SECTION A

1. Let R be a commutative ring with identity. Say what is meant by a *unit* in R. In each of the following cases say whether the element r is a unit in the ring R. Justify your answers.

(i) $R = \mathbf{Z}$, $r = -1$,

(ii) $R = \mathbf{Z}/7\mathbf{Z}$, $r = 5$,

(iii) $R = \mathbf{Z}/8\mathbf{Z}$, $r = 5$,

(iv) $R = \mathbf{Z}[x]$, $r = x^2 + 1$,

(v) $R = \mathbf{Z}[i]$, $r = 1 + i$. [9 marks]

2. Let R be a commutative ring with identity. Say what is meant by an *irreducible* element of R. In each of the following cases say whether the polynomial $f(x)$ is irreducible in the ring R. Justify your answers.

(i) $R = (\mathbf{Z}/5\mathbf{Z})[x]$, $f(x) = x^3 + 2x^2 + x + 2$,

(ii) $R = \mathbf{Z}[x]$, $f(x) = x^4 + x - 1$,

(ii) $R = \mathbf{R}[x]$, $f(x) = x^4 + x - 1$. [9 marks]

3. List the elements of the ring $R = (\mathbf{Z}/2\mathbf{Z})[x]/\langle x^2+x+1\rangle$ in standard form. Write down the multiplication table of R. Is R a field? Justify your answer.

[9 marks]

4. Find the greatest common divisor $g = \gcd(5, 1+3i)$ of 5 and $1+3i$ in $\mathbf{Z}[i]$. Also find $a, b \in \mathbf{Z}[i]$ with

$$5 = ag \quad \text{and} \quad 1 + 3i = bg$$

and $c, d \in \mathbf{Z}[i]$ such that

$$g = 5c + (1 + 3i)d.$$

[9 marks]

5. Explain what is meant by a t-(v, k, r)-design. Give examples of

a) a 1-$(5, 2, 4)$-design; b) a 2-$(7, 3, 1)$-design. [9 marks]

6. Let C be the code with check matrix

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

a) Give the length, dimension and an effective lower bound on the weight of this code. Also, give the number of words in the code and a lower bound on the number of errors that can be corrected.

b) Determine which of the following are words of C, and correct any which are not words of C, assuming only one error:

(i) 1110001,

(ii) 1101110. [10 marks]

SECTION B

7. Define what is meant by a *ring homomorphism* from a ring R to a ring S. (Both R and S are commutative rings, each with a multiplicative identity.)

For each map φ below decide whether it is a ring homomorphism. You should give brief justifications of your answers and, in the cases where φ is a ring homomorphism, determine the kernel of φ.

(i) $\varphi : \mathbf{Z} \to \mathbf{Z}/6\mathbf{Z} : m \mapsto m \bmod 6$,

(ii) $\varphi : \mathbf{Z} \to \mathbf{Z} : m \mapsto m^2$,

(iii) $\varphi : \mathbf{Q}[x] \to \mathbf{Q} : p(x) \mapsto p(3)$,

(iv) $\varphi : (\mathbf{Z}/2\mathbf{Z})[x] \to (\mathbf{Z}/2\mathbf{Z})[x] : p(x) \mapsto p(x)^2$.

[15 marks]

8. Let $R = (\mathbf{Z}/2\mathbf{Z})[x]$ and let $I \subset R$ be the ideal generated by

$$f(x) = x^4 + x^3 + 1.$$

You may assume that $f(x)$ is irreducible in R.

a) Write down the number of elements in the quotient ring R/I and the number of elements in $(R/I)^*$. State the possible orders of elements in $(R/I)^*$.

b) Show that the element $x+1$ has order 5 in $(R/I)^*$, and that the element $x^3 + x$ has order 3 in $(R/I)^*$.

c) Write $(x+1)(x^3+x)$ in standard form and deduce the order of x^2+x+1.

[15 marks]

9. a) Find the minimal polynomial of $\sqrt{2}$ in $\mathbf{Q}[x]$. This means showing that the polynomial you find is irreducible. Also show that $\alpha = \sqrt{2} + \sqrt{7}$ is a zero of a polynomial of degree 4 in $\mathbf{Q}[x]$. Finally, by computing $\alpha(\alpha^2 - 9)$, or otherwise, show that $\sqrt{2} \in \mathbf{Q}[\alpha]$.

b) Now assume that $\sqrt{7} \notin \mathbf{Q}[\sqrt{2}]$ and find

(i) $[\mathbf{Q}[\sqrt{2}] : \mathbf{Q}]$,

(ii) $[\mathbf{Q}[\alpha] : \mathbf{Q}[\sqrt{2}]]$,

(iii) $[\mathbf{Q}[\alpha] : \mathbf{Q}]$.

[15 marks]

10. a) A panel of three tasters has nine ice-creams to test. Testing takes place in four sessions. In each session, each taster takes three of the ice-creams to compare. Each pair of ice-creams is tested against one another in exactly one session (by which we mean there is some taster who tastes both ice-creams in the pair in that session). By considering lines in $(\mathbf{Z}/3\mathbf{Z})^2$ or otherwise, draw up a schedule to show that this is possible.

b) Now suppose that there are sixteen ice-creams, four tasters, and five sessions. Explain why a schedule is still possible, but do NOT write it down in detail.

[15 marks]

11. a) Write down the irreducible degree 2 polynomial in $(\mathbf{Z}/2\mathbf{Z})[x]$, and the three irreducible degree 4 polynomials in $(\mathbf{Z}/2\mathbf{Z})[x]$. You need not justify your answer. Hence factorize $x^{15}+1$ into irreducibles in $(\mathbf{Z}/2\mathbf{Z})[x]$, explaining what theory you are using.

b) Now take the factor $f(x) = (x+1)(x^4+x+1)$ of $x^{15}+1$, and find $g(x)$ such that $f(x)g(x) = x^{15}+1$. Hence, find the check matrix of the cyclic code with generator $f(x)$, and show that it has weight ≥ 3.

c) Give the number of cyclic codes of length 15 with dimension 7, and the number with dimension 8, giving a brief explanation.

[15 marks]