Question 1

Let m and p be the polynomials in $\mathbf{Z}_5[t]$ defined by

$$m(t) = t^3 + t + 1$$
$$p(t) = t + 3.$$

(i) Prove that m is irreducible over $\mathbf{Z}_5$. [3]

(ii) Find a highest common factor of m and p and express it in the form $um + vp$, where u and v are polynomials in $\mathbf{Z}_5[t]$. [3]

(iii) Write down the multiplicative inverse of $p + \langle m \rangle$ in $\mathbf{Z}_5[t]/\langle m \rangle$. [2]

(iv) Write down the number of elements in the quotient field $\mathbf{Z}_5[t]/\langle m \rangle$. [2]

Question 2

In this question you may assume that

$$\mathbf{Z} \times \mathbf{Z} = \{(m, n) : m, n \in \mathbf{Z}\}$$

is a ring, with componentwise addition and multiplication.

Let K be an ideal in $\mathbf{Z} \times \mathbf{Z}$. Let I and J be defined by

$$I = \{m \in \mathbf{Z} : (m, n) \in K \text{ for some } n \in \mathbf{Z}\},$$
$$J = \{n \in \mathbf{Z} : (m, n) \in K \text{ for some } m \in \mathbf{Z}\}.$$

(i) Show that I is an ideal in $\mathbf{Z}$. [5]

For the final part of this question you may assume that J is also an ideal in $\mathbf{Z}$.

(ii) Show that $K = I \times J$. [5]

Question 3

Let K, W and V be the following subsets of complex numbers, where $i^2 = -1$.

$$K = \left\{a + b\sqrt{7} + ci + di\sqrt{7} : a, b, c, d \in \mathbf{Q}, i^2 = -1\right\},$$
$$W = \left\{a + b\sqrt{7} + ci : a, b, c \in \mathbf{Q}, i^2 = -1\right\},$$
$$V = \left\{a + b\sqrt{7} : a, b \in \mathbf{Q}\right\}.$$

You may assume that K and V are fields under addition and multiplication of complex numbers, that K and V are vector spaces over $\mathbf{Q}$ and that $i \notin \mathbf{R}$.

(i) Prove that W is a vector subspace of K. [4]

(ii) Prove that $\{1, \sqrt{7}\}$ is a basis for V over $\mathbf{Q}$. [2]

(iii) Prove that $\{1, \sqrt{7}, i\}$ is a basis for W over $\mathbf{Q}$. [2]

(iv) Prove that W is not a subfield of K. [2]

Question 4

(i) Find two elements of the permutation group $\mathbf{S}_6$ which are both of order 6 and which are *not* conjugate in $\mathbf{S}_6$. [2]

(ii) Let p and q be two distinct primes. Prove that there exist two elements of the permutation group $\mathbf{S}_{pq}$ which are both of order pq and which are *not* conjugate in $\mathbf{S}_{pq}$. [4]

(iii) Prove that, if $p \in \mathbf{N}$ is prime, then all elements of order p in $\mathbf{S}_p$ are conjugate in $\mathbf{S}_p$. [4]