UNIVERSITY OF SURREY ©

B. Sc. Undergraduate Programmes in Mathematical Studies

Level HE2 Examination

MS219 Algebra and Codes

Time allowed - 2 hours

Autumn Semester 2006

Answer any **three** of the five questions.

If you attempt more than three questions, only your BEST THREE answers will be taken into account.

Each question carries 30 marks.

Any results established in the course may be assumed and used without proof unless a proof is requested.

Question 1

(a) (i) Give a reason why $\mathbb{Z}_{26}$, with the operations of addition and multiplication modulo 26, is not a field. [2]

(ii) State, with explanation, whether 15 is a unit in the ring $\mathbb{Z}_{26}$. [3]

(iii) A is the matrix $\begin{pmatrix} 9 & 3 \\ 16 & 7 \end{pmatrix}$ in $M_2(\mathbb{Z}_{26})$.

Find A^{-1}, giving its entries as positive integers modulo 26. [8]

(iv) A 2-letter message is converted to numbers by setting $a = 1, b = 2, \ldots, z = 26$, and then encrypted using the above matrix A. The result is the same as the original message. Find a message with this property. [5]

(b) $\mathcal{F}(\mathbb{R})$ is the vector space of all functions of a real variable x.

Let $B : \mathcal{F}(\mathbb{R}) \times \mathcal{F}(\mathbb{R}) \to \mathbb{R}$ be defined by $B(\mathrm{f}(x), \mathrm{g}(x)) = \mathrm{f}(0)\,\mathrm{g}(0)$.

(i) Show that B is a symmetric bilinear form on $\mathcal{F}(\mathbb{R})$. [6]

(ii) Find $B(x, \mathrm{g}(x))$ for any $\mathrm{g}(x)$. Hence or otherwise determine whether B is positive definite and whether it is degenerate. [6]

Question 2

(a) (i) Let A be an $m \times n$ matrix over a field K. Prove that the null-space of A is the orthogonal complement of the row-space of A in K^n. [5]

(ii) Show that $(1,1,1,1,1)$ and $(1,2,3,0,4)$ are orthogonal in ${\mathbb{F}_5}^5$. [2]

(iii) Let $U = \text{span}\{(1,1,1,1,1),(1,2,3,0,4)\} \subset {\mathbb{F}_5}^5$.
Find a basis for $U^\perp$, the orthogonal complement of U in ${\mathbb{F}_5}^5$. [6]
Determine whether or not $U \oplus U^\perp = {\mathbb{F}_5}^5$. [3]

(b) Define the terms:

(i) a **linear** $[n,k]$ code over $\mathbb{F}_q$, [2]

(ii) a **generator matrix** for a linear code C, [2]

(iii) a **parity-check matrix** for a linear code C. [2]

(c) A linear code C over $\mathbb{F}_2$ has generator matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

(i) Show that 1011011 is not a codeword in C. [4]

(ii) State, with a reason, whether a single error in the received message 1011011 can be corrected, and if so decode the message. [4]

Question 3

(a) Prove that if S and T are subrings of a ring R, their intersection $S \cap T$ is also a subring of R. [5]

(b) Let K be a field and $K^2 = \{(a, b) \ : \ a, b \in K\}$.

Let addition and multiplication be defined on K^2 by $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b)(c, d) = (ac + bd, ad + bc)$ for any $a, b, c, d \in K$.

You are given that K^2 with these operations is a ring, which we shall denote by R.

(i) State, with explanation, whether the multiplication defined above is commutative on R. [2]

(ii) Find the multiplicative identity in R. [3]

(iii) If (a, b) has a multiplicative inverse (p, q) in R, express p and q in terms of a and b. Hence determine whether R with the given operations is a field. [6]

(iv) When $K = \mathbb{F}_2$, show that R has four elements and draw up a multiplication table for these elements. State, with a reason, whether R is isomorphic to $(\mathbb{Z}_4, +_4, \times_4)$. [8]

(v) Still taking $K = \mathbb{F}_2$, find an ideal I of R which has two elements. List the distinct elements of the quotient ring $\dfrac{R}{I}$. [6]

Question 4

(a) (i) State what extra properties a ring must have if it is an **integral domain**. [2]

(ii) Define the **characteristic** of a ring. [3]

(iii) Prove that the characteristic of an integral domain is either 0 or a prime number. [6]

(b) Let K be a subfield of $\mathbb{R}$, such that $\sqrt{2} \notin K$.
Let $K(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in K\}$.

(i) Prove that $K(\sqrt{2})$ is a subfield of $\mathbb{R}$. [8]

(ii) The map $\phi : K(\sqrt{2}) \to K(\sqrt{2})$ is given by $\phi(a + b\sqrt{2}) = b + a\sqrt{2}$. Determine, with explanation, whether or not ϕ is a automorphism of $K(\sqrt{2})$. [5]

(c) The map $\psi_{\sqrt{2}} : \mathbb{Q}[t] \to \mathbb{R}$ is defined by $\psi_{\sqrt{2}}(\mathrm{f}) = \mathrm{f}(\sqrt{2})$.

(i) Find $\psi_{\sqrt{2}}(t^4 - t^2 + 1)$. [2]

(ii) Given that $\psi_{\sqrt{2}}$ is a ring homomorphism, describe its kernel and its image. [4]

Question 5

(a) (i) Show that the polynomial f $= t^3 + t^2 + 1$ is irreducible over $\mathbb{F}_2$. [3]

(ii) Briefly describe how the principal ideal generated by f is used to construct a field K in which f has a zero. Give the usual notation for this field. [5]

(iii) If α is a zero of f in K, show that $\alpha^4 = \alpha^2 + \alpha + 1$. [5]

(b) Let C be a cyclic linear $[n, k]$ code over $\mathbb{F}_2$. Explain what is meant by saying that C is **generated** by a polynomial g. [3]

(c) C is a binary cyclic $[7, 4]$ code with generator matrix $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

(i) Write down a generating polynomial for C and find a check polynomial h. [7]

(ii) Write the message 0100011 in polynomial form and use h to determine whether it is a codeword in C. [5]

(iii) Write down a parity-check matrix for C. [2]

INTERNAL EXAMINER: DR D.J. FISHER
EXTERNAL EXAMINER: PROF P. GLENDINNING