Part IA

Groups

Year

Paper 3, Section I

1D Groups

Let G be a finite group and N a normal subgroup of G. Let C_n denote the cyclic group of order n.

Are the following statements true or false? Justify your answers.

(i) If $G/N \cong C_2$ and $N \cong C_2$ then $G \cong C_4$.

(ii) If $G/N \cong C_3$ and $N \cong C_2$ then $G \cong C_6$.

(iii) Let H be a finite group and M a normal subgroup of H. If $G/N \cong H/M$ and $N \cong M$ then $G \cong H$.

Paper 3, Section I

2D Groups

Prove that a Möbius map is determined by the image of just 3 points.

Paper 3, Section II

5D Groups

State and prove Lagrange's theorem.

Let H and K be subgroups of a finite group G. Show that $H \cap K$ is a subgroup of G. What can be said about $H \cap K$ if H and K have co-prime orders? Justify your answer.

Let G be a finite group and x an element of G. Define the *order* of x in G and denote it by $o(x)$. Let k be a positive integer. Prove that $x^k = e$ if and only if $o(x)$ divides k. (Here e denotes the identity element of G.)

Now suppose x and y are elements of G with co-prime orders. Further suppose $xy = yx$. Prove that $o(xy) = o(x)o(y)$.

Let x and y be two non-identity elements of G.

(i) If $o(x)$ and $o(y)$ are co-prime is it always true that $o(xy) = o(x)o(y)$?

(ii) If $xy = yx$ is it always true that $o(xy) = o(x)o(y)$?

State Cauchy's theorem. Hence, or otherwise, show that there are exactly two groups of order 26 up to isomorphism.

Paper 3, Section II

6D Groups

Let N be a normal subgroup of a group G and let G/N denote the set of left cosets of N in G. Explain how G/N is given a well-defined group structure.

Let $x, y \in G$. The *commutator* of x and y is defined by $[x, y] = x^{-1}y^{-1}xy$. Let $\overline{G}$ be the set of finite products of commutators of G, that is elements of $\overline{G}$ are of the form $[x_1, y_1][x_2, y_2] \ldots [x_k, y_k]$, where $x_i, y_i \in G$ for $1 \leqslant i \leqslant k$. Prove that $\overline{G}$ is a normal subgroup of G.

Show that $G/\overline{G}$ is an abelian group. Further, show that if N is a normal subgroup of G and G/N is abelian, then $\overline{G}$ is a subgroup of N.

Determine $\overline{G}$ when G is each of the following groups. Justify your answers.

(i) D_8 the dihedral group of order 8.

(ii) A_5 the alternating group of degree 5.

(iii) S_5 the symmetric group of degree 5.

Paper 3, Section II

7D Groups

Let H and K be subgroups of a finite group G. Show that

$$|HK| = \frac{|H||K|}{|H \cap K|}\,,$$

where $HK = \{hk : h \in H, k \in K\}$.

Let a and b be co-prime. If $|G : H| = a$ and $|G : K| = b$, show that $HK = G$.

Let $x \in G$. Define the *conjugacy class* of x in G and denote it by $\mathrm{Conj}_G(x)$. Define the *centraliser* of x in G and denote it by $C_G(x)$.

Let $x, y \in G$. Suppose $|\mathrm{Conj}_G(x)| = a$ and $|\mathrm{Conj}_G(y)| = b$ with a and b co-prime. Show that $C_G(x)C_G(y) = G$. Prove that

$$\mathrm{Conj}_G(xy) = \mathrm{Conj}_G(x)\mathrm{Conj}_G(y)\,,$$

where $\mathrm{Conj}_G(x)\mathrm{Conj}_G(y) = \{uv : u \in \mathrm{Conj}_G(x), v \in \mathrm{Conj}_G(y)\}$. [*Hint: Observe that $g^{-1}xgh^{-1}yh$ may be written as $h^{-1}(hg^{-1}xgh^{-1}y)h$, where $g, h \in G$.*]

Paper 3, Section II

8D Groups

State and prove the first isomorphism theorem. [You may assume that images of homomorphisms are subgroups and that kernels of homomorphisms are normal subgroups.]

Define the groups $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{SL}_n(\mathbb{R})$. Prove that $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$ and identify $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$.

Let $\mathrm{M}_2(\mathbb{Z})$ denote the set of 2×2 matrices with entries in $\mathbb{Z}$. Let

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}) : ad - bc \neq 0 \text{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \mathrm{M}_2(\mathbb{Z}) \right\}.$$

Check that G is a group and that it is infinite. Show that

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}) : ad - bc = \pm 1 \right\}.$$

Consider the following subset of G,

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G : a, d \equiv 1 \bmod 2, \ \ b, c \equiv 0 \bmod 2 \right\}.$$

By considering a suitable homomorphism, or otherwise, show that H is a normal subgroup of finite index in G.

Paper 3, Section I
1E Groups

Let G and H be finite groups and $g \in G$.

Define the *order* of g.

Show that if $\phi\colon G \to H$ is a homomorphism then the order of $\phi(g)$ divides the order of g.

Show that if ϕ is surjective and H has an element of order m then G has an element of order m.

How many homomorphisms $C_9 \to S_4$ are there?

Paper 3, Section I
2E Groups

What does it mean to say a group is *abelian*? What does it mean to say a group is *cyclic*?

Show that every cyclic group is abelian. Show that not every abelian group is cyclic.

Recall that the *proper subgroups* of a group G are the subgroups of G not equal to G. If every proper subgroup of a group G is cyclic then must G be abelian? Justify your answer.

Paper 3, Section II
5E Groups

What does it mean for a group G to *act* on a set X. Given such an action and $x \in X$ define the *orbit* and *stabiliser* of x. State and prove the orbit–stabiliser theorem for a finite group.

State and prove Cauchy's theorem.

Suppose that G is a group of order 33. By considering the conjugation action of a subgroup of G on G, show that G must be cyclic.

Paper 3, Section II
6E Groups

What is a *Möbius transformation*?

Show carefully that if (z_1, z_2, z_3) and (w_1, w_2, w_3) are two ordered subsets of the extended complex plane $\widehat{\mathbb{C}}$, each consisting of three distinct points, then there is a unique Möbius transformation f such that $f(z_i) = w_i$ for $i = 1, 2, 3$. [You may assume that the Möbius transformations form a group under composition.]

Define the *cross-ratio* $[z_1, z_2, z_3, z_4]$ of four distinct points $z_1, z_2, z_3, z_4 \in \widehat{\mathbb{C}}$. Show that a bijection $f\colon \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ is a Möbius transformation if and only if f preserves the cross-ratio of any four distinct points in $\widehat{\mathbb{C}}$; that is, if and only if

$$[z_1, z_2, z_3, z_4] = [f(z_1), f(z_2), f(z_3), f(z_4)]$$

for any four distinct points z_1, z_2, z_3, z_4 in $\widehat{\mathbb{C}}$.

Are there complex numbers a and b such that the map that sends z to $a\bar{z} + b$ for $z \in \mathbb{C}$ and fixes ∞ is Möbius? Justify your answer. [Here $\bar{z}$ denotes the complex conjugate of z.]

Paper 3, Section II
7E Groups

Suppose G is a group. What does it mean to say that a subset K of G is a *normal subgroup* of G? For N a normal subgroup of G explain how to define the *quotient group* G/N. Briefly explain why G/N is a group.

Define the *kernel* and the *image* of a group homomorphism. Show that a subset K of G is a normal subgroup of G if and only if there is a group H and a group homomorphism $\theta\colon G \to H$ such that K is the kernel of θ. Show moreover that in this case the image of θ is a subgroup of H and G/K is isomorphic to the image of θ.

By defining a suitable group homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{C}\backslash\{0\}, \cdot)$, show that $\mathbb{R}/\mathbb{Z}$ is isomorphic to the subgroup of $(\mathbb{C}\backslash\{0\}, \cdot)$ consisting of complex numbers of modulus 1. What characterises the elements of the image of $\mathbb{Q}/\mathbb{Z}$ under this isomorphism?

Paper 3, Section II

8E Groups

Show that the set $S(\mathbb{N})$ of invertible functions $\tau\colon \mathbb{N} \to \mathbb{N}$ is a group under composition. Show that the subset $S^{\mathrm{fin}}(\mathbb{N})$ of invertible functions $\tau\colon \mathbb{N} \to \mathbb{N}$ such that there is some $n \geqslant 1$ with $\tau(m) = m$ for all $m > n$ is a subgroup of $S(\mathbb{N})$.

A *cycle* is a non-identity element σ of $S^{\mathrm{fin}}(\mathbb{N})$ such that for every $m, n \in \mathbb{N}$ either $\sigma(m) = m$ or $\sigma(n) = n$ or there is an integer a such that $\sigma^a(m) = n$. Show that if σ is a cycle and $n \in \mathbb{N}$ such that $\sigma(n) \neq n$ then the order of σ is the least positive integer l such that $\sigma^l(n) = n$. Show in particular that the order of σ is always finite.

Show that every element τ of $S^{\mathrm{fin}}(\mathbb{N})$ can be written as a product of cycles $\sigma_1 \cdots \sigma_k$ such that for every $1 \leqslant i < j \leqslant k$ and every $n \in \mathbb{N}$ either $\sigma_i(n) = n$ or $\sigma_j(n) = n$ (or both). Show moreover that $\sigma_i \sigma_j = \sigma_j \sigma_i$ for all $1 \leqslant i < j \leqslant k$. What is the relationship between the order of τ and the orders of $\sigma_1, \ldots, \sigma_k$? Justify your answer.

Paper 3, Section I
1D Groups

Let G be a finite group and denote the *centre* of G by $Z(G)$. Prove that if the quotient group $G/Z(G)$ is cyclic then G is abelian. Does there exist a group H such that

(i) $|H/Z(H)| = 7$?

(ii) $|H/Z(H)| = 6$?

Justify your answers.

Paper 3, Section I
2D Groups

Let g and h be elements of a group G. What does it mean to say g and h are *conjugate* in G? Prove that if two elements in a group are conjugate then they have the same order.

Define the Möbius group $\mathcal{M}$. Prove that if $g, h \in \mathcal{M}$ are conjugate they have the same number of fixed points. Quoting clearly any results you use, show that any nontrivial element of $\mathcal{M}$ of finite order has precisely 2 fixed points.

Paper 3, Section II

5D Groups

(a) Let x be an element of a finite group G. Define the *order* of x and the *order* of G. State and prove Lagrange's theorem. Deduce that the order of x divides the order of G.

(b) If G is a group of order n, and d is a divisor of n where $d < n$, is it always true that G must contain an element of order d? Justify your answer.

(c) Denote the cyclic group of order m by C_m.

(i) Prove that if m and n are coprime then the direct product $C_m \times C_n$ is cyclic.

(ii) Show that if a finite group G has all non-identity elements of order 2, then G is isomorphic to $C_2 \times \cdots \times C_2$. [The direct product theorem may be used without proof.]

(d) Let G be a finite group and H a subgroup of G.

(i) Let x be an element of order d in G. If r is the least positive integer such that $x^r \in H$, show that r divides d.

(ii) Suppose further that H has index n. If $x \in G$, show that $x^k \in H$ for some k such that $0 < k \leqslant n$. Is it always the case that the least positive such k is a factor of n? Justify your answer.

Paper 3, Section II

6D Groups

(a) Let G be a finite group acting on a set X. For $x \in X$, define the *orbit* $\mathrm{Orb}(x)$ and the *stabiliser* $\mathrm{Stab}(x)$ of x. Show that $\mathrm{Stab}(x)$ is a subgroup of G. State and prove the orbit-stabiliser theorem.

(b) Let $n \geqslant k \geqslant 1$ be integers. Let $G = S_n$, the symmetric group of degree n, and X be the set of all ordered k-tuples $(x_1, \ldots, x_k)$ with $x_i \in \{1, 2, \ldots, n\}$. Then G acts on X, where the action is defined by $\sigma(x_1, \ldots, x_k) = (\sigma(x_1), \ldots, \sigma(x_k))$ for $\sigma \in S_n$ and $(x_1, \ldots, x_k) \in X$. For $x = (1, 2, \ldots, k) \in X$, determine $\mathrm{Orb}(x)$ and $\mathrm{Stab}(x)$ and verify that the orbit-stabiliser theorem holds in this case.

(c) We say that G acts *doubly transitively* on X if, whenever (x_1, x_2) and (y_1, y_2) are elements of $X \times X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists some $g \in G$ such that $gx_1 = y_1$ and $gx_2 = y_2$.

Assume that G is a finite group that acts doubly transitively on X, and let $x \in X$. Show that if H is a subgroup of G that properly contains $\mathrm{Stab}(x)$ (that is, $\mathrm{Stab}(x) \subseteq H$ but $\mathrm{Stab}(x) \neq H$) then the action of H on X is transitive. Deduce that $H = G$.

Paper 3, Section II

7D Groups

Let G be a finite group of order n. Show that G is isomorphic to a subgroup H of S_n, the symmetric group of degree n. Furthermore show that this isomorphism can be chosen so that any nontrivial element of H has no fixed points.

Suppose n is even. Prove that G contains an element of order 2.

What does it mean for an element of S_m to be odd? Suppose H is a subgroup of S_m for some m, and H contains an odd element. Prove that precisely half of the elements of H are odd.

Now suppose $n = 4k + 2$ for some positive integer k. Prove that G is not simple. [*Hint: Consider the sign of an element of order 2.*]

Can a nonabelian group of even order be simple?

Paper 3, Section II

8D Groups

(a) Let A be an abelian group (not necessarily finite). We define the *generalised dihedral group* to be the set of pairs

$$D(A) = \{(a,\ \varepsilon) : a \in A,\ \varepsilon = \pm 1\}\,,$$

with multiplication given by

$$(a,\ \varepsilon)(b,\ \eta) = (ab^{\varepsilon},\ \varepsilon\eta)\,.$$

The identity is $(e, 1)$ and the inverse of (a, ε) is $(a^{-\varepsilon}, \varepsilon)$. You may assume that this multiplication defines a group operation on $D(A)$.

(i) Identify A with the set of all pairs in which $\varepsilon = +1$. Show that A is a subgroup of $D(A)$. By considering the index of A in $D(A)$, or otherwise, show that A is a normal subgroup of $D(A)$.

(ii) Show that every element of $D(A)$ not in A has order 2. Show that $D(A)$ is abelian if and only if $a^2 = e$ for all $a \in A$. If $D(A)$ is non-abelian, what is the centre of $D(A)$? Justify your answer.

(b) Let $\mathrm{O}(2)$ denote the group of 2×2 orthogonal matrices. Show that all elements of $\mathrm{O}(2)$ have determinant 1 or -1. Show that every element of $\mathrm{SO}(2)$ is a rotation. Let $J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Show that $\mathrm{O}(2)$ decomposes as a union $\mathrm{SO}(2) \cup \mathrm{SO}(2)J$.

[You may assume standard properties of determinants.]

(c) Let B be the (abelian) group $\{z \in \mathbb{C} : |z| = 1\}$, with multiplication of complex numbers as the group operation. Write down, without proof, isomorphisms $\mathrm{SO}(2) \cong B \cong \mathbb{R}/\mathbb{Z}$ where $\mathbb{R}$ denotes the additive group of real numbers and $\mathbb{Z}$ the subgroup of integers. Deduce that $\mathrm{O}(2) \cong D(B)$, the generalised dihedral group defined in part (a).

Paper 2, Section I

1E Groups

What does it mean for an element of the symmetric group S_n to be a *transposition* or a *cycle*?

Let $n \geqslant 4$. How many permutations σ of $\{1, 2, \ldots, n\}$ are there such that

(i) $\sigma(1) = 2$?

(ii) $\sigma(k)$ is even for each even number k?

(iii) σ is a 4-cycle?

(iv) σ can be written as the product of two transpositions?

You should indicate in each case how you have derived your formula.

Paper 2, Section II

5E Groups

Suppose that f is a Möbius transformation acting on the extended complex plane. Show that a Möbius transformation with at least three fixed points is the identity. Deduce that every Möbius transformation except the identity has one or two fixed points.

Which of the following statements are true and which are false? Justify your answers, quoting standard facts if required.

(i) If f has exactly one fixed point then it is conjugate to $z \mapsto z + 1$.

(ii) Every Möbius transformation that fixes ∞ may be expressed as a composition of maps of the form $z \mapsto z + a$ and $z \mapsto \lambda z$ (where a and λ are complex numbers).

(iii) Every Möbius transformation that fixes 0 may be expressed as a composition of maps of the form $z \mapsto \mu z$ and $z \mapsto 1/z$ (where μ is a complex number).

(iv) The operation of complex conjugation defined by $z \mapsto \bar{z}$ is a Möbius transformation.

Paper 2, Section II

6E Groups

(a) Let G be a finite group acting on a finite set X. For any subset T of G, we define the *fixed point set* as $X^T = \{x \in X : \forall g \in T,\ g \cdot x = x\}$. Write X^g for $X^{\{g\}}$ $(g \in G)$. Let $G \setminus X$ be the set of G-orbits in X. In what follows you may assume the orbit–stabiliser theorem.

Prove that

$$|X| = |X^G| + \sum_x |G|/|G_x|,$$

where the sum is taken over a set of representatives for the orbits containing more than one element.

By considering the set $Z = \{(g,x) \in G \times X : g \cdot x = x\}$, or otherwise, show also that

$$|G \setminus X| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

(b) Let V be the set of vertices of a regular pentagon and let the dihedral group D_{10} act on V. Consider the set X_n of functions $F : V \to \mathbb{Z}_n$ (the integers mod n). Assume that D_{10} and its rotation subgroup C_5 act on X_n by the rule

$$(g \cdot F)(v) = F(g^{-1} \cdot v),$$

where $g \in D_{10}$, $F \in X_n$ and $v \in V$. It is given that $|X_n| = n^5$. We define a *necklace* to be a C_5-orbit in X_n and a *bracelet* to be a D_{10}-orbit in X_n.

Find the number of necklaces and bracelets for any n.

Paper 3, Section I

1D Groups

Prove that two elements of S_n are conjugate if and only if they have the same cycle type.

Describe a condition on the centraliser (in S_n) of a permutation $\sigma \in A_n$ that ensures the conjugacy class of σ in A_n is the same as the conjugacy class of σ in S_n. Justify your answer.

How many distinct conjugacy classes are there in A_5?

Paper 3, Section I

2D Groups

What is the orthogonal group $\mathrm{O}(n)$? What is the special orthogonal group $\mathrm{SO}(n)$?

Show that every element of $\mathrm{SO}(3)$ has an eigenvector with eigenvalue 1.

Is it true that every element of $\mathrm{O}(3)$ is either a rotation or a reflection? Justify your answer.

Paper 3, Section II

5D Groups

Let H and K be subgroups of a group G satisfying the following two properties.

(i) All elements of G can be written in the form hk for some $h \in H$ and some $k \in K$.

(ii) $H \cap K = \{e\}$.

Prove that H and K are normal subgroups of G if and only if all elements of H commute with all elements of K.

State and prove Cauchy's Theorem.

Let p and q be distinct primes. Prove that an abelian group of order pq is isomorphic to $C_p \times C_q$. Is it true that all abelian groups of order p^2 are isomorphic to $C_p \times C_p$?

Paper 3, Section II

6D Groups

State and prove Lagrange's Theorem.

Hence show that if G is a finite group and $g \in G$ then the order of g divides the order of G.

How many elements are there of order 3 in the following groups? Justify your answers.

(a) $C_3 \times C_9$, where C_n denotes the cyclic group of order n.

(b) D_{2n} the dihedral group of order $2n$.

(c) S_7 the symmetric group of degree 7.

(d) A_7 the alternating group of degree 7.

Paper 3, Section II

7D Groups

State and prove the first isomorphism theorem. [You may assume that kernels of homomorphisms are normal subgroups and images are subgroups.]

Let G be a group with subgroup H and normal subgroup N. Prove that $NH = \{nh : n \in N, h \in H\}$ is a subgroup of G and $N \cap H$ is a normal subgroup of H. Further, show that N is a normal subgroup of NH.

Prove that $\frac{H}{N \cap H}$ is isomorphic to $\frac{NH}{N}$.

If K and H are both normal subgroups of G must KH be a normal subgroup of G?

If K and H are subgroups of G, but not normal subgroups, must KH be a subgroup of G?

Justify your answers.

Paper 3, Section II

8D Groups

Let $\mathcal{M}$ be the group of Möbius transformations of $\mathbb{C} \cup \{\infty\}$ and let $\mathrm{SL}_2(\mathbb{C})$ be the group of all 2×2 complex matrices of determinant 1.

Show that the map $\theta : \mathrm{SL}_2(\mathbb{C}) \to \mathcal{M}$ given by

$$\theta \begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az+b}{cz+d}$$

is a surjective homomorphism. Find its kernel.

Show that any $T \in \mathcal{M}$ not equal to the identity is conjugate to a Möbius map S where either $Sz = \mu z$ with $\mu \neq 0, 1$ or $Sz = z + 1$. [You may use results about matrices in $\mathrm{SL}_2(\mathbb{C})$ as long as they are clearly stated.]

Show that any non-identity Möbius map has one or two fixed points. Also show that if T is a Möbius map with just one fixed point z_0 then $T^n z \to z_0$ as $n \to \infty$ for any $z \in \mathbb{C} \cup \{\infty\}$. [You may assume that Möbius maps are continuous.]

Paper 3, Section I

1D Groups

Find the order and the sign of the permutation $(13)(2457)(815) \in S_8$.

How many elements of S_6 have order 6? And how many have order 3?

What is the greatest order of any element of A_9?

Paper 3, Section I

2D Groups

Prove that every member of $O(3)$ is a product of at most three reflections.

Is every member of $O(3)$ a product of at most two reflections? Justify your answer.

Paper 3, Section II

5D Groups

Define the *sign* of a permutation $\sigma \in S_n$. You should show that it is well-defined, and also that it is multiplicative (in other words, that it gives a homomorphism from S_n to $\{\pm 1\}$).

Show also that (for $n \geqslant 2$) this is the only surjective homomorphism from S_n to $\{\pm 1\}$.

Paper 3, Section II

6D Groups

Let g be an element of a group G. We define a map g^* from G to G by sending x to gxg^{-1}. Show that g^* is an *automorphism* of G (that is, an isomorphism from G to G).

Now let A denote the group of automorphisms of G (with the group operation being composition), and define a map θ from G to A by setting $\theta(g) = g^*$. Show that θ is a homomorphism. What is the kernel of θ?

Prove that the image of θ is a normal subgroup of A.

Show that if G is cyclic then A is abelian. If G is abelian, must A be abelian? Justify your answer.

Paper 3, Section II
7D Groups

Define the *quotient group* G/H, where H is a normal subgroup of a group G. You should check that your definition is well-defined. Explain why, for G finite, the greatest order of any element of G/H is at most the greatest order of any element of G.

Show that a subgroup H of a group G is normal if and only if there is a homomorphism from G to some group whose kernel is H.

A group is called *metacyclic* if it has a cyclic normal subgroup H such that G/H is cyclic. Show that every dihedral group is metacyclic.

Which groups of order 8 are metacyclic? Is A_4 metacyclic? For which $n \leqslant 5$ is S_n metacyclic?

Paper 3, Section II
8D Groups

State and prove the Direct Product Theorem.

Is the group $O(3)$ isomorphic to $SO(3) \times C_2$? Is $O(2)$ isomorphic to $SO(2) \times C_2$?

Let $U(2)$ denote the group of all invertible 2×2 complex matrices A with $A\overline{A}^{\mathrm{T}} = I$, and let $SU(2)$ be the subgroup of $U(2)$ consisting of those matrices with determinant 1.

Determine the centre of $U(2)$.

Write down a surjective homomorphism from $U(2)$ to the group T of all unit-length complex numbers whose kernel is $SU(2)$. Is $U(2)$ isomorphic to $SU(2) \times T$?

Paper 3, Section I

1E Groups

Let w_1, w_2, w_3 be distinct elements of $\mathbb{C} \cup \{\infty\}$. Write down the Möbius map f that sends w_1, w_2, w_3 to $\infty, 0, 1$, respectively. [*Hint: You need to consider four cases.*]

Now let w_4 be another element of $\mathbb{C} \cup \{\infty\}$ distinct from w_1, w_2, w_3. Define the *cross-ratio* $[w_1, w_2, w_3, w_4]$ in terms of f.

Prove that there is a circle or line through w_1, w_2, w_3 and w_4 if and only if the cross-ratio $[w_1, w_2, w_3, w_4]$ is real.

[*You may assume without proof that Möbius maps map circles and lines to circles and lines and also that there is a unique circle or line through any three distinct points of* $\mathbb{C} \cup \{\infty\}$.]

Paper 3, Section I

2E Groups

What does it mean to say that H is a *normal subgroup* of the group G? For a normal subgroup H of G define the quotient group G/H. [You do not need to verify that G/H is a group.]

State the Isomorphism Theorem.

Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; a, b, d \in \mathbb{R},\ ad \neq 0 \right\}$$

be the group of 2×2 invertible upper-triangular real matrices. By considering a suitable homomorphism, show that the subset

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}$$

of G is a normal subgroup of G and identify the quotient G/H.

Paper 3, Section II

5E Groups

Let N be a normal subgroup of a finite group G of prime index $p = |G : N|$.

By considering a suitable homomorphism, show that if H is a subgroup of G that is not contained in N, then $H \cap N$ is a normal subgroup of H of index p.

Let C be a conjugacy class of G that is contained in N. Prove that C is either a conjugacy class in N or is the disjoint union of p conjugacy classes in N.

[*You may use standard theorems without proof.*]

Paper 3, Section II

6E Groups

State Lagrange's theorem. Show that the order of an element x in a finite group G is finite and divides the order of G.

State Cauchy's theorem.

List all groups of order 8 up to isomorphism. Carefully justify that the groups on your list are pairwise non-isomorphic and that any group of order 8 is isomorphic to one on your list. [You may use without proof the Direct Product Theorem and the description of standard groups in terms of generators satisfying certain relations.]

Paper 3, Section II
7E Groups

(a) Let G be a finite group acting on a finite set X. State the Orbit-Stabiliser theorem. [Define the terms used.] Prove that

$$\sum_{x\in X}|\mathrm{Stab}(x)| = n|G| ,$$

where n is the number of distinct orbits of X under the action of G.

Let $S = \{(g,x) \in G\times X : g\cdot x = x\}$, and for $g \in G$, let $\mathrm{Fix}(g) = \{x \in X : g\cdot x = x\}$. Show that

$$|S| = \sum_{x\in X}|\mathrm{Stab}(x)| = \sum_{g\in G}|\mathrm{Fix}(g)| ,$$

and deduce that

$$n = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| . \qquad (*)$$

(b) Let H be the group of rotational symmetries of the cube. Show that H has 24 elements. [If your proof involves calculating stabilisers, then you must carefully verify such calculations.]

Using $(*)$, find the number of distinct ways of colouring the faces of the cube red, green and blue, where two colourings are distinct if one cannot be obtained from the other by a rotation of the cube. [A colouring need not use all three colours.]

Paper 3, Section II
8E Groups

Prove that every element of the symmetric group S_n is a product of transpositions. [You may assume without proof that every permutation is the product of disjoint cycles.]

(a) Define the *sign* of a permutation in S_n, and prove that it is well defined. Define the *alternating group* A_n.

(b) Show that S_n is generated by the set $\{(1\ 2), (1\ 2\ 3\ \ldots\ n)\}$.

Given $1 \leqslant k < n$, prove that the set $\{(1\ 1{+}k), (1\ 2\ 3\ \ldots\ n)\}$ generates S_n if and only if k and n are coprime.

Paper 3, Section I

1D Groups

Let G be a group, and let H be a subgroup of G. Show that the following are equivalent.

(i) $a^{-1}b^{-1}ab \in H$ for all $a, b \in G$.

(ii) H is a normal subgroup of G and G/H is abelian.

Hence find all abelian quotient groups of the dihedral group D_{10} of order 10.

Paper 3, Section I

2D Groups

State and prove Lagrange's theorem.

Let p be an odd prime number, and let G be a finite group of order $2p$ which has a normal subgroup of order 2. Show that G is a cyclic group.

Paper 3, Section II

5D Groups

For each of the following, either give an example or show that none exists.

(i) A non-abelian group in which every non-trivial element has order 2.

(ii) A non-abelian group in which every non-trivial element has order 3.

(iii) An element of S_9 of order 18.

(iv) An element of S_9 of order 20.

(v) A finite group which is not isomorphic to a subgroup of an alternating group.

Paper 3, Section II

6D Groups

Define the *sign*, $\operatorname{sgn}(\sigma)$, of a permutation $\sigma \in S_n$ and prove that it is well defined. Show that the function $\operatorname{sgn} : S_n \to \{1, -1\}$ is a homomorphism.

Show that there is an injective homomorphism $\psi : GL_2(\mathbb{Z}/2\mathbb{Z}) \to S_4$ such that $\operatorname{sgn} \circ \psi$ is non-trivial.

Show that there is an injective homomorphism $\phi : S_n \to GL_n(\mathbb{R})$ such that $\det(\phi(\sigma)) = \operatorname{sgn}(\sigma)$.

Paper 3, Section II

7D Groups

State and prove the orbit-stabiliser theorem.

Let p be a prime number, and G be a finite group of order p^n with $n \geqslant 1$. If N is a non-trivial normal subgroup of G, show that $N \cap Z(G)$ contains a non-trivial element.

If H is a proper subgroup of G, show that there is a $g \in G \backslash H$ such that $g^{-1}Hg = H$.

[You may use Lagrange's theorem, provided you state it clearly.]

Paper 3, Section II

8D Groups

Define the *Möbius group* $\mathcal{M}$ and its action on the Riemann sphere $\mathbb{C}_\infty$. [You are not required to verify the group axioms.] Show that there is a surjective group homomorphism $\phi : SL_2(\mathbb{C}) \to \mathcal{M}$, and find the kernel of ϕ.

Show that if a non-trivial element of $\mathcal{M}$ has finite order, then it fixes precisely two points in $\mathbb{C}_\infty$. Hence show that any finite abelian subgroup of $\mathcal{M}$ is either cyclic or isomorphic to $C_2 \times C_2$.

[You may use standard properties of the Möbius group, provided that you state them clearly.]

Paper 3, Section I

1D Groups

Say that a group is *dihedral* if it has two generators x and y, such that x has order n (greater than or equal to 2 and possibly infinite), y has order 2, and $yxy^{-1} = x^{-1}$. In particular the groups C_2 and $C_2 \times C_2$ are regarded as dihedral groups. Prove that:

(i) any dihedral group can be generated by two elements of order 2;

(ii) any group generated by two elements of order 2 is dihedral; and

(iii) any non-trivial quotient group of a dihedral group is dihedral.

Paper 3, Section I

2D Groups

How many cyclic subgroups (including the trivial subgroup) does S_5 contain? Exhibit two isomorphic subgroups of S_5 which are not conjugate.

Paper 3, Section II

5D Groups

What does it mean for a group G to *act on* a set X? For $x \in X$, what is meant by the *orbit* $\text{Orb}(x)$ to which x belongs, and by the *stabiliser* G_x of x? Show that G_x is a subgroup of G. Prove that, if G is finite, then $|G| = |G_x| \cdot |\text{Orb}(x)|$.

(a) Prove that the symmetric group S_n acts on the set $P^{(n)}$ of all polynomials in n variables $x_1, \ldots, x_n$, if we define $\sigma \cdot f$ to be the polynomial given by

$$(\sigma \cdot f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

for $f \in P^{(n)}$ and $\sigma \in S_n$. Find the orbit of $f = x_1x_2 + x_3x_4 \in P^{(4)}$ under S_4. Find also the order of the stabiliser of f.

(b) Let r, n be fixed positive integers such that $r \leqslant n$. Let B_r be the set of all subsets of size r of the set $\{1, 2, \ldots, n\}$. Show that S_n acts on B_r by defining $\sigma \cdot U$ to be the set $\{\sigma(u) : u \in U\}$, for any $U \in B_r$ and $\sigma \in S_n$. Prove that S_n is transitive in its action on B_r. Find also the size of the stabiliser of $U \in B_r$.

Paper 3, Section II
6D Groups

Let G, H be groups and let $\varphi\colon G \to H$ be a function. What does it mean to say that φ is a *homomorphism* with *kernel* K? Show that if $K = \{e, \xi\}$ has order 2 then $x^{-1}\xi x = \xi$ for each $x \in G$. [If you use any general results about kernels of homomorphisms, then you should prove them.]

Which of the following four statements are true, and which are false? Justify your answers.

(a) There is a homomorphism from the orthogonal group $\mathrm{O}(3)$ to a group of order 2 with kernel the special orthogonal group $\mathrm{SO}(3)$.

(b) There is a homomorphism from the symmetry group S_3 of an equilateral triangle to a group of order 2 with kernel of order 3.

(c) There is a homomorphism from $\mathrm{O}(3)$ to $\mathrm{SO}(3)$ with kernel of order 2.

(d) There is a homomorphism from S_3 to a group of order 3 with kernel of order 2.

Paper 3, Section II
7D Groups

(a) State and prove Lagrange's theorem.

(b) Let G be a group and let H, K be fixed subgroups of G. For each $g \in G$, any set of the form $HgK = \{hgk : h \in H, k \in K\}$ is called an (H, K) *double coset*, or simply a double coset if H and K are understood. Prove that every element of G lies in some (H, K) double coset, and that any two (H, K) double cosets either coincide or are disjoint.

Let G be a finite group. Which of the following three statements are true, and which are false? Justify your answers.

(i) The size of a double coset divides the order of G.

(ii) Different double cosets for the same pair of subgroups have the same size.

(iii) The number of double cosets divides the order of G.

Paper 3, Section II

8D Groups

(a) Let G be a non-trivial group and let $Z(G) = \{h \in G : gh = hg \text{ for all } g \in G\}$. Show that $Z(G)$ is a normal subgroup of G. If the order of G is a power of a prime, show that $Z(G)$ is non-trivial.

(b) The *Heisenberg group* H is the set of all 3×3 matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix},$$

with $x, y, z \in \mathbb{R}$. Show that H is a subgroup of the group of non-singular real matrices under matrix multiplication.

Find $Z(H)$ and show that $H/Z(H)$ is isomorphic to $\mathbb{R}^2$ under vector addition.

(c) For p prime, the *modular Heisenberg group* H_p is defined as in (b), except that x, y and z now lie in the field of p elements. Write down $|H_p|$. Find both $Z(H_p)$ and $H_p/Z(H_p)$ in terms of generators and relations.

Paper 3, Section I

1D Groups

Let $G = \mathbb{Q}$ be the rational numbers, with addition as the group operation. Let x, y be non-zero elements of G, and let $N \leqslant G$ be the subgroup they generate. Show that N is isomorphic to $\mathbb{Z}$.

Find non-zero elements $x, y \in \mathbb{R}$ which generate a subgroup that is not isomorphic to $\mathbb{Z}$.

Paper 3, Section I

2D Groups

Let G be a group, and suppose the centre of G is trivial. If p divides $|G|$, show that G has a non-trivial conjugacy class whose order is prime to p.

Paper 3, Section II

5D Groups

Let S_n be the group of permutations of $\{1, \ldots, n\}$, and suppose n is even, $n \geqslant 4$.

Let $g = (1\,2) \in S_n$, and $h = (1\,2)(3\,4) \ldots (n{-}1\;\, n) \in S_n$.

(i) Compute the centraliser of g, and the orders of the centraliser of g and of the centraliser of h.

(ii) Now let $n = 6$. Let G be the group of all symmetries of the cube, and X the set of faces of the cube. Show that the action of G on X makes G isomorphic to the centraliser of h in S_6. [*Hint: Show that* $-1 \in G$ *permutes the faces of the cube according to* h.]

Show that G is also isomorphic to the centraliser of g in S_6.

Paper 3, Section II

6D Groups

Let p be a prime number. Let G be a group such that every non-identity element of G has order p.

(i) Show that if $|G|$ is finite, then $|G| = p^n$ for some n. [You must prove any theorems that you use.]

(ii) Show that if $H \leqslant G$, and $x \notin H$, then $\langle x \rangle \cap H = \{1\}$.

Hence show that if G is abelian, and $|G|$ is finite, then $G \simeq C_p \times \cdots \times C_p$.

(iii) Let G be the set of all 3×3 matrices of the form

$$\begin{pmatrix} 1 & a & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix},$$

where $a, b, x \in \mathbb{F}_p$ and $\mathbb{F}_p$ is the field of integers modulo p. Show that every non-identity element of G has order p if and only if $p > 2$. [You may assume that G is a subgroup of the group of all 3×3 invertible matrices.]

Paper 3, Section II

7D Groups

Let p be a prime number, and $G = GL_2(\mathbb{F}_p)$, the group of 2×2 invertible matrices with entries in the field $\mathbb{F}_p$ of integers modulo p.

The group G acts on $X = \mathbb{F}_p \cup \{\infty\}$ by Möbius transformations,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

(i) Show that given any distinct $x, y, z \in X$ there exists $g \in G$ such that $g \cdot 0 = x$, $g \cdot 1 = y$ and $g \cdot \infty = z$. How many such g are there?

(ii) G acts on $X \times X \times X$ by $g \cdot (x, y, z) = (g \cdot x, g \cdot y, g \cdot z)$. Describe the orbits, and for each orbit, determine its stabiliser, and the orders of the orbit and stabiliser.

Paper 3, Section II

8D Groups

(a) Let G be a group, and N a subgroup of G. Define what it means for N to be normal in G, and show that if N is normal then G/N naturally has the structure of a group.

(b) For each of (i)–(iii) below, give an example of a non-trivial finite group G and non-trivial normal subgroup $N \leqslant G$ satisfying the stated properties.

(i) $G/N \times N \simeq G$.

(ii) There is no group homomorphism $G/N \to G$ such that the composite $G/N \to G \to G/N$ is the identity.

(iii) There is a group homomorphism $i\colon G/N \to G$ such that the composite $G/N \to G \to G/N$ is the identity, but the map

$$G/N \times N \to G, \qquad (gN, n) \mapsto i(gN)n$$

is not a group homomorphism.

Show also that for any $N \leqslant G$ satisfying (iii), this map is always a bijection.

Paper 3, Section I
1D Groups

State Lagrange's Theorem.

Let G be a finite group, and H and K two subgroups of G such that

(i) the orders of H and K are coprime;

(ii) every element of G may be written as a product hk, with $h \in H$ and $k \in K$;

(iii) both H and K are normal subgroups of G.

Prove that G is isomorphic to $H \times K$.

Paper 3, Section I
2D Groups

Define what it means for a group to be *cyclic*, and for a group to be *abelian*. Show that every cyclic group is abelian, and give an example to show that the converse is false.

Show that a group homomorphism from the cyclic group C_n of order n to a group G determines, and is determined by, an element g of G such that $g^n = 1$.

Hence list all group homomorphisms from C_4 to the symmetric group S_4.

Paper 3, Section II
5D Groups

(a) Let G be a finite group. Show that there exists an injective homomorphism $G \to Sym(X)$ to a symmetric group, for some set X.

(b) Let H be the full group of symmetries of the cube, and X the set of edges of the cube.

Show that H acts transitively on X, and determine the stabiliser of an element of X. Hence determine the order of H.

Show that the action of H on X defines an injective homomorphism $H \to Sym(X)$ to the group of permutations of X, and determine the number of cosets of H in $Sym(X)$.

Is H a normal subgroup of $Sym(X)$? Prove your answer.

Paper 3, Section II

6D Groups

(a) Let p be a prime, and let $G = SL_2(p)$ be the group of 2×2 matrices of determinant 1 with entries in the field $\mathbb{F}_p$ of integers mod p.

(i) Define the action of G on $X = \mathbb{F}_p \cup \{\infty\}$ by Möbius transformations. [You need not show that it is a group action.]

State the orbit-stabiliser theorem.

Determine the orbit of ∞ and the stabiliser of ∞. Hence compute the order of $SL_2(p)$.

(ii) Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}.$$

Show that A is conjugate to B in G if $p = 11$, but not if $p = 5$.

(b) Let G be the set of all 3×3 matrices of the form

$$\begin{pmatrix} 1 & a & x \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

where $a, b, x \in \mathbb{R}$. Show that G is a subgroup of the group of all invertible real matrices.

Let H be the subset of G given by matrices with $a = 0$. Show that H is a normal subgroup, and that the quotient group G/H is isomorphic to $\mathbb{R}$.

Determine the centre $Z(G)$ of G, and identify the quotient group $G/Z(G)$.

Paper 3, Section II
7D Groups

(a) Let G be the dihedral group of order $4n$, the symmetry group of a regular polygon with $2n$ sides.

Determine all elements of order 2 in G. For each element of order 2, determine its conjugacy class and the smallest normal subgroup containing it.

(b) Let G be a finite group.

(i) Prove that if H and K are subgroups of G, then $K \cup H$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.

(ii) Let H be a proper subgroup of G, and write $G \setminus H$ for the elements of G not in H. Let K be the subgroup of G generated by $G \setminus H$.

Show that $K = G$.

Paper 3, Section II
8D Groups

Let p be a prime number.

Prove that every group whose order is a power of p has a non-trivial centre.

Show that every group of order p^2 is abelian, and that there are precisely two of them, up to isomorphism.

Paper 3, Section I

1E Groups

State Lagrange's Theorem. Deduce that if G is a finite group of order n, then the order of every element of G is a divisor of n.

Let G be a group such that, for every $g \in G$, $g^2 = e$. Show that G is abelian. Give an example of a non-abelian group in which every element g satisfies $g^4 = e$.

Paper 3, Section I

2E Groups

What is a *cycle* in the symmetric group S_n? Show that a cycle of length p and a cycle of length q in S_n are conjugate if and only if $p = q$.

Suppose that p is odd. Show that any two p-cycles in A_{p+2} are conjugate. Are any two 3-cycles in A_4 conjugate? Justify your answer.

Paper 3, Section II

5E Groups

(i) State and prove the Orbit-Stabilizer Theorem.

Show that if G is a finite group of order n, then G is isomorphic to a subgroup of the symmetric group S_n.

(ii) Let G be a group acting on a set X with a single orbit, and let H be the stabilizer of some element of X. Show that the homomorphism $G \to \mathrm{Sym}(X)$ given by the action is injective if and only if the intersection of all the conjugates of H equals $\{e\}$.

(iii) Let Q_8 denote the quaternion group of order 8. Show that for every $n < 8$, Q_8 is not isomorphic to a subgroup of S_n.

Paper 3, Section II

6E Groups

Let G be $SL_2(\mathbb{R})$, the groups of *real* 2×2 matrices of determinant 1, acting on $\mathbb{C} \cup \{\infty\}$ by Möbius transformations.

For each of the points 0, i, $-i$, compute its stabilizer and its orbit under the action of G. Show that G has exactly 3 orbits in all.

Compute the orbit of i under the subgroup

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \,\middle|\, a,\ b,\ d \in \mathbb{R},\ ad = 1 \right\} \subset G\,.$$

Deduce that every element g of G may be expressed in the form $g = hk$ where $h \in H$ and for some $\theta \in \mathbb{R}$,

$$k = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\,.$$

How many ways are there of writing g in this form?

Paper 3, Section II

7E Groups

Let $\mathbb{F}_p$ be the set of (residue classes of) integers mod p, and let

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,\, b,\, c,\, d \in \mathbb{F}_p,\, ad - bc \neq 0 \right\}$$

Show that G is a group under multiplication. [You may assume throughout this question that multiplication of matrices is associative.]

Let X be the set of 2-dimensional column vectors with entries in $\mathbb{F}_p$. Show that the mapping $G \times X \to X$ given by

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \right) \mapsto \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

is a group action.

Let $g \in G$ be an element of order p. Use the orbit-stabilizer theorem to show that there exist $x,\, y \in \mathbb{F}_p$, not both zero, with

$$g \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} .$$

Deduce that g is conjugate in G to the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} .$$

Paper 3, Section II

8E Groups

Let p be a prime number, and a an integer with $1 \leqslant a \leqslant p-1$. Let G be the Cartesian product

$$G = \{ (x,u) \mid x \in \{0,1,\ldots,p-2\},\ u \in \{0,1,\ldots,p-1\} \}$$

Show that the binary operation

$$(x,u) * (y,v) = (z,w)$$

where

$$\begin{aligned} z &\equiv x + y \pmod{p-1} \\ w &\equiv a^y u + v \pmod{p} \end{aligned}$$

makes G into a group. Show that G is abelian if and only if $a = 1$.

Let H and K be the subsets

$$H = \{ (x,0) \mid x \in \{0,1,\ldots,p-2\} \}, \qquad K = \{ (0,u) \mid u \in \{0,1,\ldots,p-1\} \}$$

of G. Show that K is a normal subgroup of G, and that H is a subgroup which is normal if and only if $a = 1$.

Find a homomorphism from G to another group whose kernel is K.

Paper 3, Section I

1D Groups

(a) Let G be the group of symmetries of the cube, and consider the action of G on the set of edges of the cube. Determine the stabilizer of an edge and its orbit. Hence compute the order of G.

(b) The symmetric group S_n acts on the set $X = \{1, \ldots, n\}$, and hence acts on $X \times X$ by $g(x, y) = (gx, gy)$. Determine the orbits of S_n on $X \times X$.

Paper 3, Section I

2D Groups

State and prove Lagrange's Theorem.

Show that the dihedral group of order $2n$ has a subgroup of order k for every k dividing $2n$.

Paper 3, Section II

5D Groups

(a) Let G be a finite group, and let $g \in G$. Define the *order* of g and show it is finite. Show that if g is conjugate to h, then g and h have the same order.

(b) Show that every $g \in S_n$ can be written as a product of disjoint cycles. For $g \in S_n$, describe the order of g in terms of the cycle decomposition of g.

(c) Define the alternating group A_n. What is the condition on the cycle decomposition of $g \in S_n$ that characterises when $g \in A_n$?

(d) Show that, for every n, A_{n+2} has a subgroup isomorphic to S_n.

Paper 3, Section II
6D Groups

(a) Let

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1, \quad a, b, c, d \in \mathbb{Z} \right\},$$

and, for a prime p, let

$$SL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1, \quad a, b, c, d \in \mathbb{F}_p \right\},$$

where $\mathbb{F}_p$ consists of the elements $0, 1, \ldots, p-1$, with addition and multiplication mod p.

Show that $SL_2(\mathbb{Z})$ and $SL_2(\mathbb{F}_p)$ are groups under matrix multiplication.

[*You may assume that matrix multiplication is associative, and that the determinant of a product equals the product of the determinants.*]

By defining a suitable homomorphism from $SL_2(\mathbb{Z}) \to SL_2(\mathbb{F}_5)$, show that

$$\left\{ \begin{pmatrix} 1+5a & 5b \\ 5c & 1+5d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid a, b, c, d \in \mathbb{Z} \right\}$$

is a normal subgroup of $SL_2(\mathbb{Z})$.

(b) Define the group $GL_2(\mathbb{F}_5)$, and show that it has order 480. By defining a suitable homomorphism from $GL_2(\mathbb{F}_5)$ to another group, which should be specified, show that the order of $SL_2(\mathbb{F}_5)$ is 120.

Find a subgroup of $GL_2(\mathbb{F}_5)$ of index 2.

Paper 3, Section II
7D Groups

(a) State the orbit–stabilizer theorem.

Let a group G act on itself by conjugation. Define the centre $Z(G)$ of G, and show that $Z(G)$ consists of the orbits of size 1. Show that $Z(G)$ is a normal subgroup of G.

(b) Now let $|G| = p^n$, where p is a prime and $n \geqslant 1$. Show that if G acts on a set X, and Y is an orbit of this action, then either $|Y| = 1$ or p divides $|Y|$.

Show that $|Z(G)| > 1$.

By considering the set of elements of G that commute with a fixed element x not in $Z(G)$, show that $Z(G)$ cannot have order p^{n-1}.

Paper 3, Section II

8D Groups

(a) Let G be a finite group and let H be a subgroup of G. Show that if $|G| = 2|H|$ then H is normal in G.

Show that the dihedral group D_{2n} of order $2n$ has a normal subgroup different from both D_{2n} and $\{e\}$.

For each integer $k \geqslant 3$, give an example of a finite group G, and a subgroup H, such that $|G| = k|H|$ and H is not normal in G.

(b) Show that A_5 is a simple group.

Paper 3, Section I
1D Groups

Write down the matrix representing the following transformations of $\mathbb{R}^3$:

(i) clockwise rotation of 45° around the x axis,

(ii) reflection in the plane $x = y$,

(iii) the result of first doing (i) and then (ii).

Paper 3, Section I
2D Groups

Express the element $(123)(234)$ in S_5 as a product of disjoint cycles. Show that it is in A_5 . Write down the elements of its conjugacy class in A_5 .

Paper 3, Section II
5D Groups

(i) State the orbit-stabilizer theorem.

Let G be the group of rotations of the cube, X the set of faces. Identify the stabilizer of a face, and hence compute the order of G.

Describe the orbits of G on the set $X \times X$ of pairs of faces.

(ii) Define what it means for a subgroup N of G to be *normal.* Show that G has a normal subgroup of order 4.

Paper 3, Section II
6D Groups

State Lagrange's theorem. Let p be a prime number. Prove that every group of order p is cyclic. Prove that every abelian group of order p^2 is isomorphic to either $C_p \times C_p$ or C_{p^2}.

Show that D_{12}, the dihedral group of order 12, is not isomorphic to the alternating group A_4.

Paper 3, Section II
7D Groups

Let G be a group, X a set on which G acts transitively, B the stabilizer of a point $x \in X$.

Show that if $g \in G$ stabilizes the point $y \in X$, then there exists an $h \in G$ with $hgh^{-1} \in B$.

Let $G = SL_2(\mathbb{C})$, acting on $\mathbb{C} \cup \{\infty\}$ by Möbius transformations. Compute $B = G_\infty$, the stabilizer of ∞. Given

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

compute the set of fixed points $\Big\{x \in \mathbb{C} \cup \{\infty\} \,\Big|\, gx = x\Big\}$.

Show that every element of G is conjugate to an element of B.

Paper 3, Section II
8D Groups

Let G be a finite group, X the set of proper subgroups of G. Show that conjugation defines an action of G on X.

Let B be a proper subgroup of G. Show that the orbit of G on X containing B has size at most the index $|G : B|$. Show that there exists a $g \in G$ which is not conjugate to an element of B.

Paper 3, Section I

1D Groups

Show that every orthogonal 2×2 matrix R is the product of at most two reflections in lines through the origin.

Every isometry of the Euclidean plane $\mathbb{R}^2$ can be written as the composition of an orthogonal matrix and a translation. Deduce from this that every isometry of the Euclidean plane $\mathbb{R}^2$ is a product of reflections.

Give an example of an isometry of $\mathbb{R}^2$ that is not the product of fewer than three reflections. Justify your answer.

Paper 3, Section I

2D Groups

State and prove Lagrange's theorem. Give an example to show that an integer k may divide the order of a group G without there being a subgroup of order k.

Paper 3, Section II

5D Groups

State and prove the orbit–stabilizer theorem.

Let G be the group of all symmetries of a regular octahedron, including both orientation-preserving and orientation-reversing symmetries. How many symmetries are there in the group G? Let D be the set of straight lines that join a vertex of the octahedron to the opposite vertex. How many lines are there in the set D? Identify the stabilizer in G of one of the lines in D.

Paper 3, Section II

6D Groups

Let $S(X)$ denote the group of permutations of a finite set X. Show that every permutation $\sigma \in S(X)$ can be written as a product of disjoint cycles. Explain briefly why two permutations in $S(X)$ are conjugate if and only if, when they are written as the product of disjoint cycles, they have the same number of cycles of length n for each possible value of n.

Let $\ell(\sigma)$ denote the number of disjoint cycles, including 1-cycles, required when σ is written as a product of disjoint cycles. Let τ be a transposition in $S(X)$ and σ any permutation in $S(X)$. Prove that $\ell(\tau\sigma) = \ell(\sigma) \pm 1$.

Paper 3, Section II

7D Groups

Define the *cross-ratio* $[a_0, a_1, a_2, z]$ of four points a_0, a_1, a_2, z in $\mathbb{C} \cup \{\infty\}$, with a_0, a_1, a_2 distinct.

Let a_0, a_1, a_2 be three distinct points. Show that, for every value $w \in \mathbb{C} \cup \{\infty\}$, there is a unique point $z \in \mathbb{C} \cup \{\infty\}$ with $[a_0, a_1, a_2, z] = w$. Let S be the set of points z for which the cross-ratio $[a_0, a_1, a_2, z]$ is in $\mathbb{R} \cup \{\infty\}$. Show that S is either a circle or else a straight line together with ∞.

A map $J : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ satisfies

$$[a_0, a_1, a_2, J(z)] = \overline{[a_0, a_1, a_2, z]}$$

for each value of z. Show that this gives a well-defined map J with J^2 equal to the identity.

When the three points a_0, a_1, a_2 all lie on the real line, show that J must be the conjugation map $J : z \mapsto \overline{z}$. Deduce from this that, for any three distinct points a_0, a_1, a_2, the map J depends only on the circle (or straight line) through a_0, a_1, a_2 and not on their particular values.

Paper 3, Section II

8D Groups

What does it mean to say that a subgroup K of a group G is *normal*?

Let $\phi : G \to H$ be a group homomorphism. Is the kernel of ϕ always a subgroup of G? Is it always a normal subgroup? Is the image of ϕ always a subgroup of H? Is it always a normal subgroup? Justify your answers.

Let $\mathrm{SL}(2, \mathbb{Z})$ denote the set of 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. Show that $\mathrm{SL}(2, \mathbb{Z})$ is a group under matrix multiplication. Similarly, when $\mathbb{Z}_2$ denotes the integers modulo 2, let $\mathrm{SL}(2, \mathbb{Z}_2)$ denote the set of 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbb{Z}_2$ and $ad - bc = 1$. Show that $\mathrm{SL}(2, \mathbb{Z}_2)$ is also a group under matrix multiplication.

Let $f : \mathbb{Z} \to \mathbb{Z}_2$ send each integer to its residue modulo 2. Show that

$$\phi : \mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}_2) \ ; \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} f(a) & f(b) \\ f(c) & f(d) \end{pmatrix}$$

is a group homomorphism. Show that the image of ϕ is isomorphic to a permutation group.

3/I/1E **Groups**

Define the *signature* $\epsilon(\sigma)$ of a permutation $\sigma \in S_n$, and show that the map $\epsilon : S_n \to \{-1, 1\}$ is a homomorphism.

Define the *alternating group* A_n, and prove that it is a subgroup of S_n. Is A_n a normal subgroup of S_n? Justify your answer.

3/I/2E **Groups**

What is the *orthogonal group* $O(n)$? What is the *special orthogonal group* $SO(n)$?

Show that every element of the special orthogonal group $SO(3)$ has an eigenvector with eigenvalue 1. Is this also true for every element of the orthogonal group $O(3)$? Justify your answer.

3/II/5E **Groups**

For a normal subgroup H of a group G, explain carefully how to make the set of (left) cosets of H into a group.

For a subgroup H of a group G, show that the following are equivalent:

(i) H is a normal subgroup of G;

(ii) there exist a group K and a homomorphism $\theta : G \to K$ such that H is the kernel of θ.

Let G be a finite group that has a proper subgroup H of index n (in other words, $|H| = |G|/n$). Show that if $|G| > n!$ then G cannot be simple. [Hint: Let G act on the set of left cosets of H by left multiplication.]

3/II/6E **Groups**

Prove that two elements of S_n are conjugate if and only if they have the same cycle type.

Describe (without proof) a necessary and sufficient condition for a permutation $\sigma \in A_n$ to have the same conjugacy class in A_n as it has in S_n .

For which $\sigma \in S_n$ is σ conjugate (in S_n) to σ^2 ?

For every $\sigma \in A_5$, show that σ is conjugate to σ^{-1} (in A_5). Exhibit a positive integer n and a $\sigma \in A_n$ such that σ is not conjugate to σ^{-1} (in A_n).

3/II/7E **Groups**

Show that every Möbius map may be expressed as a composition of maps of the form $z \mapsto z+a$, $z \mapsto \lambda z$ and $z \mapsto 1/z$ (where a and λ are complex numbers).

Which of the following statements are true and which are false? Justify your answers.

(i) Every Möbius map that fixes ∞ may be expressed as a composition of maps of the form $z \mapsto z+a$ and $z \mapsto \lambda z$ (where a and λ are complex numbers).

(ii) Every Möbius map that fixes 0 may be expressed as a composition of maps of the form $z \mapsto \lambda z$ and $z \mapsto 1/z$ (where λ is a complex number).

(iii) Every Möbius map may be expressed as a composition of maps of the form $z \mapsto z+a$ and $z \mapsto 1/z$ (where a is a complex number).

3/II/8E **Groups**

State and prove the orbit–stabilizer theorem. Deduce that if x is an element of a finite group G then the order of x divides the order of G .

Prove Cauchy's theorem, that if p is a prime dividing the order of a finite group G then G contains an element of order p .

For which positive integers n does there exist a group of order n in which every element (apart from the identity) has order 2?

Give an example of an infinite group in which every element (apart from the identity) has order 2.