

The University of Melbourne
Semester Two 2006
Department of Mathematics and Statistics
620-142 Mathematics B

Exam duration: Three hours

Reading time: 15 minutes

This paper has 6 pages.

The total number of marks allocated is 120.

Common Content: This examination paper contains questions in common with the paper for 620-122 Mathematics B (Advanced).

Authorized Materials: No materials are authorized. Calculators and mathematical tables are not permitted. Candidates are reminded that no written or printed materials related to the subject may be brought into the examination. If you have any such materials in your possession, you should immediately surrender it to an invigilator.

Instructions to Invigilators: One 14 page script book is to be given to each student initially. Students may retain this examination paper. No written or printed materials related to the subject may be brought into the examination. No mathematical tables or calculators may be used.

Instructions to Students: This examination consists of 8 questions. All questions may be attempted. The number of marks for each question is indicated on the examination paper. Use of calculators is not allowed.

Paper to be held by Baillieu Library: This paper may be reproduced and lodged with the Baillieu Library.

1. (a) (i) Use the Euclidean algorithm to show that the greatest common divisor of 52 and 135 is 1.
(ii) Find integers x and y such that

$$52x + 135y = 1.$$

- (iii) Write down the value of 52^{-1} in \mathbb{Z}_{135} .
- (b) State Fermat's Little Theorem, and use this to help you calculate 2^{100} in \mathbb{Z}_{97} .
- (c) (i) Find the prime factorization of 40.
(ii) Calculate the number of units in \mathbb{Z}_{40} .
(iii) Calculate the order of 21 in \mathbb{Z}_{40} .
- (d) If u , v and w are positive integers, u is factor of v , and u is a factor of w , prove that u^2 is a factor of $5v^2 + 10w^2$.
- (e) Use Mathematical Induction to prove that $n^3 - n + 3$ is divisible by 3 for all positive integers n .

[22 marks]

2. In this question, the RSA public key cryptosystem is being implemented with base $m = 5 \times 13 = 65$.

- (a) Calculate $\phi(m)$.
- (b) Explain why $e = 11$ is a suitable choice of encrypting key.
- (c) Using this encrypting key, encrypt the message '2'.
- (d) Which one of the following is a suitable decrypting key: $d = 6$ or $d = 35$? Explain your answer.
- (e) Using this decrypting key, decrypt the message '3'.

[10 marks]

3. Let

$$A = \begin{bmatrix} 1 & 1 & 4 & 1 & 2 \\ 0 & 1 & 2 & 1 & 1 \\ 1 & 2 & 6 & 2 & 3 \\ 1 & -1 & 0 & 0 & 2 \\ 2 & 1 & 6 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

where the matrix B is obtained from the matrix A by applying elementary row operations. You may use the information above to answer the following questions:

- (a) What is the rank of A ?
- (b) Write down a basis for, and the dimension of, the column space of A .
- (c) Write down a basis for, and the dimension of, the row space of A .
- (d) Write down the dimension of the solution space of A .
- (e) Are the rows of A linearly dependent? Explain your answer.
- (f) Write $(2, 1, 3, 2, 1)$ as a linear combination of $(1, 0, 1, 1, 2)$, $(1, 1, 2, -1, 1)$ and $(1, 1, 2, 0, 0)$.
- (g) Do the columns of A span \mathbb{R}^5 ? Give a reason for your answer.

[11 marks]

4. (a) Determine whether the set of all polynomials of the form

$$ax^2 + bx + c, \quad \text{where } a + b = c$$

is a subspace of the vector space \mathcal{P}_2 of real polynomials of degree ≤ 2 . Explain your answer, either by using the subspace theorem or by providing a counter-example.

(b) Determine whether the polynomial

$$p(x) = x^2 + x + 2$$

belongs to $\text{span}\{p_1(x), p_2(x), p_3(x)\}$, where

$$p_1(x) = 2x^2 + x + 2, \quad p_2(x) = x^2 - 2x, \quad p_3(x) = 5x^2 - 5x + 2.$$

[11 marks]

5. (a) (i) Using \mathbb{Z}_2 arithmetic, find a basis for the solution space of

$$\begin{aligned}x_1 + x_4 + x_5 &= 0 \\x_2 + x_5 + x_6 &= 0 \\x_3 + x_4 + x_6 &= 0.\end{aligned}$$

- (ii) Write down the number of vectors in the solution space of (i).
(iii) Consider the binary code with check matrix

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

Use this matrix to decode the received message 111001 (using nearest neighbour decoding).

- (b) Consider the binary code $\{00000, 01110, 10111, 11001\}$.
(i) Is this a linear code? (Give a reason for your answer.)
(ii) What is the minimum Hamming distance between pairs of distinct code-words?
(iii) How many errors in transmission could this code detect, and how many errors could it correct, if the nearest neighbour principle is used?

[12 marks]

6. (a) For column vectors \mathbf{u} and \mathbf{v} in \mathbb{R}^2 , suppose that we define

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^T A \mathbf{v}, \text{ where } A = \begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix},$$

or equivalently

$$\langle (u_1, u_2), (v_1, v_2) \rangle = 3u_1v_1 - u_1v_2 - u_2v_1 + 2u_2v_2.$$

- (i) Prove that $\langle \cdot, \cdot \rangle$ defines an inner product on \mathbb{R}^2 , by checking the inner product axioms.
(ii) Use this inner product to find $\|(1, -1)\|$.
(b) Suppose that W is the subspace of \mathbb{R}^4 with basis $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, where $\mathbf{v}_1 = (1, 0, 0, -1)$, $\mathbf{v}_2 = (1, -1, 0, 0)$ and $\mathbf{v}_3 = (0, 1, 0, 1)$.
(i) Use the Gram-Schmidt process to transform S to an orthonormal basis $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ for W , using the dot product as inner product.
(ii) Check your answer by verifying that $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ is an orthogonal set.
(c) Suppose that W is the subspace of \mathbb{R}^3 with orthonormal basis $\{\mathbf{u}_1, \mathbf{u}_2\}$, where $\mathbf{u}_1 = \frac{1}{3}(2, -1, -2)$ and $\mathbf{u}_2 = \frac{1}{\sqrt{2}}(1, 0, 1)$. Using the dot product as inner product, find the orthogonal projection of $\mathbf{v} = (3, 4, 1)$ onto W .

[18 marks]

7. (a) $T : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ is defined by

$$T(x, y) = (x - y, 0, 2x + 3)$$

for all (x, y) in \mathbb{R}^2 . Determine whether or not T is a linear transformation. Explain your answer.

- (b) Find a single matrix that performs the following sequence of operations in the plane: a shear in the x -direction of factor 2, then rotation through an angle of $\frac{\pi}{2}$ radians anticlockwise around the origin.
- (c) Let \mathcal{P}_n denote the vector space of all real polynomials of degree $\leq n$ in the variable x . A linear transformation $T : \mathcal{P}_3 \rightarrow \mathcal{P}_2$ is defined by

$$T(p(x)) = p(x) + p(-x).$$

- (i) Write down $T(a + bx + cx^2 + dx^3)$ and check that this is in \mathcal{P}_2 .
- (ii) Find the matrix which represents T relative to the basis $\{1, x, x^2, x^3\}$ for \mathcal{P}_3 and the basis $\{1, x, x^2\}$ for \mathcal{P}_2 .
- (iii) Find bases for the image and kernel of T .
- (d) Consider the bases $B = \{\mathbf{u}_1, \mathbf{u}_2\}$ and $B' = \{\mathbf{v}_1, \mathbf{v}_2\}$ for \mathbb{R}^2 , where

$$\mathbf{u}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{u}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \mathbf{v}_1 = \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \mathbf{v}_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

- (i) Write down the transition matrix from B' to B .
- (ii) Find the transition matrix from B to B' .
- (iii) If $[\mathbf{x}]_B = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$, calculate $[\mathbf{x}]_{B'}$.

[18 marks]

8. (a) (i) Find the eigenvalues and corresponding eigenvectors of the matrix

$$A = \begin{bmatrix} 2 & 2 & 2 \\ -1 & -1 & -2 \\ 1 & 2 & 3 \end{bmatrix}.$$

- (ii) Using your answers from (i), write down an invertible matrix P and a diagonal matrix D such that

$$D = P^{-1}AP.$$

(You do not need to calculate the inverse P^{-1} .)

Check your answer by using matrix multiplication to verify that $PD = AP$.

- (b) Consider the conic whose equation is

$$2x^2 + 4xy + 5y^2 = 3.$$

- (i) Write the conic in the standard form

$$A(x')^2 + B(y')^2 = 1,$$

and give the values of A and B .

- (ii) Identify the conic, and give the directions of its principal axes.
(iii) Sketch the conic using the new x' - y' coordinate system.

[18 marks]