Imperial College London

UNIVERSITY OF LONDON

BSc and MSci EXAMINATIONS (MATHEMATICS)

May-June 2006

This paper is also taken for the relevant examination for the Associateship.

M1P2

Algebra I

Date: Tuesday, 9th May 2006 Time: 2 pm – 4 pm

Credit will be given for all questions attempted but extra credit will be given for complete or nearly complete answers.

Calculators may not be used.

1. For each of the following statements, say whether it is true or false, and give a justification for your answer.

   (i) If, for $a, b \in \mathbb{Z}$, we define $a * b = a + b - 1$, then $(\mathbb{Z}, *)$ is a group.

   (ii) The largest order of any element of the symmetric group S_{12} is 42.

   (iii) Every group of size 4 is cyclic.

   (iv) The only elements of finite order in the group $(\mathbb{Q}^*, \times)$ are 1 and -1.

   (v) The linear code $C = \{x \in \mathbb{Z}_2^6 \,:\, Ax = 0\}$ with check matrix

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

   has minimum distance 3.

   (vi) Let C be the code in (v) above. If a codeword in C is sent, one error is made in transmission, and the received word is 100101, then the error is in the second bit.

2. (a) Let p be a prime number. Define $\mathbb{Z}_p^*$, and prove that it is a group under multiplication.

   (b) Prove that if p is a prime number, then $n^p \equiv n \bmod p$ for all integers n. (You may use any standard results from group theory provided you state them clearly.)

   (c) Find an integer x between 0 and 20 such that $2^{100} \equiv x \bmod 21$.

   (d) Find all positive integers less than 100 which divide $3^{17} - 1$.

3. (a) Let V be a vector space, and let $\{v_1, \ldots, v_k\}$ be a set of vectors in V. Define what is meant by the following statements:

   $\{v_1, \ldots, v_k\}$ is a *linearly independent* set,

   $\{v_1, \ldots, v_k\}$ is a *linearly dependent* set,

   $\{v_1, \ldots, v_k\}$ is a *spanning set* for V,

   $\{v_1, \ldots, v_k\}$ is a *basis* of V.

   (b) If $\{v_1, \ldots, v_k\}$ is a spanning set for V, and v is any vector in V, prove that the set $\{v_1, \ldots, v_k, v\}$ is linearly dependent.

   (c) If $\{v_1, \ldots, v_k\}$ is a linearly independent set in V, and $\{v, v_1, \ldots, v_k\}$ is linearly dependent, prove that v lies in the span of $\{v_1, \ldots, v_k\}$.

   (d) Let W be the following subspace of $\mathbb{R}^4$:

$$W = \{x \in \mathbb{R}^4 \,:\, Ax = 0\}, \text{ where } A = \begin{pmatrix} 1 & 1 & -1 & 1 \\ -1 & 0 & 1 & 2 \\ 1 & 3 & -1 & 7 \end{pmatrix}.$$

   Find a basis of W.

4. (a) Let V be a vector space, and let U and W be subspaces of V. Define $U \cap W$ and $U + W$, and prove that they are subspaces of V.

   (b) State (but do not prove) a result linking the dimensions of the subspaces U, W, $U \cap W$ and $U + W$.

   (c) Let U and W be 4-dimensional subspaces of $\mathbb{R}^6$, with $U \neq W$. Prove that $U \cap W$ has dimension 2 or 3. Give examples to show that both possibilities can occur.

   (d) Let U, W and X be 5-dimensional subspaces of $\mathbb{R}^7$. Prove that

$$U \cap W \cap X \neq \{0\}.$$

5. (a) Let V be a finite-dimensional vector space with a basis $B = \{v_1, \ldots, v_n\}$, and let $T : V \to V$ be a linear transformation.

   (i) Define the matrix $[T]_B$ of T with respect to B.

   (ii) Define what is meant by an eigenvector of T.

   (iii) Show that the matrix $[T]_B$ is diagonal if and only if B consists of eigenvectors of T.

   (b) Let V be the vector space consisting of all polynomials of degree at most 2 over $\mathbb{R}$. Define the linear transformation $T : V \to V$ by

$$T(p(x)) = p(1 + x) + p(1 - x) \quad \text{for all } p(x) \in V.$$

   Find the eigenvectors of T.

   Does there exist a basis B of V such that the matrix $[T]_B$ is diagonal?