Question 3 (Unit 15) – 50 marks

Let K be a field of order 81 whose prime subfield is $\mathbf{Z}_3$, and let $f(t) = t^2 + t + 2$, $g(t) = t^2 + 2t + 2$ and $h(t) = t^2 + 1$ be three polynomials in $\mathbf{Z}_3[t]$.

(i) Show that f, g and h are irreducible over $\mathbf{Z}_3$ and, furthermore, that these are the *only* three monic quadratic polynomials in $\mathbf{Z}_3[t]$ which are irreducible over $\mathbf{Z}_3$. [6]

(ii) Show that the polynomial $m(t) = t^4 + t + 2$ in $\mathbf{Z}_3[t]$ is irreducible over $\mathbf{Z}_3$. [7]

(iii) Prove that there is an element α in K such that α has minimum polynomial m over $\mathbf{Z}_3$. [15]

(iv) Show that there is an automorphism σ of K such that

$$\sigma(\alpha) = \alpha^3 + \alpha^2 + \alpha.$$ [12]

(v) Show that the field $\langle\sigma\rangle^\dagger$, the fixed field of the group of automorphisms of K generated by σ, has nine elements. [10]

Question 4 (Unit 16) – 50 marks

Part A

(i) Let K be an ordered field. Prove, using the definition of an ordered field given in Section 16.1 (HB p. 45), that if M is the subset of non-negative elements of K, i.e. $M = \{x \in K : 0 \leq x\}$, then:

(a) for each $x \in K$, either $x \in M$ or $-x \in M$;

(b) if $x \in K$, then $x \in M$ and $-x \in M$ if and only if $x = 0$;

(c) if $x, y \in M$, then $x + y \in M$ and $xy \in M$. [15]

(ii) The field K becomes an ordered field under each of two ordering relations $\leq_1$ and $\leq_2$, and M_1 and M_2 are the corresponding subsets of non-negative elements of K. Show that if $\leq_1$ and $\leq_2$ are distinct (so that for some $x, y \in K$, $x \leq_1 y$ but $x \not\leq_2 y$), then $M_1 \neq M_2$. [8]

(iii) Writing $\leq$ for the usual ordering relation on $\mathbf{Q}$, and M for the non-negative elements of $\mathbf{Q}$, suppose that $\leq'$ is another ordering relation which makes $\mathbf{Q}$ an ordered field, and that M' is the corresponding subset of non-negative elements of $\mathbf{Q}$. Use (a), (b) and (c) of part (i) above and the equation

$$(-1)^2 = 1^2 = 1$$

to show that $1 \in M'$, and hence prove, by induction or otherwise, that every integer in M is also in M'.

Prove that $M' = M$.

What can you therefore deduce about the ordering relations on $\mathbf{Q}$ which make $\mathbf{Q}$ an ordered field? [16]

Part B

(i) Deduce from a theorem of *Unit 16* that if a, b and n are positive integers, then $\mathbf{Q}(\sqrt[n]{a}, \sqrt[n]{b}) : \mathbf{Q}$ is a simple field extension. [3]

(ii) In a splitting field for the polynomial $(t^2 + 2)(t^2 + 3)$ over $\mathbf{Z}_5$, α is a zero of $t^2 + 2$ and β is a zero of $t^2 + 3$. Prove that $(\alpha + \beta)^3 + (\alpha + \beta) = 2\beta$, and hence, or otherwise, show that $\mathbf{Z}_5(\alpha, \beta) : \mathbf{Z}_5$ is a simple extension. [8]