg are 6, 10 and 6 respectively (1 mark each).

(d) Let $n \geq 3$ and consider the group S_n.

(i) Show that every element of S_n can be written as a product of transpositions. **[2]**

Solution. (Bookwork.) Every element of S_n can be written as a product of disjoint cycles $(a_{11}a_{12}\cdots a_{1n_1})(a_{21}a_{22}\cdots a_{2n_2})\cdots a_{r1}\cdots a_{rn_r})$. Every cycle $(a_1 \cdots a_n)$ can be written as the product of transpositions $(a_1a_2)(a_2a_3)\cdots(a_{n-1}a_n)$. Combining these two facts yields the result. (2 marks).

(ii) Let $(1k), (1\ell) \in S_n$ be transpositions, where $2 \leq k, \ell \leq n$ and $k \neq \ell$. Write down the permutation $(1k)(1\ell)(1k)$ in disjoint cycle notation. **[2]**

Solution. (Seen similar.) The answer is $(k\ell)$.

(iii) Suppose that H is a subgroup of S_n which contains every transposition of the form $(1k)$, where $2 \leq k \leq n$. Explain why H must be equal to S_n. **[2]**

Solution. (Unseen.) If $(k\ell)$ is an arbitrary transposition with $1 \leq k < \ell \leq n$ then $(k\ell) \in H$ by definition if $k = 1$, and $(k\ell) = (1k)(1\ell)(1k) \in H$ otherwise.

(iv) Suppose that H is a subgroup of S_n which contains the permutation (12) and also contains the permutation $(2345\cdots n)$. Show that H contains every permutation of the form $(1k)$ where $2 \leq k \leq n$. **[3]**

Solution. (Seen similar.) We have $(2345\cdots n)^{k-1}(12)(2345\cdots n)^{-(k-1)} = (1k)$ for every $k = 2, \ldots, n$. (Students should already be familiar with how to conjugate cycles, but have not seen this specific application of the calculation.)

(v) What is the group $\langle (12), (2345\cdots n) \rangle$? **[1]**

Solution. (Unseen.) This group is S_n, because by (iv) this group contains every permutation of the form $(1k)$ and by (iii) a group with this property must be S_n.

Question 3 [25 marks].

(a) Suppose that G and H are finite groups and that $\phi\colon G \to H$ is a homomorphism.

(i) What information does Lagrange's theorem give you about the relationship between $|G|$, $|G/\ker\phi|$ and $|\ker\phi|$? **[2]**

Solution. (Unseen.) The cardinality of $|G/\ker\phi|$ is the number of cosets of $\ker\phi$ in G, which is $|G : \ker\phi|$, so by Lagrange's theorem $|G| = |G/\ker\phi| \cdot |\ker\phi|$.

(ii) What information does the First Isomorphism Theorem give you about the relationship between $|G/\ker\phi|$ and $|\operatorname{im}\phi|$? **[2]**

Solution. (Unseen.) The first isomorphism theorem implies that $|G/\ker\phi|$ must equal $|\operatorname{im}\phi|$ since the two groups in question are isomorphic.

(iii) Indicate why $|\operatorname{im}\phi|$ divides both $|G|$ and $|H|$. **[3]**

Solution. (Unseen.) The previous two answers combine to give $|G| = |\operatorname{im}\phi| \cdot |\ker\phi|$, and since $\operatorname{im}\phi \leq H$ we have $|\operatorname{im}\phi|\,\big|\,|H|$ by Lagrange's theorem.

(iv) Suppose that the numbers $|G|$ and $|H|$ are coprime. Prove that $\phi(g) = 1_H$ for all $g \in G$. **[2]**

Solution. (Unseen.) By the previous answer, $|\operatorname{im}\phi|$ must divide both $|G|$ and $|H|$, so if those two numbers are coprime then $|\operatorname{im}\phi|$ must equal 1. Since necessarily $1_H = \phi(1_G) \in \operatorname{im}\phi$ the result follows.

(b) Let G be a finite group and let $H \leq G$. Show that for every $g \in G$, the set $gHg^{-1} = \{ghg^{-1}\colon h \in H\}$ is a subgroup of G. Now explain briefly why the following result holds: if H is the only subgroup of G with cardinality $|H|$, then H must be normal in G. **[5]**

Solution. (Bookwork.) Fix $g \in G$. To show that gHg^{-1} is a subgroup of G it's sufficient to show that it is nonempty, and that for every $f_1, f_2 \in gHg^{-1}$ we have $f_1f_2^{-1} \in gHg^{-1}$. To see the former we just note that $1 = g1g^{-1} \in gHg^{-1}$. To see the latter, let $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$. We have $(gh_2g^{-1})^{-1} = gh_2^{-1}g^{-1}$ so $gh_1g^{-1}(gh_2g^{-1})^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}$, using the fact that $h_1h_2^{-1} \in H$. (3 and a half marks any correct argument.) If H is the unique subgroup of G with cardinality $|H|$, then for every $g \in G$, gHg^{-1} is a subgroup of G with cardinality $|H|$ and therefore must equal H. This implies that H is normal by the definition of normality. (one and a half marks for correct reasoning along these lines: the equation $|H| = |gHg^{-1}|$ need not be proved.)

(c) Using Sylow's theorems, show that there is no simple group of order 51. **[5]**

Solution. (Seen similar.) Let G be a group of order 51. By Sylow's third theorem, the number of subgroups of G with order 17 divides 3, and also is congruent to 1 modulo 17. The only non-negative integer with these properties is 1, so there is a unique subgroup of G with order 17. By the result of the previous question this subgroup is normal in G, so G is not simple.

(d) Using Sylow's theorems, or otherwise, show that A_5 has exactly 6 subgroups of order 5. State (without proof) any facts about A_5 which are required in your argument. [**6**]

Solution. (Unseen.) Let $n_5(A_5)$ denote the number of subgroups of A_5 which have order 5. Since $|A_5| = 60$, Sylow's third theorem implies that $n_5(A_5)$ divides 12 and also is congruent to 1 modulo 5 (three marks). The only non-negative integers with these characteristics are 1 and 6. (1 mark.) If A_5 had a unique subgroup of order 5 then that subgroup would be normal, but we know that A_5 is simple, so $n_5(A_5)$ cannot equal 1 and therefore must equal 6 (2 marks). Students will have seen a proof that A_5 is simple and are also aware that $|A_n| = n!/2$, so should be familiar with the required facts.

An alternative argument is as follows. It follows from Lagrange's theorem that a group of order 5 must consist of the identity together with four elements of order 5, so the result holds if and only if A_5 contains exactly 24 elements of order 5, which holds if and only if it contains exactly twenty-four 5-cycles (three marks for these observations). Since every 5-cycle is even (1 mark for making this observation, 1 mark for justifying it) it is enough to show that S_5 contains twenty-four 5-cycles. But the number of 5-cycles in S_5 is just the number of tuples of the form $(1abcd)$ where $a, b, c, d \in \{2, 3, 4, 5\}$ and there are $4! = 24$ such tuples (two marks any correct counting argument).

Question 4 [25 marks].

(a) Consider the group $\mathrm{GL}_2(\mathbb{C})$ of all 2×2 complex matrices equipped with the usual operation of matrix multiplication. Recall that A^* denotes the conjugate transpose of the matrix A.

(i) Suppose that $\rho\colon \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}_2(\mathbb{C})$ is an inner automorphism and let $A \in \mathrm{GL}_2(\mathbb{C})$. What is $\det(\rho(A))$? [**3**]

Solution. (Unseen, but easy). If ρ is an inner automorphism then $\rho(A) = BAB^{-1}$ for some $B \in \mathrm{GL}_2(\mathbb{C})$, so $\det \rho(A) = \det(BAB^{-1}) = \det A$. (2 marks)

(ii) Show that the function $\hat{\rho}\colon \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}_2(\mathbb{C})$ defined by $\hat{\rho}(A) = (A^*)^{-1}$ is an automorphism. [**4**]

Solution. (Seen similar.) We need to check that $\hat{\rho}$ is a bijection (for 2 marks) and that it is a homomorphism (for 2 marks). To see that it is a bijection it is sufficient to note that it is its own inverse. To see that it is a homomorphism we note that for any $A, B \in \mathrm{GL}_2(\mathbb{C})$ we have $\hat{\rho}(AB) = ((AB)^*)^{-1} = (B^*A^*)^{-1}) = (A^*)^{-1}(B^*)^{-1} = \hat{\rho}(A)\hat{\rho}(B)$ using standard rules from linear algebra.

 Continue to next page

(iii) Is the function $\hat{\rho}$ defined in (ii) is an inner automorphism? Justify your answer with a proof or a counterexample. [**2**]

Solution. (Seen similar.) If it were an inner automorphism then we would have $\hat{\rho}(A) \equiv \det A$, but this is clearly not true as can be seen by, for example, taking A to be a diagonal matrix with entries 1 and 2.

(b) Recall that $\mathcal{D}_{10} = \{1, r, \ldots, r^4, s, sr, \ldots, sr^4\}$ is the group of symmetries of a regular pentagon. Let X_5 denote the set of all possible colourings of the vertices of a regular pentagon using two colours, and let us say that two colourings are **equivalent** if one of them can be transformed into the other by applying a symmetry of the polygon.

(i) How many elements does X_5 have? [**1**]

Solution. (Seen similar) There are $2^5 = 32$ elements.

(ii) Suppose that $sr^k \in \mathcal{D}_{10}$ is a reflection, where $0 \leq k < 5$. How many elements of X_5 are stabilised by sr^k? [**3**]

Solution. (Seen similar) There are 8 elements stabilised by any given reflection, since we may freely choose the vertex which lies on the line of reflection and can freely choose exactly two other vertices. So we have three free choices and get 2^3 options.

(iii) Suppose that $r^k \in \mathcal{D}_{10}$ is a rotation, where $0 < k < 5$. How many elements of X_5 are stabilised by r^k? [**3**]

Solution. (Seen similar) Only constant colourings are stabilised by a nontrivial rotation so the answer is 2.

(iv) How many elements of X_5 are stabilised by $1 \in \mathcal{D}_{10}$? [**1**]

Solution. (Seen similar) All 32 elements.

(v) Using the orbit-counting lemma, find the number of equivalence classes of elements of X_5. [**3**]

Solution. (Seen similar).

By the previous results we have 1 element with stabiliser of size 32, four elements with a stabiliser of size 2, five elements with a stabiliser of size 8. So the number of equivalence classes is

$$\frac{1}{10}(1 \times 32 + 4 \times 2 + 5 \times 8) = 8.$$

(vi) Now let $p \geq 3$ be an arbitrary prime number, let $\mathcal{D}_{2p}$ denote the group of symmetries of a regular p-sided polygon, and let X_p denote the set of all colourings of a regular p-sided polygon using two colours. We say that two elements of X_p are equivalent if one of them can be transformed into the other by the application of an element of D_{2p}. By modifying the preceding argument, find the number of equivalence classes of elements of X_p. Indicate explicitly which step of your argument uses of the fact that p is prime. [**5**]

Solution. (Unseen.) We have 2^p elements in X_p. One element of $\mathcal{D}_{2p}$ has a stabiliser of size 2^p, $p-1$ elements have a stabiliser of size 2, and p elements

 Continue to next page

have a stabiliser of size $2^{(p+1)/2)}$, so we get

$$\frac{1}{2p}\left(2^p + 2(p-1) + p2^{(p+1)/2}\right).$$

for 3 marks. We needed primeness of p to guarantee that every nontrivial rotation has a stabiliser of size 2. (2 marks just for indicating that it is the rotations which require primeness.)

End of Paper.