SECTION A

1. Define a *zero divisor* of a ring, a *unit* in a ring R with identity and its *multiplicative inverse.*
Find all the zero divisors, units and their multiplicative inverse of the ring $\mathbf{Z}_{12}$.

[8 marks]

2. Find the g.c.d. c of elements a and b in the ring R, in each of the following examples. Also, find m and $n \in R$ such that $c = ma + nb$.

a) $R = \mathbf{Z}_2[x], \quad a = x^5 + x^2 + x, \quad b = x^4 + 1.$

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

[9 marks]

3. Find the minimal polynomial in $\mathbf{Q}[x]$ of

(i) $-1 + \sqrt{7}$, (ii) $\sqrt{2} - \sqrt{6}$.

In the second case, check that the polynomial that you find (which should be of degree four) is irreducible in $\mathbf{Q}[x]$.

[12 marks]

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

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

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

[7 marks]

5. Let J be the ideal $J = (1 + x^2 + x^3)\mathbf{Z}_2[x]$ of the ring $\mathbf{Z}_2[x]$. Write down the multiplication table of the quotient ring $\mathbf{Z}_2[x]/J$.

[8 marks]

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

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

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 or ideals of the given rings.

(a) $S = \{3f(x) \mid f(x) \in \mathbf{Z}[x]\}$ in $R = \mathbf{Z}[x]$;

(b) $S = \{3f(x) \mid f(x) \in \mathbf{Z}[x]\}$ in $R = \mathbf{Q}[x]$.

Let J be an ideal of $\mathbf{Q}[x]$, and let $c(x)$ be a nonzero element of J whose degree is minimal on J. Show that any $a \in J$ must be of the type $a = bc$, for some element $b \in \mathbf{Q}[x]$.

[15 marks]

8. Show that $f_1(x)$ and $f_2(x)$ are irreducible in $\mathbf{Z}_3[x]$, where

$$f_1(x) = x^2 + x + 2, \quad f_2(x) = x^2 + 1.$$

Let $y = 2x + 1$, where addition and multiplication are in $\mathbf{Z}_3[x]$. Express x in terms of y. Show that

$$f_1(y) = f_2(x).$$

Let $J_i = f_i(x)\mathbf{Z}_3[x]$ for $i = 1, 2$. Show that $X = J_1 + x$ is a solution of $f_1(X) = 0$, where the 0 on the righthand side of this equation is the zero element J_1 in the quotient ring $\mathbf{Z}_3[x]/J_1$.
Show that for any $g_1(x)$, $g_2(x) \in \mathbf{Z}_3[x]$,

$$J_1 + g_1(x) = J_1 + g_2(x) \quad \Leftrightarrow \quad J_2 + g_1(2x+1) = J_2 + g_2(2x+1).$$

Hence, or otherwise, find an isomorphism from $\mathbf{Z}_3[x]/J_1$ to $\mathbf{Z}_3[x]/J_2$, and write down the inverse of this isomorphism.

[15 marks]

9.

a) Let $\mathbf{Z}_7^*$ denote the multiplicative group of $\mathbf{Z}_7$. Give the orders of all 6 elements of $\mathbf{Z}_7^*$.

b) Show that $x^2 + 1$ is irreducible in $\mathbf{Z}_7[x]$.

Now write $J = (x^2 + 1)\mathbf{Z}_7[x]$. Let $F = \mathbf{Z}_7[x]/J$ (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) $J + x$ (ii) $J + (5x)$.

[15 marks]

10. (a) Three people are testing nine different bikes for market research. Testing takes place in four sessions. In each session, each person rides three of the bikes. Each pair of bikes is tried by a same person in exactly one session. By considering lines in $\mathbf{Z}_3^2$ or otherwise, draw up a schedule to show that this is possible.

(b) Now suppose that a different test is needed: 8 bikes will be tested by 14 people, with two people per session, anyone trying 4 bikes, so that each pair of bikes is tried by 3 different people. Show that a schedule is still possible, by considering planes in $\mathbf{Z}_2^3$ or otherwise. (Do not write down the complete schedule).

[15 marks]

11.

(a) Decompose $x^{12}+1$ as product of irreducibles in $\mathbf{Z}_2[x]$ (possibly by factorising $x^3+1 \in \mathbf{Z}_2[x]$ first).

(b) Find all factors $g(x)$ of degree five, and all factors $h(x)$ of degree seven. Write down the check matrices H of all the cyclic codes of length 12 and canonical generators $g(x) \in \mathbf{Z}_2[x]$ of degree five. Determine which of these codes correct one error.

[15 marks]