SECTION A

1. Define a *unit* in a ring R with identity, and its *multiplicative inverse.*

Decide whether the following are units in the stated rings, giving reasons. If they are units, find their multiplicative inverse.

(a) in $R = \mathbf{Z}[\sqrt{2}]$, $a = \sqrt{2} - 1$

(b) in $R = \mathbf{Z}[\sqrt{2}]$, $a = (\sqrt{2} + 1)^{20}$

(c) in $R = \mathbf{Z}_{12}$, $a = 9$

(d) in $R = \mathbf{Z}[i]$, $a = 3 + i$.

[8 marks]

2. Find a greatest common divisor $c(x)$ of the polynomials $a(x) = x^4 + x + 2$ and $b(x) = x^2 + x + 3$ in $\mathbf{Z}_5[x]$. Find also $d(x), e(x), m(x), n(x) \in \mathbf{Z}_5[x]$ with

$$c(x) = a(x)m(x) + b(x)n(x), \qquad a(x) = d(x)c(x), \quad b(x) = e(x)c(x).$$

[8 marks]

3. Show that

$$a(x) = x^3 - 2x^2 + x + 3$$

is irreducible in $\mathbf{Z}[x]$. Decide whether or not it is irreducible in $\mathbf{Q}[x]$. Show that it is reducible in $\mathbf{Z}_5[x]$. Factorise it as a product of primes in $\mathbf{Z}_5[x]$. [8 marks]

4. In the projective plane $P^2(\mathbf{Z}_3)$ find:

(a) all points on the projective line $2X + Y + Z = 0$;

(b) all projective lines through the point $[2 : 1 : 1]$.

[8 marks]

5. Write down the multiplication table of the ring $\mathbf{Z}_2[x]/J$ in the following cases:

(a) $J = (x^2 + 1)\mathbf{Z}_2[x]$ (b) $J = (x^2 + x + 1)\mathbf{Z}_2[x]$.

[8 marks]

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

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

State a property for a check matrix which ensures that the corresponding code corrects one error; deduce that the code C given here does correct one error.

Determine which of the following words are in the code C; assuming at most one error, correct those which are not in C:

(a) 1001001, (b) 0010001.

[8 marks]

SECTION B

7. Let R be a commutative ring.
Give the definitions of *subring* and *ideal* of R.

Determine which of the following subsets are subrings of the given rings; also determine which of the following subsets are ideals of the given rings.

(a) $S = \mathbf{Z}$ in $R = \mathbf{Z}[i]$;
(b) $S = \{3m + 3ni \mid m, n \in \mathbf{Z}\}$ in $R = \mathbf{Z}[i]$;
(c) $S = \{2m + ni \mid m, n \in \mathbf{Z}\}$ in $R = \mathbf{Z}[i]$.

Let I be an ideal of $\mathbf{Z}[i]$, and let $z = a + ib$ be a nonzero element of I whose Euclidean valuation $|z|^2 = a^2 + b^2$ is minimal on I. Show that any $w \in I$ must be of the type $w = zw'$, for some element $w' \in \mathbf{Z}[i]$.

[15 marks]

8. Give the definition of *ring homomorphism.*
Consider $\varphi : \mathbf{R}[x] \to \mathbf{C}$ given by:

$$\varphi(p(x)) = p(i) \quad \forall p(x) \in \mathbf{R}[x].$$

(a) Show that φ is a ring homomorphism, and it is surjective.
(b) Find a polynomial $g(x)$ such that $\text{Ker}\varphi = g(x)\mathbf{R}[x]$.

[15 marks]

9.

a) Let $\mathbf{Z}_5^*$ denote the multiplicative group of $\mathbf{Z}_5$. Give the orders of all 4 elements of $\mathbf{Z}_5^*$.

b) Show that $x^2 + 2$ is irreducible in $\mathbf{Z}_5[x]$.

Now write $J = (x^2 + 2)\mathbf{Z}_5[x]$. Let $F = \mathbf{Z}_5[x]/J$ (which is a field) and let F^* be the multiplicative group of F.

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

d) Find the orders in F^* of

(i) $J + 2$ (ii) $J + (x + 2)$ (iii) $J + (2x + 4)$.

[15 marks]

10.

(a) A panel of 3 persons is testing 9 ice cream flavours. The testing is carried out in 4 sessions. In each session, each person tries 3 flavours. Each pair of flavours is tested by the same person in exactly one session. By considering lines in $\mathbf{Z}_3^2$, or otherwise, explain why a schedule is possible, and write down one.

(b) Would a schedule be possible for 16 ice cream flavours, a panel of 4 people testing them during 5 sessions? Give reasons (no need to write down the complete schedule).

[15 marks]

11.

(a) Decompose $x^7 + 1$ as product of prime factors in $\mathbf{Z}_2[x]$.

(b) Write down the generator for *one* of the two cyclic codes of length 7 and dimension 4. Also work out the check matrix for the code, and a linear basis. Can such a code correct one error? Justify your answer.

[15 marks]