Question 1

Let m and p be the polynomials in $\mathbf{Z}_3[t]$ defined by

$$m(t) = t^3 + 2t + 1$$
$$p(t) = t + 2.$$

(i) Prove that m is irreducible over $\mathbf{Z}_3$. [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 $\mathbf{Z}_3[t]$. [3]

(iii) Write down the multiplicative inverse of $p + \langle m \rangle$ in $\mathbf{Z}_3[t]/\langle m \rangle$. [2]

(iv) Write down the number of elements in the quotient field $\mathbf{Z}_3[t]/\langle m \rangle$. [2]

Question 2

Let R be a commutative ring with a multiplicative identity (denoted by 1).
An ideal P in R is said to be a *prime ideal* of R if and only if the quotient ring R/P is an integral domain.

(i) Prove that if P is a prime ideal of R and $x, y \in R$ then

$$xy \in P \quad \text{if and only if} \quad x \in P \text{ or } y \in P.$$ [6]

(ii) Show that the principal ideal $\langle p \rangle$ is a prime ideal if and only if for all a and b in R, if p divides ab then either p divides a or p divides b. [4]

Question 3

Let S be a set such that $\mathbf{Q} \subseteq S \subseteq \mathbf{R}$.

(i) Suppose that S is a subring of $\mathbf{R}$. Prove that S is also a $\mathbf{Q}$-vector subspace of the $\mathbf{Q}$-vector space $\mathbf{R}$. [4]

(ii) Give an example to show that S may be a $\mathbf{Q}$-vector subspace of $\mathbf{R}$ but not a subring of $\mathbf{R}$. [3]

(iii) Give an example to show that S may be a subring of $\mathbf{R}$ but not a subfield of $\mathbf{R}$. [3]

Question 4

(i) Prove that all elements of order 5 in the symmetric group $\mathbf{S}_5$ are conjugate in $\mathbf{S}_5$. [3]

(ii) Prove that if n is a prime number then all elements of order n in the symmetric group $\mathbf{S}_n$ are conjugate in $\mathbf{S}_n$. [4]

(iii) Give an example to show that the conclusion of part (ii) may be false if n is not prime. [3]

Question 5

Let N be a normal subgroup of a group G, and let $Z(G)$ be the centre of G.

(i) Prove that if $|N| = 2$ then $N \subseteq Z(G)$.

Hint: consider the conjugates of the elements of N. [5]

(ii) Prove that if $Z(G/N) \cong 1$ then $Z(G) \subseteq N$. [5]