Questions 3 and 4 both refer to the field $\mathbf{F}_8$, which is the field formed by the set $\{0, 1, a, b, c, d, e, f\}$ under the operations of addition $(+)$ and multiplication $(\times)$ defined by the following two tables. There is no need for you to prove that $\mathbf{F}_8$ is a field.

$+$	0	1	a	b	c	d	e	f
0	0	1	a	b	c	d	e	f
1	1	0	c	f	a	e	d	b
a	a	c	0	d	1	b	f	e
b	b	f	d	0	e	a	c	1
c	c	a	1	e	0	f	b	d
d	d	e	b	a	f	0	1	c
e	e	d	f	c	b	1	0	a
f	f	b	e	1	d	c	a	0

$\times$	0	1	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0
1	0	1	a	b	c	d	e	f
a	0	a	b	c	d	e	f	1
b	0	b	c	d	e	f	1	a
c	0	c	d	e	f	1	a	b
d	0	d	e	f	1	a	b	c
e	0	e	f	1	a	b	c	d
f	0	f	1	a	b	c	d	e

Note that the field $\mathbf{Z}_2 = \{0, 1\}$ is a subfield of $\mathbf{F}_8$.

Question 3 (Unit 7) – 25 marks

(i) Prove that the polynomial m in $\mathbf{Z}_2[t]$ defined by

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

is irreducible over $\mathbf{Z}_2$. [3]

(ii) Show that if $\beta \in \mathbf{F}_8$ is a zero of m, then β^2 is also a zero of m. [4]

(iii) Show that $a \in \mathbf{F}_8$ is a zero of m. [2]

(iv) Verify that the multiplicative group of $\mathbf{F}_8$ is a cyclic group generated by the element $a \in \mathbf{F}_8$, and deduce that $\mathbf{F}_8 = \mathbf{Z}_2(a)$. (The multiplicative group of the field $\mathbf{F}_8$ is the abelian group $(\mathbf{F}_8 \setminus \{0\}, \times)$, given in the definition of a field on page 6 of *Unit 2*.) [3]

(v) Show that m has three distinct zeros in $\mathbf{F}_8$. [4]

(vi) Show that the order of the Galois group $G = \Gamma(\mathbf{F}_8 : \mathbf{Z}_2)$ is 3, and write down the value of $\phi(a)$ for each $\phi \in G$. [3]

(vii) For each $\phi \in G$, find the image under ϕ of each of the eight elements of $\mathbf{F}_8$. [6]

Question 4 (Unit 8) – 25 marks

Question 3 has shown that the field $\mathbf{F}_8$ contains all the zeros of the polynomial m defined by $m(t) = t^3 + t + 1 \in \mathbf{Z}_2[t]$, and that $\mathbf{F}_8 = \mathbf{Z}_2(a)$ where $a \in \mathbf{F}_8$ is a zero of m. You may assume both of these results in answering this question.

(i) (a) Prove that the field extension $\mathbf{F}_8 : \mathbf{Z}_2$ is a normal field extension. [5]

(b) Find the minimum polynomial of the element $c \in \mathbf{F}_8$ over $\mathbf{Z}_2$. [6]

(c) Verify that $\mathbf{F}_8 : \mathbf{Z}_2$ is a normal extension by showing that the minimum polynomial of $c \in \mathbf{F}_8$, which you found in part (i)(b), has all its zeros in $\mathbf{F}_8$. [2]