Tutorial-9 Solution

1. Consider the ring Z_{10} = {0, 1, 2, . . ., 9} of integers modulo 10.
   (a) Find the units of Z_{10}.

   Solution- those integers relatively prime to the modulus to the m = 10 are the units in Z_{10}. Hence the units are 1,3,7,9.

   (b) Find −3, −8, and 3−1.
   Solution-Recall that−a in a ring R is the element such that a+(−a) = (−a)+a = 0. Hence−3 = 7 since 3+7 = 7+3 = 0 in Z_{10}. Similarly −8 = 2. Recall that a−1 in a ring R is the element such that a · a−1 = a−1 · a = 1. Hence 3−1 = 7 since 3 · 7 = 7 · 3 = 1 in Z10.
   (c) Let f (x) = $2x^2$ + 4x + 4. Find the roots of f (x) over Z_{10}.
   Solution-Substitute each of the ten elements of Z10 into f (x) to see which elements yield 0. We have
   f (0) = 4, f(2) = 0, f(4) = 2, f(6) = 0, f(8) = 4
   f (1) = 0, f(3) = 4, f(5) = 4, f(7) = 0, f(9) = 2
   Thus the roots are 1, 2, 6, and 7.
2. Prove that in a ring R:
   (i) a · 0 = 0 · a = 0;
   Solution-Since 0 = 0 + 0, we have
   a · 0 = a(0 + 0) = a · 0 + a · 0
   Adding −(a · 0) to both sides yields 0 = a · 0. Similarly 0 · a = 0.
   (ii) a(−b) = (−a)b = −ab;
   Solution-Using b + (−b) = (−b) + b = 0, we have
   ab + a(−b) = a(b + (−b)) = a · 0 = 0
   a(−b) + ab = a((−b) + b) = a · 0 = 0
   Hence a(−b) is the negative of ab; that is, a(−b) = −ab. Similarly, (−a)b = −ab.
   (iii) (−1)a = −a (when R has an identity element 1).

   Solution- We have

   a + (−1)a = 1 · a + (−1)a = (1 + (−1))a = 0 · a = 0

   (−1)a + a = (−1)a + 1 · a = ((−1) + 1)a = 0 · a = 0

   Hence (−1)a is the negative of a; that is, (−1)a = −a.

3. Solve the following-
   (i) Let f (t) = $t^4 - 3t^3 + 3t^2 + 3t - 20$. Find all the roots of f (t) given that t = 1 + 2i is a root.
   Solution- Since 1+2i is a root, then 1−2i is a root and c(t) = $t^2 - 2t + 5$ is a factor of f (t). Dividing f (t) by c(t) we get

   f (t) = $(t^2 - 2t + 5)(t^2 - t - 4)$
   The quadratic formula with $t^2 - t - 4$ gives us the other roots of f (t). That is, the four roots of f (t) follow:

   t = 1 + 2i, t = 1 − 2i, t = (1 + √17)/2, t = (1 − √17)/2
   (ii) Let K = Z_8. Find all roots of f (t) = $t^2 + 6t$.
   Solution-Here Z8 = {0, 1, 2, . . ., 7}. Substitute each element of Z8 into f (t) to obtain:

$f(0) = 0, f(2) = 0, f(4) = 0, f(6) = 0$

Then $f(t)$ has four roots, $t = 0, 2, 4, 6$.

4. Let D be an integral domain. Show that if $ab = ac$ with $a = 0$ then $b = c$.
   Solution-Since $ab = ac$, we have
   $ab - ac = 0$ and so $a(b - c) = 0$
   Since a~ = 0, we must have $b - c = 0$, since D has no zero divisors. Hence $b = c$.
5. Suppose J and K are ideals in a ring R. Prove that $J \cap K$ is an ideal in R.
   Solution- Since J and K are ideals, $0 \in J$ and $0 \in K$. Hence $0 \in J \cap K$. Now let $a, b \in J \cap K$ and let $r \in R$. Then $a, b \in J$ and $a, b \in K$. Since J and K are ideals,
   $a - b, ra, ar \in J$ and $a - b, ra, ar \in K$
   Hence $a - b, ra, ar \in J \cap K$. Therefore $J \cap K$ is an ideal.
6. Let G = Z and H= 5Z = {5n|nϵZ} = {…….,-5,0,5,10,…}.Which of the numbers 17,152,21,-18,-2 lies in the set 2+H?
   Solution- 17 = 5*3 +2
   152 = 5*30+2
   -18 = 5*(-4) +2
   21 and -2 does not belongs to 2+H.
7.

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

That is $G = (I_3 \mid A)$

What are the codewords in the code generated by this generator matrix?

Solution-

We encode each of the eight three-bit messages $x = x_1x_2x_3$ as
$E(x) = xG$. This produces the codewords 000000, 001101, 010110, 011011,
100111, 101010, 110001, and 111100. For example, we get the third of these by computing

$$E(010)=(010)\ G=(010) \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = (010110)$$

It is easy to see that we can find the codewords in a binary code generated by a generator matrix G by taking all possible linear combinations of the rows of G (since arithmetic is modulo 2, this means all sums of subsets of the set of rows of G).

8. Let C be the code {00000000, 11111000, 01010111, 10101111} .How many errors can C detect and how many can it correct?
   Solution - Computing the distance between codewords shows that the minimum distance of C is 5. By Theorem, it follows that C can detect up to $5 - 1 = 4$ errors. For example, when we use C to detect errors, we can detect the four errors made in transmission when we receive 11110000 when the codeword 00000000 was sent. By Theorem , it follows that C can correct up to b(5 − 1)/2c = 2 errors. For example, when we use C to correct errors, we can correct the two errors introduced in transmission when we receive 11100000 when the codeword 11111000 was sent.
9. Suppose that generator matrix for a binary code is

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

What is the parity check matrix H for this code?

Solution-

the bit string $x_1x_2x_3$ is encoded as $x_1x_2x_3x_4x_5x_6$

where $x_4 = x_1 + x_2 + x_3$, $x_5 = x_1 + x_2$, and $x_6 = x_1 + x_3$ (here, arithmetic is carried out modulo 2). Because we are doing arithmetic modulo 2, we see that

$x_1 + x_2 + x_3 + x_4 = 0$

$x_1 + x_2 + x_5 = 0$

$x_1 + x_3 + x_6 = 0.$

Furthermore, it is easy to see that $x_1x_2x_3x_4x_5x_6$ is a codeword if and only if it satisfies this system of equations.

We can express this system of equations as

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

that is,

$H.E(x)^t = 0,$

where $E(x)^t$ is the transpose of $E(x)$ and H, the parity check matrix, is given by

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