THE UNIVERSITY OF MELBOURNE

Student Number

Semester 2 Assessment, 2018

School of Mathematics and Statistics

MAST20022 Group Theory and Linear Algebra

Writing time: 3 hours

Reading time: 15 minutes

This is NOT an open book exam

This paper consists of 17 pages (including this page)

Authorised Materials

- Mobile phones, smart watches and internet or communication devices are forbidden.
- Calculators, tablet devices or computers must not be used.
- No handwritten or print materials may be brought into the exam venue.

Instructions to Students

- You must NOT remove this question paper at the conclusion of the examination.
- The paper is in two sections. The questions in section A are shorter and more routine than those in Section B. It is recommended that students attempt the questions in Section A first. You should attempt all questions.
- Number the questions and question parts clearly. Start each question on a new page.
- Please give complete explanations in all questions and show all your calculations and working. Give careful statements of any results from the notes or lectures that you use.
- There are 14 questions with marks as shown. The total number of marks available is 95.

Instructions to Invigilators

- Students must NOT remove this question paper at the conclusion of the examination.

Blank page (ignored in page numbering)

Section A: 50 marks total

Question 1 (5 marks)

(a) Find the multiplicative inverse of $[9]_{14}$ in $\mathbb{Z}/14\mathbb{Z}$.

(b) What can be said about the multiplicative inverse of $[6]_{14}$ in $\mathbb{Z}/14\mathbb{Z}$?

(c) Using the Euclidean Algorithm, find $\gcd(299, 377)$.

Solution:—

(a) By inspection (or the euclidean algorithim) we see that $2 \times 14 - 3 \times 9 = 1$. Therefore $[-3]_{14}[9]_{14} = [1]_{14}$ and the inverse is $[-3]_{14} = [11]_{14}$

(b) No multiplicative inverse exists because 6 and 14 are not relatively prime.

(c)

$$\begin{aligned} 377 &= 1 \times 299 + 78 \\ 299 &= 3 \times 78 + 65 \\ 78 &= 1 \times 65 + 13 \\ 65 &= 5 \times 13 + 0 \end{aligned}$$

Therefore $\gcd(377, 299) = 13$

Question 2 (5 marks)

(a) Show that $\mathbb{Q}(i) = \{a + bi \mid a, b, \in \mathbb{Q}\} \subset \mathbb{C}$ is a field (using the usual operations on $\mathbb{C}$). (Hint: You may use that $\mathbb{C}$ is a field.)

(b) (i) Give the definition of what it means to say that a field is *algebraically closed*.

(ii) Show that the field $\mathbb{Q}(i)$ is *not* algebraically closed.

Solution:—

(a) Note that

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i \qquad (a+bi)+(c+di) = (a+c)+(b+2)i$$

The set is clearly closed under addition and multiplication and $1 \in \mathbb{Q}(i)$. Moreover, if $a + bi \in \mathbb{Q}(i) \setminus \{0\}$, then

$$(a+bi)^{-1} = \frac{1}{a^2+b^2}(a-bi) \in \mathbb{Q}(i)$$

That is, the set is closed under taking inverses.
It follows that $\mathbb{Q}(i)$ is a subfield of $\mathbb{C}$.

(b)(i) F is algebraically closed if every non-constant polynomial in $F[X]$ has a root in F.

(b)(ii) The roots of the polynomial $X^2 - 2$ do not lie in $\mathbb{Q}(i)$.

Question 3 (5 marks)

Consider the matrix $M = \begin{bmatrix} i & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & i \end{bmatrix} \in M_3(\mathbb{C})$.

(a) Find the minimal polynomial of M.

(b) Use your answer for part (a) to determine whether M is diagonalizable. (Be sure to give a justification.)

Solution:—

(a) By inspection, the characteristic polynomial is $(X-i)^2(X+1)$. The minimal poly must therefore be either $(X-i)(X+1)$ or $(X-i)^2(X+1)$. Calculation gives

$$(M-iI)(M+I) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -1-i & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1+i & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1+i \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \neq 0$$

Therefore the minimal polynomial must be $(X-i)^2(X+1)$

(b) Since the minimal polynomial has a repeated linear factor, the matrix is NOT diagonalizable.

Question 4 (5 marks)

Find all possible Jordan normal forms (up to permutation of Jordan blocks) for a matrix whose characteristic polynomial is $(X+2)^2(X-5)^3$

Solution:—

$$\begin{bmatrix} -2 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 1 & 5 \end{bmatrix} \quad \begin{bmatrix} -2 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix} \quad \begin{bmatrix} -2 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

$$\begin{bmatrix} -2 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 1 & 5 \end{bmatrix} \quad \begin{bmatrix} -2 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix} \quad \begin{bmatrix} -2 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

Question 5 (5 marks)

Let V be an inner product space and $f : V \to V$ a linear transformation.

(a) Give the definition of the adjoint f^*.

(b) Show that if $f = f^*$, then all eigenvalues of f are real.

Solution:—

(a) The adjoint is a linear transformation $f^* : V \to V$ satisfying

$$\forall v, w \in V,\ \langle f(v), w\rangle = \langle v, f^*(w)\rangle$$

(b) Let λ be an eigenvalue of f and let $v \in V \setminus \{0\}$ be a corresponding eigenvector. Then

$$\lambda\langle v, v\rangle = \langle \lambda v, v\rangle = \langle f(v), v\rangle = \langle v, f^*(v)\rangle = \langle v, f(v)\rangle = \langle v, \lambda v\rangle = \bar{\lambda}\langle v, v\rangle$$

Therefore $\lambda = \bar{\lambda}$ and $\lambda \in \mathbb{R}$.

Question 6 (5 marks)

Let V be a vector space and $U, W \leq V$ two subspaces of V.

(a) Give the definition of what it means to say that $V = U \oplus W$.

(b) Suppose that $V = U \oplus W$. Show that for all $v \in V$ there exist unique vectors $u \in U$ and $w \in W$ such that $v = u + w$.

Solution:—
(a) $V = U + W$ and $U \cap W = \{0\}$. Where $U + W = \{u + w \mid u \in U, w \in W\}$
(b) Existence is clear from the definition of $U \oplus W$
For uniqueness, assume that $u_1 + w_1 = u_2 + w_2$ for some $u_1, u_2 \in U$ and $w_1, w_2 \in W$. Then

$$\begin{aligned} u_1 + w_1 = u_2 + w_2 &\implies u_1 - u_2 = w_2 - w_1 \in U \cap W \\ &\implies u_1 - u_2 = w_2 - w_1 = 0 \\ &\implies u_1 = u_2 \text{ and } w_2 = w_1 \end{aligned}$$

Question 7 (5 marks)

Let G be a group and $H, K \leq G$ two subgroups.

(a) Prove that $H \cap K$ is a subgroup of G.

(b) Give and example to show that $H \cup K$ need not be a subgroup of G.

Solution:—

(a) First note that $H \cap K \neq \emptyset$ since $e_G \in H \cap K$. Let $g, h \in H \cap K$. Since H is a subgroup $gh^{-1} \in H$. Since K is a subgroup $gh^{-1} \in K$. Therefore $gh^{-1} \in H \cap K$. It follows (from a lemma in lectures) that $H \cap K$ is a subgroup.

(b) Let $G = S_3$, $H = \langle (12) \rangle$ and $K = \langle (123) \rangle$. Then $H \cup K = \{e, (12), (123), (132)\}$. That this is not a subgroup can be seen from Lagrange since 4 does not divide 6 (or directly).

Question 8 (5 marks)

For each of the following pairs decide whether or not the two groups are isomorphic. You should justify your answers.

(a) $(\mathbb{F}_5^\times, \times)$ and $(\mathbb{Z}/5\mathbb{Z}, +)$

(b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$

(c) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and D_5

(d) $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$ and $\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})$

Solution:—

(a) Not isomorphic. Sets have different sizes (4 and 5).
(b) Yes, isomorphic. Both are abelian. There is only one abelian group of size 6. (alternatively, construct an isomorphism)
(c) No. One is abelian and the other not.
(d) No. The second contains an element of order 4 and the other does not.

Question 9 (5 marks)

(a) Let G be a finite group and $\varphi : G \to H$ a homomorphism.
Prove that the order of $\varphi(G)$ divides the order of G.

(b) How many homomorphisms are there from $\mathbb{Z}/3\mathbb{Z}$ to $S_3 \times \mathbb{Z}$?
Be careful to justify your answer.

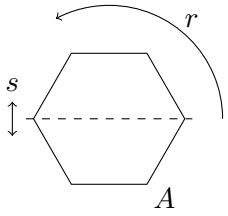
Solution:—
(a)
By the first isomorphism theorem $G/\ker(\varphi) \cong \varphi(G)$, which yields

$$|G|/|\ker(\varphi)| = |G/\ker(\varphi)| = |\varphi(G)|$$

(b) A homorphism $\varphi : \mathbb{Z}_3 \to S_3 \times \mathbb{Z}$ is uniquely determined by the image of $[1]_3$. The element $\varphi([1]) \in S_3$ must have order 1 or 3 (since its order divides 3). There are THREE possibilities: $\varphi([1]) = e$, $\varphi([1]) = ((123), 0)$, $\varphi([1] = ((132), 0)$. Each choice extends to a homomorphism.

Question 10 (5 marks)

Let $s, r \in D_6$ be the symmetries of a regular hexagon corresponding to reflection across the line shown and rotation by $2\pi/3$ respectively. Consider the subgroup $H \leq D_6$ generated by $\{s, r\}$.



(a) Find the orbit and stabilizer of the vertex A under the action of H.
(Label the vertices of the hexagon A, B, C, D, E, F clockwise from the vertex A shown.)

(b) Is the action of H transitive?

Solution:—
(a)
The orbit is $\{A, C, E\}$
The stabilizer is $\{e, sr\}$.

(b) No. There are two orbits of vertices.

Section B: 45 marks total

Question 11 (10 marks)

(a) State the Orbit-Stabilizer relation.

(b) Let G be a group of size 16 and X a set having 25 elements. Show that every action of G on X has a fixed point.

(c) Suppose that a finite group G acts non-trivially on a finite set X. Let $n = |G|$ and $r = |X|$. Prove that if $n > r!$ then G has a normal subgroup $N \lhd G$ satisfying both $N \neq \{e\}$ and $N \neq G$.

Solution:—

(a) Suppose a finite group acts on a set X. Then for all $x \in X$

$$|G| = |Stab(X)| \times |Orbit(x)|$$

(b) We need to show that there is an orbit of size 1. The orbits partition X. By the orbit stabilizer relation the size of an orbit divides 16. If every orbit had at least 2 elements, we could conclude that $|X|$ was even.

(c) The action determines a homomorphism $\varphi(G) \to S_r$. The kernel $ker(\varphi)$ is normal in G. That the action is non-trivial means that $\ker(\varphi) \neq G$. If $\ker(\varphi) = \{e\}$, then G is isomorphic to a subgroup of S_r. But this is not possible given that $n > |S_r|$. We conclude therefore that $\ker(\varphi)$ is a proper normal subgroup of G.

Question 12 (10 marks)

Let V be a K-vector space and let $f : V \to V$ be a linear transformation.

(a) Give the definition of an *f-invariant subspace* of V.

(b) Let $p(X) \in K[X]$. Prove that $W = \ker(p(f))$ is an f-invariant subspace of V.

(c) Suppose now that $p(f) = 0$ and that $p(X) = q_1(X)q_2(X)$ for some relatively prime $q_1(X), q_2(X) \in K[X]$. Show that $V = (\ker(q_1(f))) \oplus (\ker(q_2(f)))$.

Solution:—

(a) A subspace $W \leq V$ is invariant if $f(w) \in W$ for all $w \in W$

(b) Let $p(X) = \sum_{i=0}^{m} a_i X^i$. Let $w \in \ker(p(f))$ and set $u = f(w)$.

$$p(f)(u) = \sum_{i=0}^{m} a_i f^i(u) = \sum_{i=0}^{m} a_i f^{i+1}(w) = f\left(\sum_{i=0}^{m} a_i f^i(w)\right) = f(p(f)(w)) = f(0) = 0$$

Therefore $u = f(w) \in\in \ker(p(f))$

(c) Since $q_1(x)$ and $q_2(X)$ are relatively prime, there exist $a_1(X), a_2(X) \in K[X]$ such that

$$a_1(X)q_1(X) + a_2(X)q_2(X) = 1$$

and therefore

$$a_1(f)q_1(f) + a_2(f)q_2(f) = \mathrm{id}_V$$

Let $v \in V$. From above

$$v = a_1(f)q_1(f)(v) + a_2(f)q_2(f)(v) \qquad (*)$$

Note that $q_2(f)(a_1(f) \circ q_1(f)(v)) = a_1(f)(p(f)(v)) = a_1(f)(0) = 0$. So $a_1(f)q_1(f)(v) \in \ker(q_2(f))$

Similarly $a_2(f)q_2(f)(v) \in \ker(q_1(f))$. Therefore $V = (\ker(q_1(f))) + (\ker(q_2(f)))$.

It is also clear from (*) that $v \in (\ker(q_1(f))) \cap (\ker(q_2(f))) \implies v = 0$.

Question 13 (10 marks)

(a) Let V be an inner product space. Show that if $f : V \to V$ is a normal linear transformation, then $f(v) = 0$ if and only if $f^*(v) = 0$.

(b) State the Spectral Theorem for linear transformations on a finite dimensional inner product space.

(c) Let $A = \begin{bmatrix} 2 & i \\ i & 2 \end{bmatrix}$.

(i) Show that A is normal.

(ii) Find a unitary matrix U such that U^*AU is diagonal.

(iii) Show that there exists a matrix B such that $B^2 = A$.

Solution:—
(a)

$$\begin{aligned} f(v) = 0 &\iff \langle f(v), f(v)\rangle = 0 \\ &\iff \langle v, f^*f(v)\rangle = 0 \\ &\iff \langle v, ff^*(v)\rangle = 0 \qquad \text{since } f \text{ is normal} \\ &\iff \langle f^*(v), f^*(v)\rangle = 0 \\ &\iff f^*(v) = 0 \end{aligned}$$

(b)
If $f : V \to V$ is a normal linear transformation on a finite dimensional complex inner product space, then there exists an orthonormal basis $\mathcal{B}$ of V such that $[f]_{\mathcal{B}}$ is diagonal.

(c) (i)

$$AA^* = \begin{bmatrix} 2 & i \\ i & 2 \end{bmatrix}\begin{bmatrix} 2 & -i \\ -i & 2 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$
$$A^*A = \begin{bmatrix} 2 & -i \\ -i & 2 \end{bmatrix}\begin{bmatrix} 2 & i \\ i & 2 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

(ii) The char poly is given by

$$\det \begin{bmatrix} X-2 & -i \\ -i & X-2 \end{bmatrix} = (X-2)^2 + 1 = X^2 - 4X + 5$$

The eigenvalues are $2 - i$, $2 + i$

$$A - (2-i)I = \begin{bmatrix} i & i \\ i & i \end{bmatrix} \sim \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

A unit eigenvector with eigenvalue $2 - i$ is $(\frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}})$

$$A - (2+i)I = \begin{bmatrix} -i & i \\ i & -i \end{bmatrix} \sim \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}$$

A unit eigenvector with eigenvalue $2-i$ is $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$
We can therefore take

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

(iii)
Note that $U^*AU = \begin{bmatrix} 2-i & 0 \\ 0 & 2+i \end{bmatrix}$ Let $a, b \in \mathbb{C}$ be such that $a^2 = 2-i$, $b^2 = 2+i$. We have

$$A = U \begin{bmatrix} 2-i & 0 \\ 0 & 2+i \end{bmatrix} U^* = U \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} U^* = U \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} U^* U \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} U^* = B^2$$

where

$$B = U \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} U^* = \frac{1}{2} \begin{bmatrix} a+b & -a+b \\ -a+b & a+b \end{bmatrix}$$

Question 14 (15 marks)

The set

$$Q = \{1, -1, i, -i, j, -j, k, -k\}$$

has the structure of a group in which 1 is the identity element and the multiplication satisfies:

$$i^2 = j^2 = k^2 = -1, \qquad (-1)^2 = 1$$
$$ij = k, \qquad jk = i, \qquad ki = j$$
$$-i = (-1)i, \qquad -j = (-1)j, \qquad -k = (-1)k$$

(You do not have to prove that this is a group.)

(a) Show that $ji = -k$ in Q.

(b) Find the order of each element in Q.

(c) Is Q isomorphic to D_4? Justify your answer.

(d) Calculate the centre $Z(Q)$ of Q.

(e) Determine which of the following groups is isomorphic to the quotient $Q/Z(Q)$:

(i) $\mathbb{Z}/2\mathbb{Z}$
(ii) $\mathbb{Z}/4\mathbb{Z}$
(iii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
(iv) $\mathbb{Z}/8\mathbb{Z}$

Solution:—
(a) $ji = kii = k(-1) = kk^2 = k^2k = (-1)k = -k$

(b) $o(1) = 1$ since i is the identity
$o(-1) = 2$ since $(-1)^2 = 1$
$o(i) = 4$ since $i^4 = (-1)^2 = 1$ and $i^2 \neq 1$
$o(-i) = 4$ since $(-i)^2 = (i^3)^2 = i^6 = i^2 \neq 1$ and $(-i)^4 = i^{12} = 1$
$o(j) = o(-j) = o(k) = o(-k) = 4$ as for i

(c) NOT isomorphic to D_4 because D_4 has 4 elements of order 2 whereas Q has 1 element of order 2.

(d)Clearly $1, -1 \in Z(Q)$. From (a) we know that $i, j \notin Z(Q)$. Similarly $k \notin Z(G)$ as $ik = -j \neq ki$. Since $-i = (-1)i$ and $i \notin Z(G)$ we have $-i \notin Z(G)$. Similarly $-j, -k \notin Z(G)$.
We have shown that $Z(G) = \{1, -1\}$.

(e)
(i) NO, because $|Q/Z(Q)| = 8/2 = 4$
(ii) NO, since all elements in the quotient square to give the identity:

$$(iZ)^2 = i^2Z = (-1)Z = Z \quad (jZ)^2 = j^2Z = (-1)Z = Z \quad (kZ)^2 = k^2Z = (-1)Z = Z$$

where $Z = Z(Q) = \{1, -1\}$
(iii) YES, since the quotient has size four and is not cyclic
(iv)NO, because $|Q/Z(Q)| = 8/2 = 4$

End of Exam—Total Available Marks = 95