Rings Fields and Combinatorics

2MP46, June 1996

Section A

1. (a) In the ring $\mathbf{Q}[x]$ of polynomials in the variable x with rational coefficients

   i. find polynomials $q(x)$ and $r(x)$ such that

   $$x^6+x^5+x^4+3x^3+x^2+x+1 = q(x)(x^3+x^2+1)+r(x)$$

   and either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $x^3 + x^2 + 1$.

   ii. divide $f(x) = x^6+x^3+1$ by x^2+1, and verify that the remainder $r(x)$ satisfies the equation $r(i) = f(i)$.

   (b) Find the nearest gaussian integer to $\dfrac{11+7i}{1-4i}$ and hence find gaussian integers $a+ib$, $c+id$ such that

   $$11 + 7i = (1 - 4i)(a + ib) + (c + id)$$

   where $|c + id| < |1 - 4i|$.
   Also find gaussian integers $(e+if)$, $(g+ih)$ such that

   $$(11 + 7i) = (1 + 4i)(e + if) + (g + ih)$$

2. Decide, giving reasons, in which of the following cases S is a subring of R.

   (a) $S = \mathbf{Z}, R = \mathbf{Q}$
   (b) $S = \{ f(x) : f \in \mathbf{Z}[x],\ \text{degree of } f \text{ is odd} \}, R = \mathbf{Z}[x]$
   (c) $S = \{ f(x) : f \in \mathbf{Z}[x],\ \text{degree of } f \text{ is even} \}, R = \mathbf{Z}[x]$
   (d) $S = \{ 0, 2, 4 \}, R = \mathbf{Z}_6$

3. Decide, giving reasons, in which of the following cases S is an ideal of R

   (a) $S = \{ f(x) : f(x) \in \mathbf{Z}[x], f(0) \text{ is even} \}, R = \mathbf{Z}[x]$
   (b) $S = \{ f(x) : f(x) \in \mathbf{Z}[x], f(0) \text{ is odd} \}, R = \mathbf{Z}[x]$
   (c) $S = \{ (1 + x^2)f(x) : f(x) \in \mathbf{Z}[\mathbf{x}] \}, R = \mathbf{Z}[x]$
   (d) $S = \{ 0, 2, 4 \}, R = \mathbf{Z}_6$

4. Express the polynomial $x^3 - 1$ as a product of irreducible polynomials in each of the following rings:

   (a) $\mathbf{Z}[x]$
   (b) $\mathbf{C}[x]$
   (c) $\mathbf{Z}_6[x]$
   (d) $\mathbf{Z}_7[x]$

5. Find all the irreducible polynomials of degree 2 over $\mathbf{F}_3$

6. Let the set $\mathcal{C}$ of codewords in $\mathbf{F}_2^8$ be given by 00000000, 10101010, 01010101 and 11111111. Show that this is (i) a linear space code, and (ii) a cyclic code. Find a generating polynomial. Find the minimum distance between distinct codewords. Show that this code can detect three errors. Find the number of errors which the code can correct.

   If a code word was received as 11101111 what can be said about the original codeword?

Section B

7. In $\mathbf{Q}[x]$, prove that if $f = gq + r$, then $\text{hcf}(f, g) = \text{hcf}(g, r)$

   Let $f(x) = x^6 + x^5 + x^4 - x^2 - x - 1$ and $g(x) = x^5 + 2x^4 + 2x^3 + x^2$. Calculate q, r such that $f = gq + r$ and either $r = 0$ or $\partial^o r < \partial^o g$.

   Hence or otherwise determine the highest common factor h of f and g, and find polynomials u, v such that $h = uf + vg$.

8. Divide $x^6 + 2$ by $x^2 + x + 1$ over the field $\mathbf{Q}$.

Explain how code words of length n over a field $\mathbf{F}$ correspond to elements of the quotient ring $\mathbf{F}[X]/\mathbf{F}[X](X^n - 1)$.

Working over the field $\mathbf{F}_3$, show that there is a *cyclic* code $\mathcal{C}$ of length 6 with generator polynomial $x^2 + x + 1$.

Write down a generator matrix, and a parity check matrix for $\mathcal{C}$.

Show that (by consideration of dimension) $\mathcal{C}$ has 81 code words.

Show that, if $\mathcal{C}$ contained a word of weight 1, it would have 729 words.

Show that the word corresponding to $x^3 + 2$ belongs to $\mathcal{C}$.

Find the minimum weight of $\mathcal{C}$, and state the number of errors which $\mathcal{C}$ can detect.

9. Let

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

Show that H is a parity check matrix for a code $\mathcal{C}$ over $\mathbf{F}_2$. Find a generator matrix for $\mathcal{C}$ and draw up a table of syndromes and coset leaders.

Correct the following received code words:

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

10. Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and let $A = \{1, 2, 8\}$, $B = \{1, 4, 7\}$, $C = \{2, 3, 4\}$, $D = \{2, 7, 9\}$, $E = \{3, 8, 9\}$, $F = \{4, 6, 8\}$, $G = \{1, 3, 5\}$, $H = \{1, 6, 9\}$, $J = \{2, 5, 6\}$, $K = \{3, 6, 7\}$, $L = \{4, 5, 9\}$, $M = \{5, 7, 8\}$. Show how this configuration is linked to the affine plane over $\mathbf{F}_3$. Decide whether this configuration can be used to solve the nine schoolgirls problem, giving reasons for your answer.

11. Make a list of the quadratic residues modulo 7, and verify that they form a cyclic group under multiplication.

Make a list of the irreducible polynomials of degree 3 over $\mathbf{F}_2$. Let one of these polynomials be $g(x)$, and let α be a root of $g(x) = 0$. Let $f(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$. Show that $f(x) = g(x)$. Show that the cyclic code of length 7 over $\mathbf{F}_2$ generated by $f(x)$ is a quadratic residue code, and find (quoting any appropriate general theorem) its minimum distance. Give a generator matrix for this code. Find a polynomial $h(x)$ such that $f(x)h(x) = x^7 - 1$, and hence find a parity check matrix for the code.