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) $R = \mathbf{Q}$, $r = 5$,

(ii) $R = \mathbf{Z}/11\mathbf{Z}$, $r = 5$,

(iii) $R = \mathbf{Z}/12\mathbf{Z}$, $r = 5$,

(iv) $R = \mathbf{Q}[x]$, $r = x^2 - 3$,

(v) $R = \mathbf{Z}[i]$, $r = 2 + i$. [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 is irreducible in the ring R. Justify your answers.

(i) $R = (\mathbf{Z}/2\mathbf{Z})[x],\ f(x) = x^3 + x^2 + x + 1$,

(ii) $R = \mathbf{Q}[x],\ f(x) = x^4 + 3x + 1$,

(ii) $R = \mathbf{R}[x],\ f(x) = x^2 + 3x + 1$. [9 marks]

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

[9 marks]

4. Find the greatest common divisor $\gcd(f, g)$ of $f = x^3 + 6x^2 + 12x + 5$ and $g = x^2 + 5x + 6$ in $\mathbf{Q}[x]$. Also find $a, b \in \mathbf{Q}[x]$ with

$$\gcd(f, g) = af + bg.$$

[9 marks]

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

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

6. Let C be the code with check matrix

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

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) 1000111. [10 marks]

SECTION B

7. Define what is meant by an *ideal* I in a ring R and what is meant by the *quotient ring* R/I.

For each ideal I of the ring R below describe the quotient ring R/I. You should give *brief* justifications of your answers.

(i) $I = 13\mathbf{Z}$, $R = \mathbf{Z}$;

(ii) $I = \langle 2 \rangle$, $R = \mathbf{Z}[x]$;

(iii) $I = \{f : f(3) = 0\}$, $R = \mathbf{Z}[x]$;

(iv) $I = \langle x^2 + 1 \rangle$, $R = \mathbf{Z}[x]$.

[15 marks]

THE UNIVERSITY of LIVERPOOL

8. Let $R = (\mathbf{Z}/3\mathbf{Z})[x]$ and let $I \subset R$ be the ideal generated by

$$f(x) = x^2 + 2x + 2.$$

Show 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 $(R/I)^*$.

b) Say what is meant by the *order* of a unit r in R and explain why it is finite. State the possible orders of elements in $(R/I)^*$.

c) Compute the square of each element of R/I. Hence, or otherwise, compute the order of each element in $(R/I)^*$.

[15 marks]

9. Let $N : \mathbf{Z}[\sqrt{-5}] \to \mathbf{N}$ be given by $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Show that N is multiplicative i.e. for any two elements $r, s \in \mathbf{Z}[\sqrt{-5}]$ we have

$$N(rs) = N(r)N(s).$$

Show that

1. r is a unit in $\mathbf{Z}[\sqrt{-5}]$ if and only if $N(r) = 1$;
2. there are no elements r with $N(r) = 2$ in $\mathbf{Z}[\sqrt{-5}]$.

Using these results, or otherwise, show that the elements 2 and $1 \pm \sqrt{-5}$ are irreducible in $\mathbf{Z}[\sqrt{-5}]$. By considering the two factorisations

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in $\mathbf{Z}[\sqrt{-5}]$ show that 2 is not a prime in $\mathbf{Z}[\sqrt{-5}]$.

[15 marks]

10. a) A renewable energy company wants to test 7 different designs of wind turbine to see which is the most efficient. They have 7 different test sites. By considering points and lines in $\mathbf{P}^2(\mathbf{Z}/2\mathbf{Z})$, or otherwise, draw up a schedule in which 3 turbines are tested at each site and each pair of turbines are compared at precisely one site.

b) Now suppose the company has 9 turbines to test, but that they can only use 3 of the test sites. They decide to carry out the tests in 4 sessions. In each session 3 turbines are tested at each of the 3 sites. By considering points and lines in $(\mathbf{Z}/3\mathbf{Z})^2$, or otherwise, draw up a schedule for these tests in such a way that each pair of turbines are tested simultaneously at precisely one site.

[15 marks]

11. a) Let n be an integer greater than 1 and let

$$x^n + 1 = g(x)h(x)$$

in $(\mathbf{Z}/2\mathbf{Z})[x]$, where $g(x)$ has degree d and

$$h(x) = \sum_{k=0}^{n-d} h_k x^k.$$

Write down a check matrix for the cyclic code generated by $g(x)$.

b) Now take $n = 10$. Find all the possible generators $g(x) \in (\mathbf{Z}/2\mathbf{Z})[x]$ of cyclic codes of length 10. (You may write each $g(x)$ as a product of polynomials if you wish, and are NOT required to work this product out.)

c) Show there is a unique cyclic code of length 10 and dimension 4. By considering its check matrix show that it has weight at least 3.

[15 marks]