UNIVERSITY OF SURREY©

B. Sc. Undergraduate Programmes in Mathematical Studies
M. Math. Undergraduate Programmes in Mathematical Studies

Level HE2 Examination

Module MS219 Algebra and Codes

Time allowed – 2 hours Autumn Semester 2007

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) For which values of q does a finite field with q elements exist? [2]

(ii) For which values of q is the field in part (i) equal to $(\mathbb{Z}_q, +_q, \times_q)$? [1]

(iii) List the elements of $\mathbb{Z}_{15}$ which have multiplicative inverses. [3]

(b) State the conditions for a relation $\sim$ on a set S to be an **equivalence relation**. [4]

(c) V is a vector space and U is a subspace of V.

A relation is defined on V as follows: $v \sim w$ if and only if $w - v \in U$.

(i) Show that $\sim$ is an equivalence relation on V. [6]

(ii) State the usual name and notation for the equivalence classes of $\sim$, and for the set of these equivalence classes. [4]

(iii) Define the operations which make the set of equivalence classes into a vector space. [2]

(d) Let V be the vector space of all polynomials in t over $\mathbb{F}_3$, let $U = \{(t^2+t+1)\mathrm{g} \ : \ \mathrm{g} \in V\}$ and define $\sim$ on V as in part (c).

(i) Describe the equivalence classes in this case, showing that there are 9 of them. [5]

(ii) Determine whether or not $2t^3 + t + 1 \sim t^3 + t + 2$. [3]

Question 2

(a) Define the terms:

  (i) the **minimum distance** $d(C)$ of a code C, [2]

  (ii) the **weight** of a codeword in a code C. [2]

(b) Let C be a linear code.

  Prove that $d(C)$ is equal to the smallest weight of a non-zero codeword. [7]

(c) (i) Define the **binary Hamming code** $\mathrm{Ham}(r, 2)$. [2]

  (ii) State the dimensions of a generating matrix for $\mathrm{Ham}(r, 2)$. [2]

  (iii) Write down a parity-check matrix for $\mathrm{Ham}(3, 2)$.
  Using your matrix, find the syndrome of 1101101. [5]

(d) C is the subspace of ${\mathbb{F}_3}^5$ spanned by the set
  $\{(1, 1, 1, 2, 1), (0, 1, 2, 1, 2), (0, 0, 1, 1, 1)\}$.

  (i) How many elements does C have? [1]

  (ii) Determine whether 11111 is a codeword in C. [6]

  (iii) Determine whether 11111 is a codeword in the dual code of C. [3]

Question 3

(a) Let N be the set of matrices of the form $\begin{pmatrix} a & b\sqrt{3} \\ -b\sqrt{3} & a \end{pmatrix}$ where $a, b \in \mathbb{Z}$.

  Show that N is a commutative subring of $M_2(\mathbb{R})$. [8]

(b) Let $(R, +, \cdot)$ and $(S, \oplus, \times)$ be rings.

  (i) State what is meant by a **ring homomorphism** from R to S. [3]

  (ii) Let $\phi : R \to S$ be a ring homomorphism.
  Prove that the kernel of ϕ is an ideal of S. [6]

(c) Let $\phi : \mathbb{R}[t] \to M_2(\mathbb{R})$ be defined by $\phi : \mathrm{f} \mapsto \begin{pmatrix} \mathrm{f}(0) & 0 \\ \mathrm{f}'(0) & \mathrm{f}(0) \end{pmatrix}$,
  where f' is the derivative of f.

  (i) Show that ϕ is a ring homomorphism. [6]

  (ii) Find the kernel and the image of ϕ and state, with reasons, whether ϕ is injective and/or surjective. [7]

Question 4

(a) Let R be a commutative ring with unity. State what is meant by saying that R is

(i) an **integral domain**, [2]

(ii) a **principal ideal domain**, [3]

(iii) a **unique factorisation domain**. [3]

(b) Let D be an integral domain and let $a, b \in D$ be such that $a \mid b$ and $b \mid a$.
Prove that $b = ua$ where u is a unit in D. [6]

(c) Let D be an integral domain and let $a \in D$ be non-zero and not a unit.

(i) State the meaning of the notation $\langle a \rangle$. [1]

(ii) Prove that $\dfrac{D}{\langle a \rangle}$ is an integral domain only if a is irreducible in D. [7]

(d) Let K be a field and let I be a non-trivial ideal of the polynomial ring $K[t]$.
Prove that I is a principal ideal and identify a generator of I.
[You may assume the division algorithm for polynomials.] [8]

Question 5

(a) Let $\mathrm{f} = t^4 + 1 \in \mathbb{F}_5[t]$.

(i) Show that f has no zeros in $\mathbb{F}_5$. [3]

(ii) By considering factors of the form $t^2 + a$, show that f is reducible over $\mathbb{F}_5$. [3]

(b) (i) State what is meant by a **polynomial code** of length n, and a **generator** of such a code. [4]

(ii) Let h and g be polynomials such that $\mathrm{h}(t)\mathrm{g}(t) = 1 + t^n$ in $\mathbb{F}_2[t]$.
Let $u = t + \langle 1 + t^n \rangle$ in $R_n = \dfrac{\mathbb{F}_2[t]}{\langle 1 + t^n \rangle}$.
Prove that if f is an element of the binary code generated by g then $\mathrm{h}(u)\mathrm{f}(u) = 0$ in R_n. [4]

(c) (i) State a necessary and sufficient condition for a polynomial code to be cyclic. [2]

(ii) Show that there is a binary cyclic code C generated by $1 + u + u^2 \in R_6$. [4]

(iii) Use a check polynomial to determine whether $1 + u^3$ is a codeword in C. [4]

(d) Let g be a generator of a binary polynomial code C and suppose $(1 + t) \mid \mathrm{g}(t)$ in $\mathbb{F}_2[t]$. Prove that every codeword in C has even weight. [6]

INTERNAL EXAMINER: Dr D.J. Fisher
EXTERNAL EXAMINER: Dr D. Chillingworth