SECTION A

1. Give the definition of a *zero-divisor* in a ring.

For each of the following, state, with justification, whether it is a zero-divisor in the stated ring.

(a) $3+4i$ in $\mathbf{Z}[i]$;

(b) 4 in $\mathbf{Z}/15$;

(c) x in $\mathbf{Q}\,[x]/(x^2)$;

(d) 9 in $\mathbf{Z}/12$. [9 marks]

2. Factor the following into irreducibles in the indicated rings:

(a) 5 in $\mathbf{Z}[i]$;

(b) x^3+4x+4 in $\mathbf{Z}/5\,[x]$;

(c) $x^3+5x-105$ in $\mathbf{Z}\,[x]$. [9 marks]

3. (a) State the definition of *field* (in terms of the definition of "ring").

(b) Let R be the ring $\mathbf{Z}/2\,[x]$ and I the ideal of R generated by x^3+x+1. Make a list of the elements of R/I, and prove directly from the definition that it is a field.

[9 marks]

4. (a) Find the point of intersection of the lines $x+2y+2z=0$ and $2x+z=0$ in $\mathbf{P}^2(\mathbf{Z}/3)$.

(b) Find the line that passes through the points $(0:4:1)$ and $(3:1:2)$ in $\mathbf{P}^2(\mathbf{Z}/5)$. [9 marks]

5. Define *t-(v,k,r)-design*. Give an example of

(a) a 1-(6, 3, 2)-design;

(b) a 2-(4, 3, 2)-design.

[9 marks]

6. Consider a code over $\mathbf{Z}/3$ with check matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 2 \\ 2 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 1 \end{pmatrix}.$$

(a) State its dimension and its information rate.

(b) Show that 01211 is in the code and that 21110 is not.

(c) Decode the word 21110, assuming at most one error. [10 marks]

SECTION B

7. State the definition of *ring homomorphism*.

For each of the following ϕ, state whether it is a homomorphism from the given R to the given S. Justify your answers.

(a) $R = \mathbf{Z}/3$, $S = \mathbf{Z}$, $\phi(0) = 0, \phi(1) = 1, \phi(2) = 2$.

(b) $R = \mathbf{Z}[x]$, $S = \mathbf{R}$, $\phi(f) = f(1/2)$.

(c) $R = \mathbf{Z}/15$, $S = \mathbf{Z}/3$, $\phi(n) = n \pmod 3$.

(d) $R = \mathbf{Z}/2$, $S = \mathbf{Z}/10$, $\phi(0) = 0, \phi(1) = 5$.

[15 marks]

8. Define *ideal*. For each of the following rings R and subsets S of R, state whether S is an ideal of R. Justify your answers.

(a) $R = \mathbf{Z}[i]$, S is the subset consisting of all elements with nonnegative imaginary part.

(b) $R = \mathbf{Z}/5[x]$, S is the set of polynomials whose coefficients of 1 and x are 0.

(c) $R = \mathbf{R}$, $S = \mathbf{Z}$.

(d) $R = \mathbf{Z}/2[x]/(x^9 - 1)$, S is the set of classes of polynomials f with $f(1) = 0$.

[15 marks]

9. Let $R = \mathbf{Z}/2\,[x]$, let $f(x) = x^4 + x + 1$ (which you may assume to be irreducible in R).

(i) Give the number of elements of R/I and the number of elements of $(R/I)^*$. State the possible orders of elements of $(R/I)^*$.

(ii) Show that $x^2 + x$ has order 3 in $(R/I)^*$.

(iii) Write $(x^2 + x)(x^3 + x)$ and $(x^2 + x) + (x^3 + x)$ in standard form as an element of R/I.

(iv) Given that $x^3 + x$ has order 5, state the order of $(x^2 + x)(x^3 + x)$. Justify your answer. [15 marks]

10. (i) Show that neither (a) a 2-$(14, 5, 2)$-design, nor (b) a 2-$(15, 6, 1)$ design cannot exist.

(ii) Show that the set of sets

$$\{\{i, i+1, i+4, i+6\} : i \in \mathbf{Z}/13\}$$

constitutes a 2-$(13, 4, 1)$-design. [15 marks]

11. In this problem, let R be the ring $\mathbf{Z}/5\,[x]$.

(i) Find a polynomial $g \in R$ such that $g \cdot (x^3 + 3x^2 + 2x + 4) = x^6 - 1$.

(ii) Let C be the cyclic code of length 6 over $\mathbf{Z}/5$ generated by $x^3 + 3x^2 + 2x + 4$. Write down a check matrix for C.

(iii) State a theorem about check matrices that guarantees that C corrects at least one error.

(iv) Assuming at most one error, correct these words: 231204, 111102, 121303.

[15 marks]