Problems and Solutions

(1) $S = \{0, 1, x, x+1\}$ → is a polynomial set

$p(x), q(x) \in S \quad p(x) \oplus q(x) = R_{x^2+x+1}(p(x) + q(x))$

↓

Remainder after division by x^2+x+1

$p(x) \otimes q(x) = R_{x^2+x+1}(p(x) \cdot q(x))$

The coefficients of polynomial are chosen from GF(2)
(Galois field, i.e, binary field)

Show that $(S, \oplus, \otimes)$ is a field

Sln: $(S, \oplus) \xrightarrow{?}$ Group

$\oplus$	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$(S, \oplus)$ is a group

$\otimes$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

$(S, \otimes)$ is a group

Hence $(S, \oplus, \otimes)$ is a field

$x \otimes ((x+1)+1)$
$= x \otimes (x+1) + x$

Notes: $x \otimes (x+1) = R_{x^2+1}(x(x+1))$

means remainder $= R_{x^2+1}(x^2+x) \rightarrow x+1$ //

(2) $F_3 = \{0,1,2\}$ → prime field is given

$\otimes$ → mod 3 mult.

$\oplus$ → mod 3 addition

Consider the polynomial set, coefficients are chosen from F_3

$S = \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}$

$p(x), q(x)$ $\quad p(x) \oplus q(x) = p(x) + q(x)$

$p(x) \otimes q(x) = R_{x^2+x+2}\left(p(x) \cdot q(x)\right)$

Show that $(S, \oplus, \otimes)$ is a field

(3) $F_3 = \{0,1,2\}$ $\otimes$ → mod 3 mult

$\oplus$ → mod 3 addition

$\underline{V} = \{$ set of 3-tuples $\}$

a) Find all the vectors in vector set $\underline{V}$

b) Find a basis vector for $\underline{V}$

c) Find a subspace

d) Dimension of $\underline{V}$?

e) Dimension of your subspace

(4) Ex°

$F_3 = \{0, 1, 2\}$ → 3-prime field

$V = \{$ set of 4-tuples $\}$

A basis for a subspace is given of

$B = \{1000, 2010, 2001\}$

a) Find the code (subspace) generated by B

b) Find the generator matrix of code in part a)

c) Encode the dataword

$d = (1\ 2\ 1)$ $d = (1\ 2\ 1)$

S/n°

$B = \{1000, 2010, 2001\}$

$C = \{0000, 1000, 2010, 2001, 2000, 1020, 1002, 1000+2010$

$1000+2001, 2010+2001, 2\times1000+2010, 2\times1000+2001,$

$2\times2010+1000, 2\times2010+2001, 1000+2\times2001+2010+2\times2001$

$\} \rightarrow 27$ vectors

b) $G = \begin{bmatrix} 1000 \\ 2010 \\ 2001 \end{bmatrix}_{3\times4}$

a) $c = dG \rightarrow c = (1\ 2\ 1)\begin{pmatrix} 1000 \\ 2010 \\ 2001 \end{pmatrix}$

$= 1\times(1000) + 2\times(2010) + 1\times(2001)$

$= 1000 + 1020 + 2001 \rightarrow c = 1021$