SECTION A

1. Write down the multiplication table of the ring $\mathbf{Z}_7$. Identify any zero divisors in this ring, and any units. Give the multiplicative inverse of each unit.

[9 marks]

2. In each of the following rings R, show that the g.c.d. of a and b in the ring R is 1 up to associates, and write $1 = ma + nb$ for m, $n \in R$.

a) $R = \mathbf{R}[x]$, $a = x^3 + 1$, $b = x^2 + x - 1$,

b) $R = \mathbf{Z}[i]$, $a = 7 + 2i$, $b = 4 - 3i$.

[13 marks]

3. Determine which of the following polynomials are irreducible in the given rings. Give brief reasons.

a) $x^2 + 1$ in $\mathbf{C}[x]$.

b) $x^2 + 1$ in $\mathbf{R}[x]$.

c) $x^3 + 2$ in $\mathbf{Q}[x]$.

d) $x^3 + 2$ in $\mathbf{R}[x]$.

[6 marks]

4. Let F be a finite field.

(i) Write down the general equation of a line in F^2, and the general equation of a line through $(x_0, y_0) \in F^2$.

(ii) Find all points in $\mathbf{Z}_3^2$ on the line $x + 2y + 1 = 0$, and all lines through the point $(2, 1)$ in $\mathbf{Z}_3^2$.

[10 marks]

5. State, whether the following are true or false. No explanations are required, but if you attempt an explanation and subsequently get an answer wrong, you might gain some credit.

a) There is a field with four elements.

b) There is a field with six elements.

c) There is a 1-design with parameters $(10, 7, 3)$.

d) There is a 2-design with parameters $(7, 3, 1)$.

e) There is a code in $\mathbf{Z}_2^7$ with 16 words which corrects one error.

[8 marks]

6. Let C be the code in $\mathbf{Z}_2^7$ with check matrix

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

Give the property of this matrix which ensures that the code C corrects one error. Determine which of the following words are in C, and, assuming at most one error, correct those which are not.

a) 1111111, b) 0010010.

[9 marks]

SECTION B

7. (i) Let R be a commutative ring. Define what it means for S to be a *subring* of R and what it means for S to be an *ideal* in R.

(ii) Now let $R = \mathbf{Z}[\sqrt{2}]$. Determine which of the following are subrings of R and which are ideals, giving brief reasons.

a) $S = \{n\sqrt{2} : n \in \mathbf{Z}\}$.

b) $S = \{2x : x \in \mathbf{Z}[\sqrt{2}]\}$.

c) $S = \{m + n\sqrt{2} : m,\ n \in \mathbf{Z},\ m \text{ is odd}\}$.

d) $S = \{m + n\sqrt{2} : m,\ n \in \mathbf{Z},\ m \text{ is even}\}$.

(iii) Define $\varphi : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}_2$ by

$$\varphi(m + n\sqrt{2}) = m \bmod 2.$$

Assuming that φ is a homomorphism, find $\operatorname{Ker}(\varphi)$.

[15 marks]

8. (i) Show that $x^4 + x + 1$ is irreducible in $\mathbf{Z}_2[x]$. You may assume that $x^2 + x + 1$ is the only irreducible degree two polynomial in $\mathbf{Z}_2[x]$.

(ii) Let

$$J = (x^4 + x + 1)\mathbf{Z}_2[x],\ F = \mathbf{Z}_2[x]/J.$$

Give the number of elements in F, the number of elements in F^*, and the possible orders of elements in F^*.

(iii) Let $\alpha = J + x \in F^*$. Show that the order of α is 15. Give all integers n between 1 and 14 inclusive such that α^n has order 15.

(iv) Consider the equation

$$X^4 + X + 1 = 0. \tag{1}$$

Show that if $X = \beta \in F$ satisfies (1), then so does β^2.

[15 marks]

9. (i) Give the formal definition of a 2-design with parameters (v, k, r).

(ii) A supermarket is doing market research on seven annual plants (alyssum, begonias, cornflowers, d, e, f, g) by planting three plots of different varieties in each of seven locations, so that each pair of varieties is grown together in at least one location. Draw up a schedule to show that this is possible, by using points and lines in $P^2(\mathbf{Z}_2)$, making clear what the points and lines represent, and what properties of points and lines in $P^2(\mathbf{Z}_2)$ are used.

[15 marks]

10. (i) Factorise $x^7 + 1$ in $\mathbf{Z}_2[x]$ as a product of irreducibles. Hence, or otherwise, find all the factors of $x^7 + 1$ in $\mathbf{Z}_2[x]$.

(ii) For one of the generators $g(x)$ of a cyclic code over $\mathbf{Z}_2$ of length 7 and dimension 4, write $x^7 + 1 = g(x)h(x)$, and write down the corresponding generator and check matrices. Explain why the code corrects one error.

[15 marks]

11. (i) State Kirkman's Schoolgirls Problem.

(ii) Let A be the incidence matrix for the 2-design arising in Kirkman's Schoolgirls Problem, with columns indexed by schoolgirls and rows indexed by sets. State the number of rows and columns of this matrix. Let E be the matrix of the same dimensions as A with 1 in every entry, and let $A' = E - A$. Let C_1 be the code whose words are the rows of A and of A'. Find the minimum distance of C_1, explaining your answer briefly.

(iii) Repeat this exercise for the code C_2 whose words are the columns of A and of A'.

[15 marks]