M1P2 ALGEBRA I

1. Define what is meant by the order of an element of a group.

(a) (i) Explain how to find the order of a permutation from its cycle shape. (No proof is required.)

(ii) Find the order of the permutation

$$(1\,2\,4\,5\,6)\,(2\,3\,5)\,(4\,7) \in S_7.$$

(iii) Give an example of an element of order 60 in the group S_{12}.

(iv) How many elements of order 3 are there in the group S_6 ?

(b) Suppose that G is a finite group which contains elements of each of the orders 1,2,3,4,5,6,7,8.

Prove that $|G| \geq 840$.

Give an example of a group G with $|G| = 840$ such that G contains elements of each of the orders 1,2,3,4,5,6,7,8.

(*You may use any standard results provided you state them clearly.*)

2. (a) What is the remainder when 5^{111} is divided by 23 ?

(b) What is the inverse of the element [13] in the group $\mathbb{Z}_{97}^*$?

(c) Find all integers between 1 and 100 which divide $5^{17} - 1$.

(d) Let p and q be distinct prime numbers, and let n be an integer which is not divisible by p or by q. Prove that

$$n^{(p-1)(q-1)} \equiv 1 \bmod pq.$$

(*You may use any result you need from the lectures without proof, provided you state it clearly.*)

3. (a) Let u, v, w be vectors in a vector space V. Prove the following results.

(i) If $v + w,\ u + w,\ u + v$ span V then u, v, w span V.

(ii) If u, v, w span V then $v + w,\ u + w,\ u + v$ span V.

(b) (i) Show that the linear code $C = \{x \in \mathbb{Z}_2^8 : Ax = 0\}$ with check matrix

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

corrects 2 errors. (You may use any standard results you require, provided you state them clearly.)

(ii) Let C be the code in the previous part. A codeword $c \in C$ is sent, two errors are made in transmission, and the received word is

$$01011011.$$

Find the codeword c.

4. Let V, W be vector spaces. Define what is meant by a linear transformation $T : V \to W$. Define also the kernel $\operatorname{Ker} T$ and the image $\operatorname{Im} T$.

Prove the rank-nullity theorem: $\dim(\operatorname{Ker} T) + \dim(\operatorname{Im} T) = \dim V$.

Now let V be the vector space of all polynomials of degree at most 3 over $\mathbb{R}$, and define $T : V \to V$ by

$$T(p(x)) = p(x+1) + p(x-1) - 2p(x) \qquad \text{for all } p(x) \in V.$$

Giving your justification, calculate the dimensions of $\operatorname{Ker} T$ and $\operatorname{Im} T$.

5. Let V be a finite-dimensional vector space, let B be a basis of V, and let $T : V \to V$ be a linear transformation. Define the matrix $[T]_B$ of T with respect to the basis B.

Now let V be the vector space consisting of all 2×2 matrices over $\mathbb{R}$ with the usual addition and scalar multiplication. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and define $T : V \to V$ by

$$T(X) = AX \qquad \text{for all } X \in V.$$

(a) Show that T is a linear transformation.

(b) Write down a basis of V, and find the matrix $[T]_B$.

(c) Find the eigenvalues and eigenvectors of T.

(d) Does there exist a basis C of V such that the matrix $[T]_C$ is diagonal?