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

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

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

(iii) Let S be as in (ii)a), so that

$$R/S = \{S, S+1, S+\sqrt{2}, S+1+\sqrt{2}\}.$$

Write down the multiplication table for R/S. Using addition or otherwise, show that R/S is not isomorphic to $\mathbf{Z}_4$.

[20 marks]

2. (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 $\alpha = J + x$. 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

$$X^4 + X + 1 = 0. \qquad (1)$$

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

(v) Again, let $\alpha = J + x$. Find the minimal polynomials in $\mathbf{Z}_2[X]$ satisfied by α^{-1} and α^5.

[*Hint*: Find f such that $f(X^{-1}) = X^{-4}(X^4 + X + 1)$, and show that α^5 is a zero of $X^3 + 1$.]

[20 marks]

3. a) 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.

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

c) Let $\mathbf{B}$ be a 2-design with parameters (v, k, r). Write down two restrictions on (v, k, r). Show that if $r = 1$ and $k = 3$ then v is of the form $6n + 1$ or $6n + 3$ for some integer n.

[20 marks]

4. a) Show that $g(x) = x^3 + x + 1$ is an irreducible factor of $x^7 + 1$ in $\mathbf{Z}_2[x]$. Write $x^7 + 1 = g(x)h(x)$, and write down the generator and check matrices for the length 7 cyclic code with generator $g(x)$.

b) (i) Show that if m and n are positive integers and $m \mid n$ then $x^m + 1$ is a factor of $x^n + 1$ in $\mathbf{Z}_2[x]$.

(ii) Describe the connection between irreducible polynomials of degrees dividing n in $\mathbf{Z}_2[x]$, and the polynomial $x^{2^n-1} + 1$.

(iii) Show that 23 divides 2047. Hence, or otherwise, show that $x^{23} + 1$ must be a product in $\mathbf{Z}_2[x]$ of $x + 1$ and two irreducible polynomials of degree 11. Do not attempt to find these polynomials.

(iv) Show that 2 is an element of the group Q of quadratic residues mod 23. Hence or otherwise, show that if α is an element of some field of characteristic two and is a zero of the polynomial $x^{23} + 1$ in $\mathbf{Z}_2[x]$, then

$$F(\alpha) = F(\alpha)^2, \text{ where } F(\alpha) = \sum_{i \in Q} \alpha^i.$$

[20 marks]

5. (i) State Kirkman's Schoolgirls Problem. For integers i with $1 \leq i \leq 35$, let

$$X_i = \{\mathbf{x_i}, \mathbf{y_i}, \mathbf{z_i}\} \subset \mathbf{Z}_2^4 \setminus \{\mathbf{0}\},$$

where

$$\mathbf{z_i} = \mathbf{x_i} + \mathbf{y_i}.$$

Show that

$$\mathbf{z_i} + \mathbf{x_i} = \mathbf{y_i},$$

$$\mathbf{z_i} + \mathbf{y_i} = \mathbf{x_i}.$$

Explain why Kirkman's Schoolgirls Problem is solved if the sets X_i exist and are all different and X_{5n+i} for $1 \leq i \leq 5$ are disjoint, for each $1 \leq n \leq 7$.

(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'.

[20 marks]

6. Find the minimum polynomials of $\alpha = \sqrt{3}$ and $\beta = \sqrt{3} + \sqrt{5}$ in $\mathbf{Q}[x]$. This means showing that these polynomials are irreducible in each case, being careful to state any results that you use. By computing β^2 and $\beta(\beta^2 - 8)$ or otherwise, show that $\alpha \in \mathbf{Q}[\beta]$. Hence, or otherwise, find

$$[\mathbf{Q}[\alpha] : \mathbf{Q}],\ [\mathbf{Q}[\beta] : \mathbf{Q}],\ [\mathbf{Q}[\beta] : \mathbf{Q}[\alpha]].$$

[20 marks]

7. A *line* in $\mathbf{Z}_3^3$ is a set of the form

$$\{\mathbf{v_0} + t\mathbf{v_1} : t \in \mathbf{Z}_3\} = \ell(\mathbf{v_0}, \mathbf{v_1}\},$$

where$\mathbf{v_0}$, $\mathbf{v_1} \in \mathbf{Z}_3^3$ and $\mathbf{v_1} \neq (0,0,0)$.

(i) Write down the total number of points in $\mathbf{Z}_3^3$, and the number of points on any line in $\mathbf{Z}_3^3$.

(ii) Show that (1) and (2) are equivalent:

$$\ell(\mathbf{v_0}, \mathbf{v_1}) = \ell(\mathbf{v'_0}, \mathbf{v'_1}), \tag{1}$$

and

$$\mathbf{v'_0} = \mathbf{v_0} + t_0\mathbf{v_1}\,,\ \mathbf{v'_1} = s_0\mathbf{v_1} \text{ for some } t_0,\ s_0 \in \mathbf{Z}_3,\ s_0 \neq 0. \tag{2}$$

Hence, or otherwise, find the number of pairs $(\mathbf{v'_0}, \mathbf{v'_1})$ with $\ell(\mathbf{v'_0}, \mathbf{v'_1}) = \ell(\mathbf{v_0}, \mathbf{v_1})$, and find the number of lines in $\mathbf{Z}_3^3$. Also, find the number of lines in $\mathbf{Z}_3^3$ through $\mathbf{v_0}$.

(iii) Given two distinct points (a_1, b_1, c_1) , $(a_2, b_2, c_2) \in \mathbf{Z}_3^3$, show that there is exactly one line $\ell(\mathbf{v_0}, \mathbf{v_1})$ between the points, and write down $\mathbf{v_0}$ and $\mathbf{v_1}$ in terms of (a_1, b_1, c_1) and (a_2, b_2, c_2) . Hence, or otherwise, show that the set of lines in $\mathbf{Z}_3^3$ is a 1-design with parameters (v, k, r) and a 2-design with parameters $(v, k, 1)$, for some v , k , r , and give the values of v , k , r .

[20 marks]

8. a) Define the *minimum distance* and *weight* of a linear code in $\mathbf{Z}_2^n$, and show that they coincide.

b) Let H be the check matrix of a linear code $C \subset \mathbf{Z}_2^n$.

(i) Show that if no column of H is identically 0 , then C has weight > 1 .

(ii) Show that if, in addition, no two columns of H are the same, then H has weight > 2 .

(iii) Show that if, in addition, the sum of any three columns of H is not identically zero, then C has weight > 3 .

(iv) Now let

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

Show that C has weight 4 . In particular, this means that you should find a codeword in C of weight 4 .

[20 marks]