IMPERIAL

MATH70036

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2024

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Group Theory

Date: Friday, May 3, 2024

Time: 10:00 – 12:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

Candidates should start their solutions to each question on a new sheet of paper.

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO

Throughout the paper, you may use any results from the course that you require provided you state them clearly.

1. (a) Let G be a group, and let H be a subgroup of G such that $|G : H| = n$. Prove that there is a homomorphism $\phi : G \to S_n$ (where S_n is the symmetric group of degree n) with the following properties:

   (i) $\ker(\phi) \leq H$, and

   (ii) $|\mathrm{Im}(\phi)|$ is divisible by n.

   (6 marks)

   (b) Show that if H is a subgroup of G with $|G : H| = 2$, then H is a normal subgroup of G. (3 marks)

   (c) Let G be a finite group of **odd** order, and let H be a subgroup of G with $|G : H| = 3$. Prove that H is a normal subgroup of G. (Proof required - it is not enough to quote a more general result from which this follows.) (3 marks)

   (d) Let G be a finite group of odd order, and let H be a subgroup of G with $|G : H| = 5$. Prove that H is a normal subgroup of G.

   (*Hint: you may assume the standard fact from the course that all groups of order 15 are cyclic.*) (4 marks)

   (e) Give an example of a group G of odd order that has a subgroup H such that $|G : H| = 7$ and H is not a normal subgroup of G. (4 marks)

(Total: 20 marks)

2. (a) State the four Sylow theorems. (4 marks)

(b) Using the Sylow theorems, prove the following:

(i) Any group of order 66 has a normal Sylow subgroup.

(ii) Any group of order 132 has a normal Sylow subgroup.

(6 marks)

(c) Let G be a finite group and p a prime. Prove the following statements.

(i) If H is a normal subgroup of G of order p^a for some integer a, then H is contained in every Sylow p-subgroup of G.

(ii) If H is a normal subgroup of G such that $|G : H|$ is coprime to p, then H contains every Sylow p-subgroup of G.

(iii) If P is a Sylow p-subgroup of G, and $N = N_G(P)$, then $N_G(N) = N$.

(10 marks)

(Total: 20 marks)

3. (a) Let G be a finite group. Define what is meant by the statement that G is *solvable*, and also what is meant by the statement that G is *nilpotent*. (4 marks)

(b) Let p be a prime, and let $G(p)$ be the group of all upper triangular matrices in $GL_2(p)$, i.e.

$$G(p) = \left\{ \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} : a, b \in \mathbb{F}_p \setminus 0,\ x \in \mathbb{F}_p \right\}.$$

(i) Prove that $G(p)$ is solvable.

(ii) For which values of p is $G(p)$ nilpotent? Give your reasoning. (8 marks)

(c) Let G be a finite nilpotent group, and let $x, y \in G$ be elements such that the orders of x and y are coprime (i.e. if r and s are the orders of x and y respectively, then $\gcd(r, s) = 1$). Prove that $xy = yx$. (5 marks)

(d) Give an example of a finite solvable group G which contains elements x and y of coprime orders such that $xy \neq yx$. (3 marks)

(Total: 20 marks)

4. (a) Let G be a finite group and let H be a subgroup of G. Define the *normalizer* $N_G(H)$ and the *centralizer* $C_G(H)$. Prove that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. (5 marks)

(b) Let p be a prime, and C_p a cyclic group of order p. Prove that $\mathrm{Aut}(C_p)$ is an abelian group of order $p-1$. (3 marks)

(c) State Burnside's Transfer Theorem. (2 marks)

(d) Let G be a group of order $p_1 p_2 \cdots p_k$, where $k \geq 2$, each p_i is a prime, and $p_1 < p_2 < \cdots < p_k$.

(i) Let P be a Sylow p_1-subgroup of G. Show that $N_G(P) = C_G(P)$.

(ii) Show that G has a normal subgroup of order $p_2 \cdots p_k$.

(iii) Deduce that G is solvable. (10 marks)

(Total: 20 marks)

5. **(Mastery Question)** Throughout this question, let $\mathbb{F}_q$ be a finite field of order q, and let $n \geq 2$ be an integer.

(a) Define the *general linear group* $GL_n(\mathbb{F}_q)$. (1 mark)

(b) State and prove a formula for the order of $GL_n(\mathbb{F}_q)$ in terms of n and q. (4 marks)

(c) Let $G = GL_n(\mathbb{F}_q)$, let V be the vector space $\mathbb{F}_q^n$, and let Ω be the set of 1-dimensional subspaces of V. Let G act on Ω in the natural way (i.e. $A \in G$ sends $\langle v \rangle \mapsto \langle Av \rangle$ for any $\langle v \rangle \in \Omega$).

(i) Write down an expression for $|\Omega|$ in terms of n and q. (1 mark)

(ii) Prove that this action of G on Ω is transitive. (1 mark)

(iii) Let G act on $\Omega \times \Omega$ in the natural way: $g \in G$ sends $(\omega_1, \omega_2) \mapsto (g(\omega_1), g(\omega_2))$ for $\omega_1, \omega_2 \in \Omega$. Define

$$\Delta_1 = \{(\omega, \omega) : \omega \in \Omega\}, \quad \Delta_2 = \{(\omega_1, \omega_2) : \omega_1, \omega_2 \in \Omega,\ \omega_1 \neq \omega_2\}.$$

(1) Show that Δ_1 and Δ_2 are the orbits of G on $\Omega \times \Omega$.

(2) For $\delta = (\omega_1, \omega_2) \in \Delta_2$, calculate the order of the stabilizer G_δ.

(6 marks)

(iv) Let G act on $\Omega \times \Omega \times \Omega$ in the natural way: $g \in G$ sends $(\omega_1, \omega_2, \omega_3) \mapsto (g(\omega_1), g(\omega_2), g(\omega_3))$ for $\omega_1, \omega_2, \omega_3 \in \Omega$. Define

$$\Phi = \{(\omega_1, \omega_2, \omega_3) : \omega_1, \omega_2, \omega_3 \in \Omega \text{ all distinct}\}.$$

(1) Prove that if $n \geq 3$, then G is not transitive on Φ.

(2) Prove that if $n = 2$ then G is transitive on Φ.

(7 marks)

(Total: 20 marks)

1. (a) Define $\Omega = \{xH : x \in G\}$, the set of left cosets of H, so that $|\Omega| = |G : H| = n$. For $g \in G$, define a permutation $\pi_g \in Sym(\Omega)$ by

$$\pi_g : xH \mapsto gxH \quad \text{for all } xH \in \Omega.$$

Define $\phi : G \mapsto Sym(\Omega)$ to send $g \mapsto \pi_g$ for all $g \in G$.

Then ϕ is a homomorphism, as $\pi_{g_1}\pi_{g_2}(xH) = \pi_{g_1}(g_2xH) = g_1g_2xH = \pi_{g_1g_2}(xH)$.

If $g \in \ker(\phi)$, then π_g is the identity perm of Ω, so in particular sends $H \mapsto H$. Hence $gH = H$, and so $g \in H$. Therefore $\ker(\phi) \leq H$.

Finally, $|\mathrm{Im}(\phi)| = |G : \ker(\phi)| = |G : H|\,|H : \ker(\phi)|$, which is divisible by $|G : H| = n$. (**6 marks, seen, A**)

(b) Suppose $|G : H| = 2$. Let $\phi : G \mapsto S_2$ be the homom of part (a). Note that $|S_2| = 2$, so by (a)(ii), $\mathrm{Im}(\phi) = S_2$, and so $|G : \ker(\phi)| = 2$. Hence by (a)(i), $\ker(\phi) = H$, so H is normal. (**3 marks, seen, A**)

(c) (i) Let $\phi : G \mapsto S_3$ be the homom of part (a). Then $\mathrm{Im}(\phi)$ is a subgroup of S_3 of odd order divisible by 3, so $|\mathrm{Im}(\phi)| = 3$. Hence $|G : \ker(\phi)| = 3$ and so $\ker(\phi) = H$, a normal subgroup. (**3 marks, unseen, B**)

(ii) Let $\phi : G \mapsto S_5$ be the homom of part (a). Then $\mathrm{Im}(\phi)$ is a subgroup of S_5 of odd order divisible by 5, so $|\mathrm{Im}(\phi)| = 5$ or 15. If $|\mathrm{Im}(\phi)| = 15$ then by a standard result, it is a cyclic subgroup of S_5; however S_5 has no element of order 15, so this is not possible. Hence $|\mathrm{Im}(\phi)| = 5$ and so $\ker(\phi) = H$, a normal subgroup. (**4 marks, unseen, D**)

(iii) There is a non-abelian group G_{21} of order 21 which was constructed in lectures as a semidirect product $C_7 \rtimes C_3$; it has presentation

$$G_{21} = \langle x, y : x^7 = y^3 = 1, y^{-1}xy = x^2 \rangle.$$

It has a subgroup $\langle y \rangle \cong C_3$ of index 7 which is not normal (since $xyx^{-1} = yx \notin \langle y \rangle$). (**4 marks, unseen, C**)

2. (a) The Sylow theorems:

Sylow I: Let $|G| = p^a m$, where p is prime and p does not divide m. Then G has a subgroup of order p^a.

Sylow II: If $n_p(G)$ denotes the number of Sylow p-subgroups of G, then $n_p(G) \equiv 1 \bmod p$.

Sylow III: Let Q be a p-subgroup of G. Then there exists $P \in Syl_p(G)$ such that $Q \leq P$.

Sylow IV: $Syl_p(G)$ is a single conjugacy class of subgroups of G; that is, for any $P, Q \in Syl_p(G)$, there exists $g \in G$ such that $Q = {}^gP$.

(**Bookwork, 4 marks, A**)

(b) (i) Suppose $|G| = 66 = 2 \cdot 3 \cdot 11$. By Sylow II, $n_{11}(G) \equiv 1 \bmod 11$, and by a standard result it divides $|G|$. Hence $n_{11}(G) = 1$, and so G has a normal Sylow 11-subgroup. (**Similar seen, 2 marks, A**)

(ii) Suppose $|G| = 132 = 2^2 \cdot 3 \cdot 11$, and suppose G does not have a normal Sylow subgroup. Then $n_{11}(G) \neq 1$, so by the reasoning in (i), $n_{11}(G) = 12$. Also $n_3(G) = 4$ or 22. Any two Sylow 11-subgroups intersect only in 1, so the total number of elements in G of order 11 is $N_{11} = 12 \times 10 = 120$. Similarly, the total number of elements in G of order 3 is at least $N_3 = 4 \times 2 = 8$. Hence the number of non-identity elements that can lie in Sylow 11-subgroups or Sylow 3-subgroups of G is at least $N_{11} + N_3 = 128$. As $|G|_2 = 4$, this means there can only be 1 Sylow 2-subgroup, which is hence normal in G. (**Similar seen, 4 marks, B**)

(c) (i) Let $H \lhd G$ with $|H| = p^a$. By Sylow III, there is a Sylow p-subgroup of G such that $H \leq P$. If Q is any other Sylow p-subgroup, then by Sylow IV, $Q = {}^gP$ for some $g \in G$, so ${}^gH \leq Q$. As H is normal, ${}^gH = H$, and so $H \leq Q$. (**Unseen, 3 marks, B**)

(ii) Let $H \lhd G$ with $|G : H|$ coprime to p. Let $P \in Syl_p(H)$. By the coprime condition, $P \in Syl_p(G)$ also. If $Q \in Syl_p(G)$, then $Q = {}^gP$ for some g, and so $Q \leq {}^gH = H$, as H is normal. (**Unseen, 3 marks, B**)

(iii) We have $P \in Syl_p(G)$ and $N = N_G(P)$. Obviously $P \in Syl_p(N)$.

Let $g \in N_G(N)$. Then $P^g \leq N^g = N$, so $P^g \in Syl_p(N)$. By Sylow IV, there exists $n \in N$ such that $P^g = P^n$. Then $gn^{-1} \in N_G(P) = N$, and so $g \in Nn = N$. Hence $N_G(N) = N$. (**Unseen, 4 marks, D**)

3. (a) There are quite a few correct definitions - here are the original ones in lectures:

G is solvable if there is a series of normal subgroups $1 = G_0 < G_1 < \cdots < G_r = G$ such that G_{i+1}/G_i is abelian for all i. (**Bookwork, 2 marks, A**)

G is nilpotent if there is a series of normal subgroups $1 = G_0 < G_1 < \cdots < G_r = G$ such that $G_{i+1}/G_i \leq Z(G/G_i)$ for all i. (**Bookwork, 2 marks, A**)

(b) (i) Let .

$$N(p) = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_p \right\}.$$

Then $N(p) \lhd G(p)$. Also $N(p) \cong (\mathbb{F}_p, +)$ and $G(p)/N(p) \cong (\mathbb{F}_p^\times)^2$, both abelian groups. Hence $G(p)$ is solvable. (**3 marks, similar to an exercise, B**)

(ii) Suppose $p > 2$. We claim that the commutator subgroup $G(p)' = N(p)$. Clearly $G(p)' \leq N(p)$ since $G(p)/N(p)$ is abelian. Also

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2x \\ 0 & 1 \end{pmatrix},$$

which shows that $N(p) \leq G(p)'$, proving the claim. The above calculation also shows that $[G(p), N(p)] = N(p)$. So the lower central series of $G(p)$ does not terminate at 1, showing that $G(p)$ is not nilpotent when $p > 2$.

On the other hand, if $p = 2$ then $|G(p)| = 2$, so $G(2)$ is nilpotent. (**5 marks, similar to an exercise, C**)

(c) Suppose G is nilpotent. By a standard result, $G \cong P_1 \times \cdots \times P_k$, the direct product of its Sylow subgroups. As x, y have coprime orders, we can re-order the Sylow subgroups so that $x \in P_1 \cdots P_r$ and $y \in P_{r+1} \cdots P_k$ for some r. As the Sylow subgroups all commute with each other, it follows that x, y commute. (**5 marks, unseen, D**)

(d) Let $G = S_3$ and take $x = (1\,2)$, $y = (1\,2\,3)$. (**3 marks, unseen, B**)

4. (a) $N_G(H) = \{g \in G : gHg^{-1} = H\}$, $C_G(H) = \{g \in G : gh = hg \ \forall h \in H\}$. (**Bookwork, 2 marks, A**)

For $n \in N_G(H)$, let $\iota_n : H \mapsto H$ be the conjugation map sending $h \mapsto nhn^{-1}$. Then $\iota_n \in \mathrm{Aut}(H)$, and the map $\iota : N_G(H) \mapsto \mathrm{Aut}(H)$ sending $n \mapsto \iota_n$ is a homomorphism with kernel $C_G(H)$. Hence $N_G(H)/C_G(H) \cong \mathrm{Im}(\iota) \leq \mathrm{Aut}(H)$. (**Bookwork, 3 marks, A**)

(b) Let $C_p = \langle x \rangle$. If $\alpha \in \mathrm{Aut}(C_p)$ then α sends x to x^i for some $1 \leq i \leq p-1$. Every such i gives an aut, namely $x^k \mapsto x^{ik}$ for all k; call this aut α_i. Thus $\mathrm{Aut}(C_p) = \{\alpha_i : 1 \leq i \leq p-1\}$. This is abelian, as both $\alpha_i\alpha_j$ and $\alpha_j\alpha_i$ send $x \mapsto x^{ij}$. (**Seen as exercise, 3 marks, B**)

(c) **Burnside's transfer theorem**: Let p be prime, $P \in Syl_p(G)$, and suppose that $P \leq Z(N_G(P))$. Then G has a normal p-complement (ie. a normal subgroup N such that $G = PN$ and $P \cap N = 1$). (**Bookwork, 2 marks, A**)

(d) (i) We have $|P| = p_1$, so $P \cong C_{p_1}$. By (a), $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(C_{p_1})$, which by (b) has order $p_1 - 1$. As p_1 is the smallest prime dividing $|G|$, $p_1 - 1$ is coprime to $|G|$, and so $N_G(P)/C_G(P)$ must be 1, i.e. $N_G(P) = C_G(P)$. (**4 marks, C**)

(ii) By (i) we have $P = C_G(P) = N_G(P)$, so Burnside's theorem shows that G has a normal p_1-complement, which is a normal subgroup of order $p_2 \cdots p_k$. (**2 marks, C**)

(iii) Proceed by induction on $k \geq 1$. If $k = 1$ then G is cyclic, hence solvable. For $k \geq 2$, we saw in (ii) that G has a normal subgroup N of order $p_2 \cdots p_k$, which by induction is solvable. Then both N and $G/N \cong C_{p_1}$ are solvable, so by a standard result, G is solvable. (**4 marks, C – all of (c) is a simplified version of a more general result in lectures**)

Mastery Question 5.

(a) $GL_n(\mathbb{F}_q)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_q$, under matrix multiplication. (**1 mark**)

(b) **Claim** $|GL_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i)$.

Proof Pick a basis $e_1, \ldots, e_n$ of $V = \mathbb{F}_q^n$. For each basis $f_1, \ldots, f_n$ there is a unique element of $GL_n(\mathbb{F}_q)$ that maps $e_i \mapsto f_i$ for all i. Hence $|GL_n(q)|$ is equal to the number of (ordered) bases of V. We count these as follows:

$$\begin{aligned} &\text{no. of choices for } f_1 = |V \setminus 0| = q^n - 1, \\ &\text{no. of choices for } f_2 = |V \setminus \langle f_1 \rangle| = q^n - q, \\ &\text{no. of choices for } f_3 = |V \setminus \langle f_1, f_2 \rangle| = q^n - q^2, \end{aligned}$$

and so on. Hence the number of bases is as in the Claim. (**4 marks**)

(c) (i) $|\Omega| = (q^n - 1)/(q - 1)$. (**1 mark**)

(ii) Let $\omega_1 = \langle v_1 \rangle$, $\omega_2 = \langle v_2 \rangle \in \Omega$. There exists $g \in G$ sending $v_1 \mapsto v_2$, hence sendiong $\omega_1 \mapsto \omega_2$. So the action is transitive. (**1 mark**)

(iii) (1) Clearly G is transitive on Δ_1 by (ii). For Δ_2, let (ω_1, ω_2), $(\omega_1', \omega_2') \in \Delta_2$. Then

$$(\omega_1, \omega_2) = (\langle v_1 \rangle, \langle v_2 \rangle),\ (\omega_1', \omega_2') = (\langle v_1' \rangle, \langle v_2' \rangle).$$

Since $\langle v_1 \rangle \neq \langle v_2 \rangle$, the vectors v_1, v_2 are linearly indep, and so are v_1', v_2'. We can extend both pairs to bases of V, and hence there exists $g \in G$ sending $v_1 \mapsto v_1'$, $v_2 \mapsto v_2'$. So g maps $(\omega_1, \omega_2) \mapsto (\omega_1', \omega_2')$. Thus G is transitive on Δ_2 and we've shown Δ_1, Δ_2 are the orbits on $\Omega \times \Omega$. (**3 marks**)

(2) We have $|\Delta_2| = |\Omega|(|\Omega| - 1) = \frac{(q^n-1)(q^n-q)}{(q-1)^2}$, and so

$$|G_\delta| = |G|/|\Delta_2| = (q-1)^2 \prod_{i=2}^{n-1}(q^n - q^i),$$

(where for $n = 2$, the empty product is 1). (**3 marks**)

(iv) (1) Let $n \geq 3$ and let v_1, v_2, v_3 be linearly indep vectors. Then $(\langle v_1 \rangle, \langle v_2 \rangle, \langle v_3 \rangle)$ and $(\langle v_1 \rangle, \langle v_2 \rangle, \langle v_1 + v_2 \rangle)$ are both in Φ but are clearly in different orbits of G, so G is not transitive on Φ. (**3 marks**)

(2) Let $n = 2$ and let $\phi_1, \phi_2 \in \Phi$. We can write these as

$$\phi_1 = (\langle v_1 \rangle, \langle v_2 \rangle, \langle \alpha v_1 + \beta v_2 \rangle),\ \ \phi_2 = (\langle w_1 \rangle, \langle w_2 \rangle, \langle \gamma w_1 + \delta w_2 \rangle),$$

where $\alpha, \beta, \gamma, \delta \neq 0$. Now choose $g \in G = GL_2(\mathbb{F}_q)$ mapping

$$v_1 \mapsto \alpha^{-1}\gamma w_1,\ v_2 \mapsto \beta^{-1}\delta w_2.$$

Then g snds $\phi_1 \mapsto \phi_2$. So G is transitive on Φ. (**4 marks**)

The ideas for the calculations in this question can be found within proofs in the Mastery source material.

MATH60036 Group Theory

Question	Marker's comment
1	This was reasonably well done, although there were not many successful attempts at the last part.
2	Pretty good attempts by almost all candidates.
3	Rather variable performance on this question. Many did not answer the example in part (b) too well.
4	Quite a standard question, quite well answered.

MATH70036 Group Theory

Question	Marker's comment
1	This was reasonably well done, although there were not many successful attempts at the last part.
2	Pretty good attempts by almost all candidates.
3	Rather variable performance on this question. Many did not answer the example in part (b) too well.
4	Quite a standard question, quite well answered.
5	There was only one serious lengthy attempt at the mastery question. That attempt gained full marks, so it was certainly possible to do well on the question. All others just picked up a few marks for easy bookwork and left it there.