Rings Fields and Combinatorics

Answer all questions from section A and
three questions from section B

January 1997

Section A

1. (a) In $\mathbf{Q}[x]$ find polynomials $q(x)$ and $r(x)$ such that

$$x^6 + x^5 + x^3 + x^2 + 1 = q(x)(x^3 - 1) + r(x)$$

where either $r(x) = 0$ or the degree of $r(x)$ is less than that of $x^3 - 1$

(b) In $\mathbf{Q}[x]$, divide $f(x) = x^5 - x^4 - x^3 + x$ by $x + 2$ and show that the remainder is $f(-2)$.

(c) In the field of complex numbers, find the nearest Gaussian integer to $\dfrac{5-i}{2+3i}$.
Hence or otherwise find Gaussian integers

$$a + bi, c + di(a, b, c, d \in \mathbf{Z})$$

such that $5 - i = (2 + 3i)(a + bi) + (c + di)$ where $c^2 + d^2 < 13$.

[9 marks]

2. Decide, giving reasons, in which of the following cases A is (i) a subring of B and (ii) an ideal of B

   (a) $A = \mathbf{Z}, B = \mathbf{Q}$

   (b) $A = \{f(x^2) : f \in B\}, B = \mathbf{R}[x]$

   (c) $A = \{2n (\mathrm{mod}\, 8) : n \in B\}, B = \mathbf{Z}_8$

[9 marks]

3. Prove that the polynomial x^2+x+1 is irreducible in $\mathbf{F}_2[x]$. Let α be a zero of x^2+x+1 in a suitable extension of $\mathbf{F}_2$. Prove that the four elements $\{0, 1, \alpha, 1+\alpha\}$ form a field of four elements, and write down its multiplication table.

[9 marks]

4. Show that the projective plane over $\mathbf{F}_2$ has seven points and seven lines, and write down an incidence matrix of points and lines for this plane. Write down a Steiner triple system with seven varieties.

[9 marks]

5. Find three distinct irreducible monic polynomials of degree 2 in $\mathbf{Z}[x]$ which are also distinct and irreducible modulo 3. Show that they can be chosen so that two of these

are also irreducible modulo 2, and the third is the square of a linear factor modulo 2.

[9 marks]

6. Let $\mathcal{C}$ be a set of codewords in $\mathbf{F}_2^6$ such that

   (a) $110110 \in \mathcal{C}$;

   (b) $\mathcal{C}$ is a group under addition;

   (c) $\mathcal{C}$ is cyclic.

   Show that the smallest possible set $\mathcal{C}$ consists of four words, and list them. Show also that the minimum distance of $\mathcal{C}$ is 4 and that it can detect one error and correct three. Show that 101000 has at least two errors, but that there is a unique nearest codeword.

[10 marks]

Section B

7. In $\mathbf{Q}[x]$ let $f(x) = x^6 - x^5 - x^4 + x^3 + x^2 - x - 1$ and $g(x) = x^5 + x^4 - 2x^2 - 2x - 1$.

   Find polynomials $q(x)$ and $r(x)$ such that $f = gq + r$ where either $r = 0$ or the degree of r is less than that of g.

   Show that any common divisor of g and r is also a common divisor of f and g.

   By calculating the greatest common divisor of g and r, find the greatest common divisor $h(x)$ of f and g.

   Also find polynomials $a(x), b(x)$ such that $h = af + bg$.

   [15 marks]

8. In $\mathbf{Q}[x]$, divide $x^9 + 1$ by $x^6 + x^3 + 1$.

   Show that there is a cyclic code of length 9 generated by $x^6 + x^3 + 1$ over $\mathbf{F}_2$.

   Find a generator matrix and a parity check matrix for this code. Show that it has eight words altogether, and find the weight of each codeword. Find the number of errors which this code (i) detects and (ii) corrects.

   By calculating Hamming distances, or otherwise, show that 100100111 has at least two errors, but has a unique nearest code word.

   [15 marks]

9. Let

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

Show that H is the parity check matrix for a linear code $\mathcal{C}$ over $\mathbf{F}_2$. Make a table of syndromes and coset leaders for $\mathcal{C}$.

Write down a generator matrix for $\mathcal{C}$, find the minimum distance of $\mathcal{C}$ and the number of errors it can (i) detect (ii) correct. Correct the following received code words:

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

[15 marks]

10. Show that the affine plane over $\mathbf{F}_3$ has nine points and twelve lines. Draw up an intersection table of points and lines, in which the parallel lines are grouped together.

(a) Nine children are to walk out daily in three groups of three. Show how to arrange schedules for four successive days so that no two children are in the same group on more than one occasion.

(b) A bar committee of four members tests twelve brands of beer over three successive nights, each member drinking three pints of different brands on each evening. Show how to arrange that each possible pair of beers is compared by one member of the committee on one occasion.

[15 marks]

11. Show that $x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1)$ over $\mathbf{F}_2$.

Show that the quadratic residues modulo 7 are 1, 2 and 4, and the non-residues are 3, 5 and 6.

Show that any non-zero member of $\mathbf{F}_8$ satisfies the equation $x^7 - 1 = 0$. Show that there exists α, a root of this equation, also satisfying $\alpha^3 + \alpha + 1 = 0$.

Let $q(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$. Show, by means of the equation $\alpha^3 = 1 + \alpha$ that $q(x) = x^3 + x + 1$. Deduce that the cyclic code of length seven generated by $q(x)$ is a quadratic residue code, and show (quoting any necessary general theorem) that it has minimum distance 3.

[15 marks]