HOMEWORK 6.

1 a) $p(x) = x^4 + x^3 + x^2 + x + 1$.

$GF(2^4) = \mathbb{F}_2[x]/p(x)$.

$\xi = x + p(x)$

b) $GF(2^4) = \{a_3\xi^3 + a_2\xi^2 + a_1\xi + a_0,$

where $a_3, a_2, a_1, a_0 \in \mathbb{F}_2\}$

a_3	a_2	a_1	a_0	
0	0	0	0	0
0	0	0	1	1
0	0	1	0	c
0	0	1	1	$c+1$
0	1	0	0	c^2
0	1	0	1	c^2+1
0	1	1	0	c^2+c
0	1	1	1	c^2+c+1
1	0	0	0	c^3
1	0	0	1	c^3+1
1	0	1	0	c^3+c
1	0	1	1	c^3+c+1
1	1	0	0	c^3+c^2
1	1	0	1	c^3+c^2+1
1	1	1	0	c^3+c^2+c
1	1	1	1	c^3+c^2+c+1

(c) Since $\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$

$$\xi^4 = \xi^3 + \xi^2 + \xi + 1$$

$$\xi^0 = 1$$

$$\xi^1 = \xi$$

$$\xi^2 = \xi^2$$

$$\xi^3 = \xi^3$$

$$\xi^4 = \xi^3 + \xi^2 + \xi + 1$$

$$\xi^5 = \xi^4 + \xi^3 + \xi^2 + \xi$$
$$= \xi^3 + \xi^2 + \xi + 1 + \xi^3 + \xi^2 + \xi$$
$$= 1$$

It is not a complete set of all the non zero elements of GF(2^4) because $p(x)$ is a nonprimitive polynomal.

2 (a) $n = 15$

(b) $k = \dim V = \operatorname{codeg}(g) = 15 - 8 = 7$

(c)

$$G = \begin{bmatrix} x^{\operatorname{codeg}(g)-1} g(x) \\ \vdots \\ x^2 g(x) \\ x\, g(x) \\ 1\, g(x) \end{bmatrix}$$

$$= \begin{bmatrix} x^6 g(x) \\ x^5 g(x) \\ x^4 g(x) \\ x^3 g(x) \\ x^2 g(x) \\ x\, g(x) \\ 1\, g(x) \end{bmatrix} = \begin{bmatrix} x^{14} + x^{10} + x^8 + x^7 + x^6 \\ x^{13} + x^9 + x^7 + x^6 + x^5 \\ x^{12} + x^8 + x^6 + x^5 + x^4 \\ x^{11} + x^7 + x^5 + x^4 + x^3 \\ x^{10} + x^6 + x^4 + x^3 + x^2 \\ x^9 + x^5 + x^3 + x^2 + x \\ x^8 + x^4 + x^2 + x + 1 \end{bmatrix}$$

(d) $$h(x) = \frac{x^{15}+1}{g(x)} = x^7 + x^3 + x + 1$$

(e)

$$\begin{aligned} h^*(x) &= x^7 h(x^{-1}) \\ &= x^7(x^{-7} + x^{-3} + x^{-1} + 1) \\ &= 1 + x^4 + x^6 + x^7 \end{aligned}$$

$\operatorname{codeg}(h^*(x)) = \deg(g) = 8$

$$H = \begin{bmatrix} x^{\operatorname{codeg}(h)-1} h^*(x) \\ \vdots \\ x^2 h^*(x) \\ x\, h^*(x) \\ 1\, h^*(x) \end{bmatrix}$$

$$H = \begin{bmatrix} x^7 h^*(x) \\ x^6 h^*(x) \\ x^5 h^*(x) \\ x^4 h^*(x) \\ x^3 h^*(x) \\ x^2 h^*(x) \\ x\, h^*(x) \\ h^*(x) \end{bmatrix}$$

$$H = \begin{bmatrix} x^{14} + x^{13} + x^{11} + x^7 \\ x^{13} + x^{12} + x^{10} + x^6 \\ x^{12} + x^{11} + x^9 + x^5 \\ x^{11} + x^{10} + x^8 + x^4 \\ x^{10} + x^9 + x^7 + x^3 \\ x^9 + x^8 + x^6 + x^2 \\ x^8 + x^7 + x^5 + x \\ x^7 + x^6 + x^4 + 1 \end{bmatrix}$$

3(a) $x^9+1 = \underbrace{(x+1)}_{p1}\underbrace{(x^2+x+1)}_{p2}\underbrace{(x^6+x^3+1)}_{p3}$

Lattice.

$$\begin{tikzcd}
 & (1) & \\
(p1) \arrow[ur] & (p2) \arrow[u] & (p3) \arrow[ul] \\
(p1p2) \arrow[u] \arrow[ur] & (p2p3) \arrow[u] \arrow[ur] & (p1p3) \arrow[u] \arrow[ull] \\
 & (p1p2p3) \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

(b) & (c)

Ideal.	Deg.	Codeg.	# elements
1	0	9	2^9
p1	1	8	2^8
p2	2	7	2^7
p3	6	3	2^3
p1p2	3	6	2^6
p2 p3	8	1	2^1
p1 p3	7	2	2^2
p1p2p3	9	0	2^0

(c) $g(x) = x^6 + x^3 + 1$

$$G = \begin{bmatrix} x^{\operatorname{codeg} g - 1} g(x) \\ \vdots \\ x\, g(x) \\ 1\, g(x) \end{bmatrix}$$

$$= \begin{bmatrix} x^2\, g(x) \\ x\, g(x) \\ 1\, g(x) \end{bmatrix} = \left\{ (a_2x^2 + a_1x + a_0)\, g(x) \,\middle|\, a_2, a_1, a_0 \in \mathbb{F} \right\}$$

$$u(x) = (x+1)(x^6 + x^3 + 1)$$

$$G = \begin{bmatrix} x\, u(x) \\ u(x) \end{bmatrix} = \left\{ (a_1x^2 + a_0)\, u(x) \,\middle|\, a_1, a_0 \in \mathbb{F}_2 \right\}.$$