

**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

Linear Algebra and Groups

Date: Thursday, May 9, 2024

Time: 14:00 – 17:00 (BST)

Time Allowed: 3 hours

This paper has 6 Questions.

Please Answer Each Question in a Separate 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

1. (a) Let $n \in \mathbb{N}$ and let $A, B, C \in M_{n \times n}(F)$ be $n \times n$ matrices with entries in a field F . From first principles (i.e. using the definition of matrix multiplication and addition) prove carefully that $A(B + C) = AB + AC$.

You may of course use the field axioms for F . (4 marks)

- (b) For each of the following statements say it is TRUE or FALSE, give a proof or counter example.

If you say it is TRUE you need to prove it for all $n \in \mathbb{N}$ (over any arbitrary field F), if you say it is FALSE you just need to find a counterexample for some n (and some field F).

Let F be a field. For all $n \in \mathbb{N}$ and all $A, B \in M_{n \times n}(F)$:

- (i) if A and B have inverses then so does $A + B$, (2 marks)
 - (ii) if A and B have inverses then so does AB , (2 marks)
 - (iii) if $AB = BA$ then either A or B is diagonal, (2 marks)
 - (iv) if A is diagonal then $AB = BA$. (2 marks)
- (c) Let $\mathbb{A}$ be a set of matrices that is closed under multiplication. The centre of $\mathbb{A}$ is defined to be the subset of matrices in $\mathbb{A}$ which commute with all elements of $\mathbb{A}$. It is denoted

$$Z(\mathbb{A}) = \{A \in \mathbb{A} : \forall B \in \mathbb{A}, AB = BA\}.$$

Find $Z(\mathbb{A})$ for the following definitions of the set $\mathbb{A}$.

- (i) $\mathbb{A} = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$, (1 mark)
- (ii) $\mathbb{A} = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$, (3 marks)
- (iii) For $n \in \mathbb{N}$, $\mathbb{A} = \{A = (a_{ij}) \in M_{n \times n}(\mathbb{R}) : a_{ij} = 0 \text{ if } i \geq j\}$, i.e. the set of strictly upper-triangular matrices.
Hint: Given a matrix A , you may assume without proof that $f_A(B) = AB - BA$ is a linear transformation. Then A is such that $f_A = 0$ if and only if it is zero on all the standard basis elements. Also note that part (ii) is the case where $n = 2$. (4 marks)

(Total: 20 marks)

2. Let A, B, C be subspaces of a vector space V over a field F .

(a) Show that $A \cap B$ is a subspace of V . (3 marks)

(b) Suppose that A, B, C are finite dimensional and that $C \subseteq B$. Show that:

(i)

$$\dim(A \cap B) \geq \dim(A \cap C)$$

(3 marks)

(ii)

$$\dim(A \cap B) = \dim(A \cap C) \text{ if and only if } A \cap B \subseteq C$$

(4 marks)

(c) Show that V is infinite dimensional if and only if for any A, B and C finite dimensional subspaces of V with $C \subseteq B$ there is an A' with $\dim(A') = \dim(A)$, $\dim(A' \cap B) = \dim(A' \cap C)$, and $A \cap C = A' \cap C$. (7 marks)

(d) Suppose that:

$$V = \mathbb{R}[x]$$

$$A = \{a(x+1) + bx^2 : a, b \in \mathbb{R}\}$$

$$B = \{c + dx + ex^2 : c, d, e \in \mathbb{R}\}$$

$$C = \{rx^2 : r \in \mathbb{R}\}$$

Find a suitable candidate for A' in part (c) for this example. How many possibilities for A' are there in this case? (3 marks)

(Total: 20 marks)

3. (a) Let $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ be the linear transformation defined by

$$f \begin{pmatrix} x \\ y \\ z \end{pmatrix} = x + y + z.$$

(i) Find a basis for $\ker f$ (where $\ker f$ denotes the kernel of f). Justify your answer. (4 marks)

(ii) Find an isomorphism from $\mathbb{R}^2$ to $\ker f$. (3 marks)

(iii) Find $\dim(\operatorname{Im} f)$ (that is, the dimension of the image of f) (1 mark)

(b) Let V be a vector space over $\mathbb{R}$. We call a function $\rho : V \times V \rightarrow \mathbb{R}$ *pink* if it satisfies the properties

$$\rho(u + v, w) = \rho(u, w) + \rho(v, w)$$

$$\rho(u, v + w) = \rho(u, v) + \rho(u, w)$$

$$\rho(u, \lambda w) = \lambda \rho(u, w)$$

$$\rho(\lambda u, w) = \lambda \rho(u, w)$$

for all $u, v, w \in V$ and $\lambda \in \mathbb{R}$. We call a function *very pink* if it is pink and $\rho(v, v) = 0$ for all $v \in V$.

(i) Show that for a very pink function ρ we have that $\rho(v, w) = -\rho(w, v)$ for all $v, w \in V$.
HINT: Consider $\rho(v + w, v + w)$. (3 marks)

(ii) Is the function $\rho : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ such that $\rho(v, w) = v^T w$ pink? Is it very pink? Justify your answers. (4 marks)

(iii) Let $V = \mathbb{R}^2$. Find a matrix $A \in SL_2(\mathbb{R})$ (that is, $A \in M_{2 \times 2}(\mathbb{R})$ with $\det(A) = 1$) such that $\rho : V \times V \rightarrow \mathbb{R}$ defined as $\rho(v, w) = v^T A w$ is very pink. (5 marks)

(Total: 20 marks)

4. (a) Let $V = \mathbb{R}^3$ and $T : V \rightarrow V$ be the linear transformation defined by

$$T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ 6x_1 + 3x_2 + 2x_3 \\ -12x_1 - 4x_2 - 3x_3 \end{pmatrix}.$$

Let $E = \{e_1, e_2, e_3\}$ be the standard basis of $\mathbb{R}^3$ and $A = [T]_E$.

- (i) Write down A , explaining your answer. (2 marks)
- (ii) Find the eigenspaces of T (show the details of your calculation), and determine whether T is diagonalisable or not (explain your answer). (6 marks)
- (b) Let $\{a_i\}_{i \in \mathbb{N}}$, $\{b_i\}_{i \in \mathbb{N}}$, and $\{c_i\}_{i \in \mathbb{N}}$ be three sequences of real numbers. Let $n \in \mathbb{N} \setminus \{0\}$. We define $T_n \in M_{n \times n}(\mathbb{R})$ by

$$T_1 = a_1, \quad T_n = \begin{pmatrix} a_1 & b_1 & 0 & \cdots & 0 & 0 \\ c_1 & a_2 & b_2 & \cdots & 0 & 0 \\ 0 & c_2 & a_3 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & c_{n-1} & a_n \end{pmatrix} \quad \text{for } n \geq 2.$$

(Where only the entries on the diagonal and those adjacent to it are non-zero.)

- (i) Define $d_n = \det(T_n)$. For $n > 2$, express d_n as a recursive formula, that is as an expression in terms of $d_1, \dots, d_{n-1}$. (5 marks)
- (ii) Assume there are $b, c \in \mathbb{R}$ with $b \neq c$ and such that $a_i = b + c$, $b_i = b$ and $c_i = c$ for all $i \in \mathbb{N}$. Find a closed form expression for d_n in terms of b and c by diagonalising a 2×2 matrix. (7 marks)

(Total: 20 marks)

5. (a) Give the definition of a *cycle* in S_n . (2 marks)

(b) Let $\sigma = (1\ 2\ 3\ 4)$ and consider $\tau = (1\ 4)(2\ 3)$ be permutations S_4 . Define the set

$$D := \{\sigma^i, \sigma^i \circ \tau \mid i \in \{0, \dots, 3\}\}.$$

(i) Write the elements of D as products of disjoint cycles. How many elements does D have? (Justify your answer.) (3 marks)

(ii) Show that $\sigma\tau = \tau\sigma^{-1}$ and $\tau\sigma^n\tau^{-1} = \sigma^{-n}$, for all $n \in \{1, \dots, 4\}$. (3 marks)

(iii) Use the subgroup test to prove that D is a subgroup of S_4 . (You are not allowed to use any results about the dihedral group for this part.) (5 marks)

(c) Let $A \in M_{n \times n}(\mathbb{R}^n)$. Consider the group $(\mathbb{R}^n, +)$ and its subgroup

$$W = \{w \in \mathbb{R}^n \mid Aw = 0\} \leq (\mathbb{R}^n, +).$$

Fix $b \in \mathbb{R}^n$. Show that the set of inhomogeneous solutions

$$U = \{x \in \mathbb{R}^n \mid Ax = b\}$$

is either empty or a coset of W by some $u \in (\mathbb{R}^n, +)$. (4 marks)

(d) Let G be a finite group and let H and K be subgroups with relatively prime order. Show that $H \cap K = \{e\}$, where e is the identity of G . (3 marks)

(Total: 20 marks)

6. (a) For each of the following definitions of the group G determine if G is cyclic. Justify your answers.
- (i) $G = (\mathbb{Z}, +)$, where $+$ is the usual addition in $\mathbb{Z}$. (1 mark)
 - (ii) $G = (\mathbb{Q}, +)$, where $+$ is the usual addition in $\mathbb{Q}$. (2 marks)
 - (iii) $G = (M_{2 \times 2}(\mathbb{R}), +)$, where $+$ denotes the usual matrix addition. (2 marks)
- (b) Let G, H be groups and let $\varphi : G \rightarrow H$ be a homomorphism. Suppose G is cyclic. Prove that $\text{Im } \varphi$ is cyclic. (3 marks)
- (c) Let $p \in \mathbb{N}$ be a prime number and let G be a group of order p . Let H be a group with identity e_H and let $\varphi : G \rightarrow H$ be a homomorphism. Suppose that there is $g \in G$ such that $\varphi(g) \neq e_H$. Prove that φ is injective. (5 marks)
- (d) Let G be a group. Define

$$\text{Aut}(G) = \{\varphi : G \longrightarrow G \mid \varphi \text{ is an isomorphism}\}.$$

- (i) Prove that if $\varphi \in \text{Aut}(G)$ then $\varphi^{-1} \in \text{Aut}(G)$, where φ^{-1} is the inverse function of φ . (1 mark)
- (ii) Prove that, for all $\varphi_1, \varphi_2 \in \text{Aut}(G)$, $\varphi_1 \circ \varphi_2 \in \text{Aut}(G)$ where $\circ$ is the composition of functions. (1 mark)
- (iii) Hence, or otherwise, conclude that $(\text{Aut}(G), \circ)$ is a group. (1 mark)
- (iv) Consider the following subset of G :

$$Z(G) = \{x \in G \mid gx = xg \text{ for all } g \in G\}.$$

Find a homomorphism $C : G \rightarrow \text{Aut}(G)$ such that $Z(G) = \ker C$. (Justify your answer.) (4 marks)

(Total: 20 marks)

Solutions

1. (a) We write $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$ and $C = (c_{ij})_{ij}$. For all $i, j \in \{1, \dots, n\}$, let $d_{ij} = a_{ij} + b_{ij}$.
By definition of matrix addition

$$A + B = (d_{ij})_{ij}.$$

On the one hand, by definition of matrix multiplication

$$\begin{aligned} C(A + B) &= \left(\sum_{k=1}^n c_{ik} d_{kj} \right)_{ij} \\ &= \left(\sum_{k=1}^n c_{ik} (a_{kj} + b_{kj}) \right)_{ij} \\ &= \left(\sum_{k=1}^n c_{ik} a_{kj} + \sum_{k=1}^n c_{ik} b_{kj} \right)_{ij} \end{aligned}$$

where the last equality holds by the distributive law in F .

On the other hand, the definition of matrix multiplication gives that

$$CA = \left(\sum_{k=1}^n c_{ik} a_{kj} \right)_{ij}, \quad CB = \left(\sum_{k=1}^n c_{ik} b_{kj} \right)_{ij}.$$

Thus by definition of matrix addition we get

$$CA + CB = \left(\sum_{k=1}^n c_{ik} a_{kj} + \sum_{k=1}^n c_{ik} b_{kj} \right)_{ij}.$$

We conclude that $C(A + B) = CA + CB$ because we have proved that, for all $i, j \in \{1, \dots, n\}$, the ij -th entry of $C(A + B)$ is equal to the ij -th entry of $CA + CB$.

(4 marks)Cat A Seen

- (b) (i) This is False. Take $A = I_n$ and $B = -I_n$ for a counter example: I_n is invertible (with inverse I_n) and $-I_n$ is also invertible (with inverse $-I_n$), but their sum is the zero matrix which is not invertible (its rank is 0 which is less than n).

(2 marks)Cat A Seen

- (ii) This is True. Indeed, suppose that both A and B have inverses. This means exactly that there exist $A^{-1}, B^{-1} \in M_{n \times n}(F)$ such that

$$AA^{-1} = A^{-1}A = I_n = BB^{-1} = B^{-1}B.$$

By associativity of the matrix product, it follows that

$$\begin{aligned} (AB)(B^{-1}A^{-1}) &= A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n \\ (B^{-1}A^{-1})(AB) &= B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n. \end{aligned}$$

Thus AB is invertible. (Some people might use that $\text{GL}_n(F)$ is a group and use a general result for inverses of products in a group, but doing this in detail is not easier than the direct proof.)

(2 marks)Cat A Seen

(iii) This is False. Indeed, for all $n > 1$, if A is not diagonal and $B = A$

$$AB = AA = BA,$$

but neither A or B is diagonal.

(2 marks)Cat B Unseen

(iv) This is false. Let $n = 2$ and let

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

Then A is diagonal but $AB \neq BA$. This counter example works over any field, if the candidate does not specify the field of definition and the counter example works over $\mathbb{R}$, full marks should be awarded.

(2 marks)Cat B Unseen

(c) (i) Let

$$A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

One checks that $AB = BA = A$, thus $Z(\mathbb{A}) = \mathbb{A}$.

(1 mark)Cat A Unseen

(ii) One observes that for all $a, b \in \mathbb{R}$

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Hence, for $A, B \in \mathbb{A}$, $AB = BA$ and therefore $Z(\mathbb{A}) = \mathbb{A}$.

(3 marks)Cat C Unseen

(iii) For $i, j \in \{1, \dots, n\}$, we define e_{ij} to be the matrix with 1 in position (i, j) and zeroes everywhere else. For $A, B \in M_{n \times n}(F)$ we set

$$[A, B] = AB - BA.$$

Then, for $i, j, k, \ell \in \{1, \dots, n\}$,

$$e_{ij}e_{k\ell} = \delta_{jk}e_{i\ell}, \tag{1}$$

where δ_{jk} is the Kronecker delta and is defined as

$$\delta_{jk} = \begin{cases} 1 & j = k \\ 0 & j \neq k. \end{cases}$$

The matrices $e_{k\ell}$ with $k < \ell$ form a basis of the strictly upper-triangular matrices. Moreover, if we fix A , the map $B \mapsto [A, B]$ is linear; therefore, $A \in Z(\mathbb{A})$ if and only if $[A, e_{k\ell}] = 0$ for all $k, \ell \in \{1, \dots, n\}$.

We claim that $Z(\mathbb{A}) = \text{Span}\{e_{1n}\}$. We argue by induction on n . If $n = 1$ the claim holds because we are looking at the set $\mathbb{A} = \{0\}$. If $n = 2$ we showed the claim in the previous part of this question. Suppose that $n \geq 3$. If $k > 1$ and we remove the last row

and the last column of from $e_{k\ell}$ we obtain an $(n-1) \times (n-1)$ matrix, so by induction A can only be supported on the last column or in position $(1, n-1)$, by this we mean that

$$A = \sum_{i=1}^n a_{in} e_{in} + a_{1,n-1} e_{1,n-1}$$

for some a_{ij} 's in F . Similarly, if we consider $\ell < n$ and remove the first row and column from $e_{k\ell}$ we obtain that A can only be supported in positions $(1, n-1)$, $(1, n)$, and $(2, n)$.

Suppose that $A = a_{1,n-1} e_{1,n-1} + a_{1,n} e_{1,n} + a_{2,n} e_{2,n}$ with $a_{1,n-1} \neq 0$, then $[A, e_{n-1,n}] \neq 0$ by (1). Similarly, $A \notin Z(\mathbb{A})$ if $a_{2,n} \neq 0$, by considering $[A, e_{1,2}]$. We conclude that $Z(\mathbb{A}) \subseteq \text{Span}\{e_{1n}\}$. Conversely (1) readily implies that $[e_{1n}, B] = 0$ for all B , so we conclude that $Z(\mathbb{A}) = \text{Span}\{e_{1n}\}$.

Alternative solutions are possible: for example for the first of the three above, one could observe that $\mathbb{A}$ is a group of order 2 and therefore abelian (so $Z(\mathbb{A}) = \mathbb{A}$), but one needs to prove carefully that $\mathbb{A}$ is a group.

(4 marks) Cat D Unseen

2. (a) $A \cap B \subseteq V$ and thus we can use the subspace test:

– Non-empty: $0_V \in A$ and $0_V \in B$ as they are subspaces, thus $0_V \in A \cap B$.

(1 mark)Cat A Seen

– Closed under addition: Let $v_1, v_2 \in A \cap B$ then $v_1, v_2 \in A$ and $v_1, v_2 \in B$ so $v_1 + v_2 \in A$ and $v_1 + v_2 \in B$, thus $v_1 + v_2 \in A \cap B$.

(1 mark)Cat A Seen

– Closed under scalar multiplication: Let $v \in A \cap B$ and $\lambda \in F$ then $v \in A$ and $v \in B$ so $\lambda v \in A$, $\lambda v \in B$ so $\lambda v \in A \cap B$.

(1 mark)Cat A Seen

(b) (i) We know that $A \cap B$ is a subspace of V (and thus a vector space in its own right). Also, as $B \supseteq C$ we have $A \cap B \supseteq A \cap C$. Now $A \cap C$ is a subset of $A \cap B$ and thus we can apply the subspace test, and by an argument similar to part (a) we see that $A \cap C$ is a subspace of $A \cap B$. We thus have that $\dim(A \cap B) \geq \dim(A \cap C)$.

(3 marks)Cat B Unseen

(ii) ($\Rightarrow$) Suppose $\dim(A \cap B) = \dim(A \cap C)$. We know from part (i) that $A \cap B \supseteq A \cap C$ as these are both finite dimensional vector spaces we have that if they have equal dimensions then they are equal. I.e $A \cap B = A \cap C \subseteq C$.

(2 marks)Cat C Unseen

($\Leftarrow$) Suppose $A \cap B \subseteq C$, then note also $A \cap B \subseteq A$ so $A \cap B \subseteq A \cap C$. Also as $B \supseteq C$ we have $A \cap B \supseteq A \cap C$ thus $A \cap B = A \cap C$ and so $\dim(A \cap B) = \dim(A \cap C)$.

(2 marks)Cat A Unseen

(c) ($\Leftarrow$) Suppose V is finite dimensional. Then choose $V = A = B$ and $C = \{0_V\}$ then if $\dim(A') = \dim(A)$ we have $\dim(A') = \dim(V)$ and so $A' = V$. However, we then have that $A' \cap C = \{0_V\}$ and thus $\dim(A' \cap B) \neq \dim(A' \cap C)$.

(2 marks)Cat C Unseen

($\Rightarrow$) Suppose V is infinite dimensional. Let A , B and C be finite dimensional subspaces of V with $C \subseteq B$. Suppose $\dim(A) = n$, and that $c_1, \dots, c_m$ is a basis for $A \cap C$. This can be extended to a basis for $A \cap B$, and then to a basis for B , say $c_1, \dots, c_m, b_1, \dots, b_r$.

As V is infinite dimensional we can find $n - m$ linearly independent vectors, $v_{m+1}, \dots, v_n$, in V that are not in the span of $c_1, \dots, c_m, b_1, \dots, b_r$.

(2 marks)Cat D Unseen

Let $A' = \text{Span}\{c_1, \dots, c_m, v_{m+1}, \dots, v_n\}$ then:

– $\dim(A') = n = \dim(A)$.

– $\dim(A' \cap B) = \dim(\text{Span}(c_1, \dots, c_m)) = \dim(A' \cap C)$

– $A' \cap C = \text{Span}(c_1, \dots, c_m) = A' \cap C$

Proof: The first point is obvious, the last two points follow because $A' \cap B = A' \cap C = \text{Span}(c_1, \dots, c_m)$. Clearly $A' \cap B \supseteq A' \cap C \supseteq \text{Span}(c_1, \dots, c_m)$. So it is sufficient to show

$A' \cap B \subseteq \text{Span}(c_1, \dots, c_m)$, suppose $x \in A' \cap B$ then

$$x = \sum_{i=1}^m \lambda_i c_i + \sum_{i=m+1}^n \mu_i v_i = \sum_{i=1}^m \nu_i c_i + \sum_{i=m+1}^r \beta_i b_i$$

So

$$0_V = \sum_{i=1}^m (\lambda_i - \nu_i) c_i + \sum_{i=m+1}^n (-\mu_i) v_i + \sum_{i=m+1}^r (-\beta_i) b_i$$

So as $\{c_1, \dots, c_m, b_1, \dots, b_r, v_{m+1}, \dots, v_n\}$ is linearly independent we have $\lambda_i = \nu_i$ and $\mu_i = \beta_i = 0$ for all i .

Thus $x \in \text{Span}\{c_1, \dots, c_m\}$.

(3 marks)Cat D Unseen

- (d) Now, $\dim(A) = 2$, $A \cap C = C = \text{Span}(x^2)$, by part (c) we need $v \notin \text{Span}(1, x, x^2)$, e.g. $v = x^3$, so let $A' = \text{Span}(x^2, x^3)$.

(2 marks)Cat A Unseen

There are infinitely many possibilities for v , and so infinitely many possibilities for A' .

(1 mark)Cat B Unseen

3. (a) (i) The kernel of f is $\ker f = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : x + y + 1 = 0 \right\}.$

(1 mark) Cat A Seen

One possible basis is $B = \left\{ \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \right\}.$

(1 mark) Cat A Seen

B is linearly independent because if $a \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ then a and b must be zero.

(1 mark) Cat A Seen

Then B is a spanning set, because if $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \ker f$ then we can write

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = x \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$$

since $z = -x - y$.

(1 mark) Cat A Seen

(ii) Consider the map $F : \mathbb{R}^2 \rightarrow \ker f$ such that $F(e_1) = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$ and $F(e_2) = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$. This is a linear map by a Proposition in the notes (5.14). The function $F' : \ker f \rightarrow \mathbb{R}^2$ such that $x \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \end{pmatrix}$ is the inverse of this function, so F is a bijection and hence an isomorphism.

(3 marks) Cat A Seen

(iii) It follows from a(i) and (ii) that the dimension of $\ker f$ is 2 and so by the Rank-Nullity Theorem, $\dim(\text{Im } f) = 1$.

(1 mark) Cat A Seen

(b) (i) Since ρ is a pink function, we have that

$$\rho(v + w, v + w) = \rho(v, v) + \rho(w, w) + \rho(v, w) + \rho(w, v). \quad (2)$$

As ρ is very pink, it is also true that $\rho(v + w, v + w) = \rho(v, v) + \rho(w, w) + \rho(v, w) + \rho(w, v)$. Putting this into (2) we get that

$$\rho(v, w) + \rho(w, v) = 0.$$

Rearranging gives the result.

(3 marks) Cat C Unseen

(ii) We know that $(u + v)^T = u^T + v^T$ and $(\lambda u)^T = \lambda u^T$. Using these we get that

$$\rho(u + v, w) = (u + v)^T w = u^T w + v^T w = \rho(u, w) + \rho(v, w)$$

and

$$\rho(\lambda u, w) = (\lambda u)^T w = \lambda u^T w = \lambda \rho(u, w).$$

The other two conditions are similar. Hence ρ is pink.

(3 marks) Cat B Seen

We show that it is not very pink. Choose $v = e_1$ the first standard basis vector. Then $\rho(e_1, e_1) = e_1^T e_1 = 1$, so ρ is not very pink.

(1 mark) Cat B Seen

(iii) We can choose for example $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Now A is invertible and we can compute using the formula in the notes that $\det(A) = 0 - (-1)1 = 1$, so it is in $SL_2(\mathbb{R})$.

(3 marks) Cat D Unseen

Similarly to 3b(ii) we can show using properties of the transpose and matrix multiplication that ρ is a pink function.

(1 mark) Cat B Seen

To see that ρ is very pink, let $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$. Then

$$\begin{aligned} \rho(v, v) &= v^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} v = \begin{pmatrix} v_1 & v_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \\ &= \begin{pmatrix} -v_2 & v_1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = -v_2 v_1 + v_1 v_2 = 0, \end{aligned}$$

as required.

(1 mark) Cat D Unseen

(Total: 20 marks)

4. (a) (i) The images of the vectors in E are

$$T(e_1) = \begin{pmatrix} 1 \\ 6 \\ -12 \end{pmatrix}, T(e_2) = \begin{pmatrix} 0 \\ 3 \\ -4 \end{pmatrix}, T(e_3) = \begin{pmatrix} 0 \\ 2 \\ -3 \end{pmatrix}.$$

Thus

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 6 & 3 & 2 \\ -12 & -4 & -3 \end{pmatrix}.$$

(2 marks) **Cat A Seen**

- (ii) The characteristic polynomial of A is $\det(XI_3 - A) = (X - 1)^2(X + 1)$. Thus there are two eigenvalues: $1, -1$.

(2 marks) **Cat A Seen**

The eigenspace for 1 is

$$E_1 = \ker(I_3 - A) = \ker \begin{pmatrix} 0 & 0 & 0 \\ -6 & -2 & -2 \\ 12 & 4 & 4 \end{pmatrix} = \text{Span} \left\{ \begin{pmatrix} 1 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix} \right\}.$$

The eigenspace for -1 is

$$E_{-1} = \ker \begin{pmatrix} -2 & 0 & 0 \\ -6 & -4 & -2 \\ 12 & 4 & 2 \end{pmatrix} = \text{Span} \left\{ \begin{pmatrix} 0 \\ -1 \\ 2 \end{pmatrix} \right\}.$$

(3 marks) **Cat A Seen**

There is a basis of $\mathbb{R}^3$ consisting of eigenvectors of A . Hence A is diagonalisable.

(1 mark) **Cat A Seen**

- (b) (i) If $n > 2$, a Laplace expansion along the last row gives that

$$d_n = a_n \cdot d_{n-1} - c_n \det \begin{pmatrix} a_1 & b_1 & 0 & \cdots & 0 & 0 \\ c_1 & a_2 & b_2 & \cdots & 0 & 0 \\ 0 & c_2 & a_2 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & c_{n-1} & a_{n-1} & b_{n-1} \end{pmatrix} \quad (3 \text{ marks}) \text{ **Cat B Seen**}$$

$$= a_n \cdot d_{n-1} - b_n c_n d_{n-2} \text{ (by column exp. along the last col.)} \quad (2 \text{ marks}) \text{ **Cat B Seen**}$$

- (ii) This is similar to the exercise on finding the closed form for the Fibonacci sequence, which is in one of the problem sheets.

We re-write the recursive relation above with the new assumptions: for $n > 2$

$$d_n = a d_{n-1} - b c d_{n-2}.$$

(1 mark) Cat C Unseen

In fact, if we set $d_{-1} = 0$ and $d_0 = 1$, the relation above holds for all $n \geq 1$. In other words for all $n \geq 1$ we have

$$\begin{pmatrix} d_n \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} a & -bc \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d_{n-1} \\ d_{n-2} \end{pmatrix}.$$

Let A be the matrix in the equality above. By induction on n we get

$$\begin{pmatrix} d_n \\ d_{n-1} \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

(2 marks) Cat C Unseen

Thus, it now suffices to show that A is diagonalisable and that to express e_1 as a linear combination of its eigenvalues.

The characteristic polynomial of A is

$$X(X - a) + bc = X^2 - (b + c)X + bc = (X - b)(X - c).$$

(1 mark) Cat D Unseen

The assumptions on b and c imply that the polynomial above has two distinct roots, namely $X = b$ and $X = c$. Therefore A is diagonalisable and we may proceed with finding the close form expression.

We compute the eigenspaces for A :

- Eigenvalue b . The eigenspace is

$$E_b = \ker \begin{pmatrix} -c & bc \\ -1 & b \end{pmatrix} = \text{Span} \left\{ \begin{pmatrix} b \\ 1 \end{pmatrix} \right\}.$$

(1 mark) Cat D Unseen

- Eigenvalue c . The eigenspace is

$$E_c = \ker \begin{pmatrix} -b & bc \\ -1 & c \end{pmatrix} = \text{Span} \left\{ \begin{pmatrix} c \\ 1 \end{pmatrix} \right\}.$$

(1 mark) Cat D Unseen

Let

$$v_x = \begin{pmatrix} x \\ 1 \end{pmatrix}, \text{ for } x = b, c.$$

Then $e_1 = (b - c)^{-1}(v_b - v_c)$. Applying A^n and using the fact that v_b and v_c are eigenvectors, we obtain that

$$A^n e_1 = (b - c)^{-1}(b^n v_b - c^n v_c).$$

Thus, $d_n = (b^{n+1} - c^{n+1})/(b - c)$.

(1 mark) Cat D Unseen

(Total: 20 marks)

5. (a) A permutation $\sigma \in S_n$ is called a **cycle** if there is a sequence of distinct numbers $a_1, \dots, a_k \in \{1, \dots, n\}$ such that

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \quad \dots, \quad \sigma(a_{k-1}) = a_k, \quad \sigma(a_k) = a_1$$

and $\sigma(i) = i$ for every number not in this sequence.

(2 marks) Cat A seen

- (b) (i) Recall that a 4-cycle has order 4, hence $\text{ord}(\sigma) = 4$ and the set D is given by

$$\begin{aligned} D &= \{\sigma^0, \sigma, \sigma^2, \sigma^3, \sigma^0 \circ \tau, \sigma \circ \tau, \sigma^2 \circ \tau, \sigma^3 \circ \tau\} \\ &= \{id, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 4)(2\ 3), (2\ 4), (1\ 3), (1\ 2)(3\ 4)\}. \end{aligned}$$

And $|D| = 8$

(3 marks) Cat A seen

- (ii) $(1\ 2\ 3\ 4)^{-1} = (1\ 4\ 3\ 2)$ (just run the cycle backwards). From the previous computation $\sigma\tau = (2\ 4)$, and so is $\tau\sigma^{-1}$.

$$\sigma^{-n} = (\sigma^{-1})^n = (\tau^{-1}\sigma\tau)^n = (\tau^{-1}\sigma\tau)(\tau^{-1}\sigma\tau) \dots (\tau^{-1}\sigma\tau) = \tau\sigma^n\tau^{-1}.$$

(3 marks) Cat A unseen

- (iii) We will use the subgroup test. Clearly the identity is in D as $\sigma^0 = id$, hence D is not empty. We just need to show that if g, h are in D , then $gh^{-1} \in D$. Assume that g and h are in D . Note first that τ is its own inverse as it is a disjoint product of 2-cycles. Moreover σ is a 4-cycle, and is hence an element of order 4, meaning that $\sigma^i \in \{\sigma^0, \sigma, \sigma^2, \sigma^3\}$ for all $i \in \mathbb{Z}$. Then we have four cases and we get using part ii):

- If $g = \sigma^i$ and $h = \sigma^j$, for some i, j in $\{0, \dots, 3\}$. Then $gh^{-1} = \sigma^i\sigma^{-j} = \sigma^{i-j} \in D$.
- If $g = \sigma^j$ and $h = \sigma^i \circ \tau$, then by ii) and using $\tau = \tau^{-1}$

$$gh^{-1} = \sigma^j \circ (\sigma^i \circ \tau)^{-1} = \sigma^j \circ \tau^{-1} \circ \sigma^{-i} = \sigma^j \circ \sigma^i \circ \tau^{-1} = \sigma^{i+j} \circ \tau \in D.$$

- If $g = \sigma^i \circ \tau$ and $h = \sigma^j$, $gh^{-1} = \sigma^i \circ \tau \circ \sigma^{-j} = \sigma^i \circ \tau^{-1} \circ \sigma^{-j} \in D$ by previous computation.
- $g = \sigma^i \circ \tau$ and $h = \sigma^j \circ \tau$, for some $i, j \in \{0, \dots, n\}$, $gh^{-1} = \sigma^i \circ \tau \circ \tau^{-1} \circ \sigma^{-j} = \sigma^i \circ \sigma^{-j} \in D$.

(5 marks) Cat B seen

- (c) (i) Either b is in the image of the map $T_A : \mathbb{R}^n \rightarrow \mathbb{R}^n, x \mapsto Ax$ or it is not. If it is not, $U = \emptyset$ and we are done. If it is, then $b = Au$ for some vector $u \in \mathbb{R}^n$. Claim: The solution set for the inhomogeneous equation $Ax = b$ is the coset $u + W$. Indeed assume that $x \in u + W$. Then $Ax = A(u + w) = Au + Aw = b + 0 = b$ for some $w \in W$, hence $u + W \subseteq U$. Conversely assume $x \in U$. Then $0 = Ax - b = Ax - Au = A(x - u)$. Hence $x - u = w$, for some $w \in W$ or in other words $x \in u + W$. This finishes the proof.

(4 marks) Cat d unseen

- (ii) Since $H \cap K$ is a subgroup of both H and K , its size divides both $|H|$ and $|K|$ by Lagrange. Therefore, by relative primality of these sizes, $|H \cap K| = 1$, so $H \cap K = \{e\}$.

(3 marks) Cat C unseen

(Total: 20 marks)

6. (a) (i) $\mathbb{Z}$ with the addition is cyclic because for all $a \in \mathbb{Z}$ there is $n \in \mathbb{Z}$ such that $a = n \cdot 1$, namely $n = a$.

(1 mark) Cat A seen

- (ii) $\mathbb{Q}$ with the addition is not cyclic, because if it were, there would be $a/b \in \mathbb{Q}$ such that $\mathbb{Q} = \langle a/b \rangle$, but then the denominators in $\mathbb{Q}$ would only be divisible by the divisors of b , which is a contradiction.

(2 marks) Cat A seen

- (iii) This is not cyclic because it is not abelian. For example the following two matrices do not commute:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

(2 marks) Cat A seen

- (b) Let $g \in G$ be such that $G = \langle g \rangle$. Clearly $\langle \varphi(g) \rangle \subseteq \text{Im } \varphi$ because $\text{Im } \varphi$ is a subgroup of H .

(1 mark) Cat A seen

To show the reverse inclusion, let $a \in \text{Im } \varphi$. By definition of image, there is $h \in G$ such that $a = \varphi(h)$. Since G is cyclic, there is $m \in \mathbb{Z}$ such that $h = g^m$. Hence

$$a = \varphi(h) = \varphi(g^m) = \varphi(g)^m.$$

It follows that $\text{Im } \varphi \subseteq \langle \varphi(g) \rangle$ and so $\text{Im } \varphi = \langle \varphi(g) \rangle$.

(2 marks) Cat A seen

- (c) The homomorphism φ is injective if and only if $\ker \varphi = \{e_G\}$. The kernel of the group homomorphism φ is a subgroup of G . By Lagrange's theorem, since G is finite, $|\ker \varphi|$ divides the order of G .

(2 marks) Cat B seen

However G has prime order, so either $|\ker \varphi| = |G|$ or $|\ker \varphi| = 1$. The first alternative is not possible because, by assumption, there is a $g \in G$ such that $\varphi(g) \neq e_H$. By definition of kernel of φ , $g \notin \ker \varphi$, so $|\ker \varphi| \neq |G|$. Hence $|\ker \varphi| = 1$, so (again because it is a subgroup and it contains e_G) $\ker \varphi = \{e_G\}$.

(3 marks) Cat B seen

- (d) (i) Let $x, y \in G$, since φ is bijective there exist two unique $a, b \in G$ such that $x = \varphi(a)$ and $y = \varphi(b)$. Hence, using that φ is a homomorphism,

$$\varphi^{-1}(xy) = \varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

(1 mark) Cat C seen

- (ii) Let $x, y \in G$ and $\varphi = \varphi_1 \circ \varphi_2$. Then

$$\varphi(xy) = \varphi_1(\varphi(xy)) = \varphi_1(\varphi_2(x)\varphi_2(y)) = \varphi_1(x)\varphi_1(y).$$

(1 mark) Cat C seen

(iii) Let $\text{Perm}(G)$ be group of all bijective functions $G \rightarrow G$. We prove that $\text{Aut}(G)$ is a subgroup of $\text{Perm}(G)$. (By definition, an isomorphism is a bijective function and so $\text{Aut}(G) \subseteq \text{Perm}(G)$.) It suffices to apply the subgroup test:

- clearly the identity function is an isomorphism $G \rightarrow G$ so $\text{Aut}(G) \neq \emptyset$.
- If $\varphi \in \text{Aut}(G)$ then φ^{-1} is also a (bijective) homomorphism by (i), so $\varphi^{-1} \in \text{Aut}(G)$.
- The composition of two isomorphisms $G \rightarrow G$ is also a (bijective) homomorphism by (ii), so it is an isomorphism.

(1 mark) **Cat C** seen

(iv) The homomorphism we are looking for is $C : g \mapsto \varphi_g$, where

$$\varphi_g(x) = gxg^{-1}$$

($\varphi_g(x) = g^{-1}xg$ seems to work as well but then C is actually not a homomorphism). Clearly $\varphi_g(x) = \text{id}$ if and only if $gx = xg$ for all $x \in G$, that is if and only if $g \in Z(G)$. Thus, it suffices to show that $\varphi_g \in \text{Aut}(G)$ for all $g \in G$ and that C is a homomorphism. To do this, we first note that φ_g is certainly bijective: indeed, $(\varphi_g)^{-1} = (\varphi_{g^{-1}})$, as $g^{-1}gxg^{-1}g = x$ for all $x \in G$. Moreover if $x, y \in G$

$$\varphi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y).$$

We deduce that that $\varphi_g \in \text{Aut}(G)$ for all $g \in G$.

To conclude, we show that C is a homomorphism. Let $g, h \in G$. Then, for all $x \in G$,

$$C(gh)(x) = \varphi_{gh}(x) = ghxh^{-1}g^{-1} = \varphi_g(\varphi_h(x)) = (\varphi_g \circ \varphi_h)(x) = (C(g) \circ C(h))(x).$$

Hence $C(gh) = C(g) \circ C(h)$ and C is a homomorphism. (4 marks) **Cat D** unseen

(Total: 20 marks)

Question Marker's comment

- 2 (a) Answered well in general. A few people confused the subspace test with the subgroup test. (b) (i) Most people who attempted this had the right idea but forgot to mention and use explicitly the fact that the intersections of subspaces are subspaces by part (a). (ii) Some good answers. Many people attempted a proof using $\dim(B \setminus C)$, which is not a subspace and so has no notion of dimension. (c) Very few fully correct answers. Many people skipped this part of the question. Some people found the correct A' , but did not provide a good justification. (d) Mixed answers. Some people gave a correct answer without proper justification.
- 3 (a) (i) Answered well in general. Some students forgot to prove linear independence or spanning condition; (ii) Most of the students gave a correct map, but forgot to justify linearity. Those who justified it just checked additivity and almost no one checked homogeneity of degree 1; (iii) Answered well in general, although some students gave no justification; (b) (i) Answered well in general; (ii) First part answered well in general. For the second part (very pink) some students used matrices, instead of vectors, to give a counterexample. (iii) Answered quite well in general, although some students did not check all the conditions.
- 5 a) What is important is to say that cycles are permutations and to explain how they act. Make sure to mention what happens to every single element (especially the ones that are not permuted). b) i) Main mistake was to use wrong notation: Cycle notation is different from the "tabular" that tells which element goes where. ii) Sometimes it was implicitly assumed that σ and τ commute ($\sigma \tau \sigma$)^k became $\sigma^k \tau^k \sigma^k$ - this is not true! iii) Main mistake was that case distinction (for showing that the set is closed under multiplication) was not exhaustive c) Two inclusions are to be shown. d) Note that the order of H and K need not be prime, so they need not be cyclic!
- 6 (a) (i) Answered well in general; In (ii) and (iii) some students gave wrong or no justification; (b) Answered quite well in general, although only a small number of students gave a clear and complete proof; (c) Only some ideas in general. Not so many students used "kernel is trivial iff group monomorphism"; (d) (i) Almost everyone forgot to check that the inverse function is a group homomorphism; (ii) Many students did not check that the composition is a group homomorphism. Some of them answered "as seen in lectures"; (iii) Many students forgot associativity; (iv) The majority did not attempt it or gave a wrong answer. Only a very small number of students answered well.