1. Give the definition of *ring homomorphism.*

Say which of the following are ring homomorphisms, giving reasons. In cases of positive answer, find $\operatorname{Ker}\varphi$ and $\operatorname{Im}\varphi$.

(a) $\varphi : M_2(\mathbf{R}) \to \mathbf{R}, \qquad \varphi(A) = \det A.$

(b) $\varphi : M_2(\mathbf{R}) \to \mathbf{R}, \qquad \varphi(A) = \frac{1}{2}\operatorname{Tr} A.$

(c) $\varphi : \mathbf{Z} \to \mathbf{Z}, \qquad \varphi(n) = n^3.$

(d) $\varphi : \mathbf{Z}_3[x] \to \mathbf{Z}_3[x], \qquad \varphi(p) = p^3.$

[20 marks]

2. Consider the set of matrices

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbf{R} \right\},$$

with the usual addition and multiplication of matrices.

(a) Show that S is a subring of the ring $M_2(\mathbf{R})$, and it is commutative. Is S an ideal of $M_2(\mathbf{R})$? Give reasons.

(b) Let I be the subset of S

$$I = \left\{ \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbf{R} \right\}.$$

Show that I is an ideal of S, and it is a principal ideal.

(c) Describe the quotient ring S/I, and show that it a field.

(d) Show that I is the only proper ideal of S.

[20 marks]

3. Consider the Euclidean domain $\mathbf{R}[x]$, and fix two nonzero polynomials $a, b \in \mathbf{R}[x]$ of it.

Denote by I the set $I = \{am + bn \mid m, n \in \mathbf{R}[x]\}$.

(a) Show that I is an ideal of $\mathbf{R}[x]$.

(b) Show that I is a principal ideal of $\mathbf{R}[x]$.

(c) Compute a generator for I in each of the following cases:

(i) $a = x^2 + x, \quad b = x^2 + 2x + 1;$

(ii) $a = x^2 + x, \quad b = x^5 - 2x + 1.$

[20 marks]

4. Let F be a field with characteristic p and p^n elements.

(a) Show that

$$\varphi : F \to F \quad \text{given by} \quad \varphi(a) = a^p$$

is an automorphism of F.

(b) Show that $\varphi = \mathrm{Id}_F \iff n = 1$.

(c) Show that $\mathrm{Id_F}$ is the *only* automorphism of $F \iff n = 1$.

[20 marks]

5.

Find the minimal polynomials in $\mathbf{Q}[x]$ of

$$\alpha = \sqrt{3} - 1, \qquad \beta = \sqrt{3} + i$$

and show that they are irreducible in $\mathbf{Q}[x]$.

Show that $\alpha \in \mathbf{Q}[\beta]$. Hence find the degrees

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

[20 marks]

6. Consider the polynomial $a(x) = x^3 - x^2 + 2x + 1$.

(a) Show that $a(x)$ is irreducible in $\mathbf{Z}[x]$. Decide whether it is reducible in $\mathbf{Q}[x]$ and in $\mathbf{Z}_3[x]$; give its factorisation into primes in each case where it is reducible.

(b) Consider any polynomial $b(x) \in \mathbf{Q}[x] \setminus \{0\}$, of degree at most 2. Explain why there exist two polynomials $m(x), n(x) \in \mathbf{Q}[x]$ with

$$a(x)m(x) + b(x)n(x) = 1.$$

(c) Now let $\alpha \in \mathbf{C}$ be a zero of $a(x)$, and let

$$\mathbf{Q}[\alpha] = \{p(\alpha) \mid p(x) \in \mathbf{Q}[x]\}.$$

Show that you can limit yourself to elements $p(x)$ of degree at most 2.
Show that any nonzero element $p(\alpha) \in \mathbf{Q}[\alpha]$ has a mutiplicative inverse in $\mathbf{Q}[\alpha]$. In particular find the inverse of $1 + \alpha^2$.

[20 marks]

7. Let F be a field with q elements.

(a) Find the number of points in $P^2(F)$.

(b) Find the number of lines in $P^2(F)$, and the number of points on each line.

(c) Describe how to realise a 2-design from the lines of $P^2(F)$, and give its parameters.

(d) For a general 2-design, give two necessary restrictions on its parameters (v, k, r).
From these restrictions determine what number of elements v a set may have to support a 2-design with parameters $r = 1, k = 3$. Do the same for the parameters $r = 2, k = 3$.

[20 marks]

8. Consider, for $n \in \mathbf{Z}, n > 1$, the polynomial $x^n + 1 \in \mathbf{Z}_2[x]$.
Let $g(x), h(x) \in \mathbf{Z}_2[x]$ be factors of $x^n + 1$ with $x^n + 1 = g(x)h(x)$.

(a) Describe how to build a cyclic code C from $g(x)$, and, by using the coefficients of $h(x)$, describe a check matrix H for C.
What is the code corresponding to $g(x) = 1$?
What is the code corresponding to $g(x) = x^n + 1$?

(b) Now take $n = 20$.
Factorise $x^{20} + 1 \in \mathbf{Z}_2[x]$ into irreducibles, and find all generators of cyclic codes of length 20.

(c) Consider a factorisation of $x^{20} + 1 = g(x)h(x)$ with $\deg h(x) = 14$.
Write down the number of rows and of columns of the corresponding check matrix.
How many errors will this code correct? Give reasons.

[20 marks]