## SECTION A

**1.** Define *unit* and *multiplicative inverse*.

In each of the following, state whether the given element of the ring is a unit, and, if so, state its multiplicative inverse. No justification required.

(a) $x + 2$ in $\mathbf{Z}/5\,[x]$;

(b) $2x + 1$ in $\mathbf{Z}/4\,[x]$;

(c) $4$ in $\mathbf{Z}/7$;

(d) $7$ in $\mathbf{Z}/12$.

[9 marks]

**2.** Factor $f(x) = x^3 + 4x^2 + x + 1$ as a product of irreducibles in

(a) $\mathbf{Z}/3\,[x]$;

(b) $\mathbf{Z}/5\,[x]$;

(c) $\mathbf{Z}\,[x]$.

[9 marks]

**3.** Let $R$ be the ring $\mathbf{Z}/2\,[x]$, and let $I$ be the ideal $(x^3 + x^2, x^4 + x^3 + x^2)$.

(i) Give a single element of $R$ that generates $I$.

(ii) Write the multiplication table for the ring $R/I$.

[9 marks]

**4.** In the projective plane $\mathbf{P}^2(\mathbf{Z}/3)$, find:

(i) the line passing through $[1 : 0 : 2]$ and $[2 : 1 : 2]$;

(ii) all points on this line. [9 marks]

**5.** (i) State the definition of $t$-$(v, k, r)$-*design*.

(ii) Give an example of a 1-$(6, 4, 2)$-design.

(iii) Is your example from (ii) a 2-design? [9 marks]

**6.** (i) Factor $x^7 + 1$ into irreducibles over $\mathbf{Z}/2$.

(ii) Is there a cyclic code of dimension 5 and length 7 over $\mathbf{Z}/2$? If so, give a generator; if not, explain why not. [10 marks]

SECTION B

**7.** Define *subring*. For each of the following rings $R$ and subsets $S$, determine whether $S$ is a subring of $R$.

(a) $R = \mathbf{Z}/6$, $S = \{0, 3\}$;

(b) $R = \mathbf{Z}$, $S = \{n \in \mathbf{Z} : n \geq 0\}$;

(c) $R = \mathbf{C}$, $S = \{a + b\sqrt{-3} : a, b \in \mathbf{Z}\}$;

(d) $R = \mathbf{R}[x]$, $S$ is the subset of polynomials with coefficient 0 of $x$ and $x^2$. [15 marks]

**8.** Define a *homomorphism of rings*.

(i) Prove that the map $\phi : \mathbf{R}[x] \mapsto \mathbf{C}$ given by $\phi(f) = f(i)$ is a homomorphism.

(ii) Show that there is no homomorphism $\psi : \mathbf{C} \mapsto \mathbf{R}[x]$. (Hint: consider the equation $i^2 + 1 = 0$.) [15 marks]

**9.** (i) Does there exist a field with 12 elements?

(ii) State (but do not prove) a sufficient condition on a ring $R$ and a polynomial $f(x) \in R[x]$ for $R[x]/(f(x))$ to be a field. Use it to prove that there is a field of 27 elements. (If your condition doesn't allow you to do this, it isn't strong enough. Be sure to prove that this is actually the number of elements in the field you write down.) [15 marks]

**10.**(i) Write out a 2-$(9, 3, 1)$-design. (This means: write a set of 9 elements, then give the subsets that constitute the design.)

(ii) By considering lines in a plane over a finite field, or otherwise, show that there is a 2-$(21, 5, 1)$-design. It should not be necessary to list the sets that constitute the design.

[15 marks]

**11.**(i) Let $C$ be a $k$-dimensional code of length $n$ over a field of $q$ elements that corrects $s$ errors. Prove that

$$\sum_{i=0}^{s} \binom{n}{i} (q-1)^i \leq q^{n-k}.$$

(ii) In particular, verify that a code of length 9 over $\mathbf{Z}/2$ that corrects one error has dimension at most 5.

(iii) By giving the check matrix and stating an appropriate theorem, or otherwise, show that there does exist a code of length 9 and dimension 5 over $\mathbf{Z}/2$ that corrects one error.

[15 marks]