1. Define *ring homomorphism*, and for each of the following ϕ say that it is a ring homomorphism from R to S or explain why it is not. If it is, also indicate the kernel and image of ϕ, and if the kernel is a principal ideal also give a generator of that ideal. Proofs are not required.

(a) $R = \mathbf{Z}[i]$, $S = \mathbf{Z}$, $\phi(a + bi) = a^2 + b^2$.

(b) $R = \mathbf{Z}[x]$, $S = \mathbf{R}$, $\phi(f(x)) = f(\sqrt{2})$.

(c) $R = \mathbf{Z}/2$, $S = \mathbf{Z}/6$, $\phi(0) = 0$ and $\phi(1) = 3$.

(d) $R = \mathbf{Z}$, $S = \mathbf{Z}/5$, $\phi(a) = a \bmod 5$. [20 marks]

2. (i) Let R be a ring and $r,\ s \in R$. Prove that $(r, s) = \{ar + bs : a, b \in R\}$ is an ideal of R.

(ii) Now let R be a Euclidean domain, and let t be a nonzero element of (r, s) such that $d(t)$ is as small as possible. Show that $(r, s) = (t)$ in R.

(iii) Now let $R = \mathbf{Z}[i]$ (which is a Euclidean domain, but you need not prove it) and find $t \in R$ such that $(t) = (4 + 7i, 7 + 9i)$ in R. [20 marks]

3. In this problem let $R = \mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}$, and let $S = \mathbf{Z}/7$.

(i) Prove that the function $\phi : R \mapsto S$ defined by $\phi(a + b\sqrt{2}) = a + 3b \pmod 7$ is a homomorphism, and check that the kernel of ϕ contains the ideal $(3 - \sqrt{2})$.

(ii) Show that $(3 - \sqrt{2}) | 7$ in R.

(iii) By writing $a + b\sqrt{2} = (a + 3b) - b(3 - \sqrt{2})$, or otherwise, show that every element of $\ker \phi$ is a multiple of $3 - \sqrt{2}$. [20 marks]

4. In this problem let $\alpha = \sqrt{3} + 1$ and let $\beta = \frac{\sqrt{3}-1}{2}$.

(i) Find the minimal polynomials m_α and m_β of α and β over $\mathbf{Q}$.

(ii) Find rational numbers a, b with $\alpha = a + b\beta$, and rational numbers c, d with $\beta = c + d\alpha$.

(iii) Prove that $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$. [20 marks]

5. In this problem, you may assume that $x^3 + 2x + 2$ is an irreducible polynomial in $\mathbf{Z}/3\,[x]$, so that $F = \mathbf{Z}/3\,[x]/(x^3 + 2x + 2)$ is a field of $3^3 = 27$ elements.

(i) Find the multiplicative inverse of $x + 1$ in F.

(ii) List the possible orders of elements of F^*.

(iii) Show that 2 is not a square in F. (Hint: what would the order of its square root be, if it were?)

(iv) Show that $2x^2$ is not a square in F. [20 marks]

6. State with justification whether designs with the following parameters exist. (If you believe that a design exists, you should explain how to construct it or refer to a specific theorem that guarantees its existence, but you do not have to write out the sets.)

(a) a 1-$(8, 6, 3)$-design;

(b) a 2-$(19, 3, 1)$-design;

(c) a 2-$(15, 6, 1)$-design;

(d) a 2-$(31, 6, 1)$-design. [20 marks]

7. Let F be a finite field with n elements.

(i) Find the number of points in $\mathbf{P}^3(F)$.

(ii) Find the number of planes in $\mathbf{P}^3(F)$.

(iii) Prove that the set of planes in $\mathbf{P}^3(F)$ gives a 2-design, and determine its parameters. [20 marks]

8. Define the *weight* of a word in a code.

(i) Let C be a linear code over $\mathbf{Z}/2$ of length n and dimension k, and suppose that C has words of odd weight. Prove that the set of codewords of even weight in C is a linear code of length n and dimension $k - 1$, and show how to describe the check matrix of this code in terms of that of C.

(ii) Show by example that the set of codewords of C whose weight is a multiple of 3 may not be a linear code. [20 marks]