1. Define *ring homomorphism*. For each of the following ϕ determine, with justification, whether or not it is a ring homomorphism from R to S.

(a) $R = \mathbf{Q}[x]$, $S = \mathbf{C}$, $\phi(f) = f(i)$.

(b) $R = \mathbf{Z}[i]$, $S = \mathbf{Z}/3$, $\phi(a + bi) = a + b \pmod 3$.

(c) $R = \mathbf{Z}/3$, $S = \mathbf{Z}/15$, $\phi(0) = 0$, $\phi(1) = 10$, $\phi(2) = 5$.

(d) $R = \mathbf{Z}/9$, $S = \mathbf{Z}/3$, $\phi(i) = i \pmod 3$.

[20 marks]

2. (i) Let a and b be nonzero elements of a Euclidean domain R with the degree function d, and let g be the element of R whose degree is least among all nonzero elements of R of the form $ra + sb$, where $r, s \in R$. Show that (a) g divides a (it follows that g divides b, by symmetry); (b) if h is an element of R that divides a and b then h divides g.

(ii) Now let $R = \mathbf{Z}[i]$ with the degree function $d(m + ni) = m^2 + n^2$ (you may assume that R is a Euclidean domain for this degree function). Also let $a = 6 + 2i$ and $b = -3 + 5i$. Find, with justification, an element g with the properties described in (ii) above, and give elements r, s such that $g = ar + bs$.

[20 marks]

3. Define *irreducible* and *prime*. For each of the following elements of the given rings, write the element as a product of irreducibles in the ring.

(a) $-7 + 11i$ in $\mathbf{Z}[i]$;

(b) $x^5 + x^2 + 1$ in $\mathbf{Z}/2\,[x]$;

(c) $3x^5 + 8x^3 + 7x^2 - 5$ in $\mathbf{Q}\,[x]$;

(d) $3x^3 + 18x^2 - 3x + 12$ in $\mathbf{Z}\,[x]$.

(Hint for (a): every irreducible of $\mathbf{Z}[i]$ whose norm is less than 10 is an associate of one of these: $1 + i, 1 + 2i, 2 + i, 3$. Hint for (c) and (d): you may wish to reduce the polynomials modulo certain primes.)

[20 marks]

4. In this problem let $R = \mathbf{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbf{Z}\}$, and let $S = \mathbf{Z}/11$.

(i) Prove that the function $\phi : R \mapsto S$ defined by $\phi(a + b\sqrt{3}) = a + 5b \pmod{11}$ is a homomorphism, and check that the kernel of ϕ contains the ideal $(1 + 2\sqrt{3})$.

(ii) Show that $(1 + 2\sqrt{3})|11$ in R.

(iii) By writing $a + b\sqrt{3} = a(1 + 2\sqrt{3}) - (2a + 10b - 11b)\sqrt{3}$, or otherwise, show that every element of $\ker \phi$ is a multiple of $1 + 2\sqrt{3}$.

[20 marks]

5. (i) State a property of an element f of $\mathbf{Z}/5\,[x]$ that guarantees that $\mathbf{Z}/5\,[x]/(f)$ is a field, and such that $f = x^2 + 3$ has this property. Show that $f = x^2 + 3$ has the property.

(ii) Now let R be the ring $\mathbf{Z}/5\,[x]/(x^2 + 3)$. Find the multiplicative orders of x and $3x + 2$ in R. State whether x is a square, and whether $3x + 2$ is a square.

(iii) Calculate $x(3x + 2)$ in R, and determine its order. (Hint: use your results from (ii) to find the order.)

[20 marks]

6. In this problem let $f = x^3 - 3x^2 + x + 3$.

(i) Find a prime p so that the reduction of f mod p is reducible, and give the factorization of the reduction.

(ii) Show, using reduction modulo an appropriate prime, that f is irreducible in $\mathbf{Q}\,[x]$.

(iii) Now let $R = \mathbf{Q}\,[x]/(f)$. Find the multiplicative inverse of (the class of) $x^2 - x - 2$ in R, or show that it has none.

(iv) Now let $\alpha \in \mathbf{C}$ be a root of f (you may assume that such α exists). Using your results from above, or otherwise, express $1/(\alpha^2 - \alpha - 2)$ in the form $a + b\alpha + c\alpha^2$, where a, b, c are rational numbers.

[20 marks]

7. (i) Say what it means to *develop* a subset of $\mathbf{Z}/n$.

(ii) Show that developing the subset $\{0, 1, 4, 6\}$ of $\mathbf{Z}/13$ produces a 2-$(13, 4, 1)$-design.

(iii) Show that it is not possible to obtain a 2-design by developing a 3-element subset of $\mathbf{Z}/13$.

(iv) Show that, on the other hand, the 26 sets obtained by developing the two subsets $\{0, 1, 4\}$ and $\{0, 2, 7\}$ constitute a 2-$(13, 3, 1)$-design.

[20 marks]

8. (i) Factor $x^7 + 1$ into irreducibles over $\mathbf{Z}/2\,[x]$.

(ii) Give a generator for a cyclic code of length 7 and dimension 3 over $\mathbf{Z}/2$, and write a check matrix for it.

(iii) Prove that this code has minimum weight 4.

(iv) State the number of errors corrected by this code.

[20 marks]