Sample Assignment 1
Algebra for ECC

Question 1

$GF(2^4)$ is an extension field of GF(2). There are two primitive polynomials that can be used to define the primitive element of GF(16). They are $p_1(X)=X^4+X+1$ and $p_2(X)=X^4+X^3+1$. Solve the following questions.

(a) For GF(16) defined by $p_1(X)$, what equation defines the primitive element?
(b) Repeat (a) for $p_2(X)$.
(c) For GF(16) defined by $p_1(X)$, find expressions for α^6, α^7, α^8 and α^9.
(d) Using the expressions for α^6, α^7, α^8 and α^9 in (c), show that $\alpha^6\alpha^9=1$ and $\alpha^7\alpha^8$ also equals 1.
(e) In GF(16) what is the multiplicative inverse of α^i for any i=1,2,3,…,14?

Question 2

X, Y, Z and W are variables in GF(2). From the following set of equations, find their values.

$X+Y+W=1$
$X+Z+W=0$
$X+Y+Z+W=1$
$Y+Z+W=0$

Question 3

Show that X^5+X^3+1 is irreducible in GF(2).

Question 4

Let α be the primitive element of GF(4). Solve the following set of equations
$X+\alpha Y=\alpha^2$
$\alpha X+Y=1$

Question 5

The following polynomials are defined over GF(8): $f(X)=1+\alpha^3X^2+X^3$ and $g(X)=\alpha^4X+\alpha^6X^2+\alpha^3X^3+\alpha^4X^4$. Find

(a) $\alpha f(X)+g(X)$
(b) $f(X)g(X)$
(c) $f(X)+1$

In GF(8) $\alpha^3=\alpha+1$.

Solution Assignment 1

Q1

(a) $x^4 + x + 1 \rightarrow$

$P_1(\alpha) = 0 \quad \therefore \quad \alpha^4 + \alpha + 1 = 0$

$\alpha^4 = \alpha + 1$

(b) $P_2(\alpha) = 0$

$\alpha^4 + \alpha^3 + 1 = 0$

$\alpha^4 = \alpha^3 + 1$

(c) $\alpha^4 = \alpha + 1$

$\alpha^5 = \alpha^2 + \alpha$

$\alpha^6 = \alpha^3 + \alpha^2$

$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$

$\alpha^8 = \alpha^4 + \alpha^2 + \alpha = \alpha^2 + 1$

$\alpha^9 = \alpha^3 + \alpha$

(d) $\alpha^6 \alpha^9 = (\alpha^3 + \alpha^2)(\alpha^3 + \alpha \quad)$

$= \alpha^6 + \alpha^4 + \alpha^5 + \alpha^3$

$= \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + \alpha^3$

$= \alpha^3 + \alpha^3 + \alpha^2 + \alpha^2 + \alpha + \alpha + 1$

$= 1$

$\alpha^7 \alpha^8 = (\alpha^3 + \alpha + 1)(\alpha^2 + 1)$

$= \alpha^5 + \alpha^3 + \alpha^3 + \alpha + \alpha^2 + 1$

$= \alpha^5 + \alpha^2 + \alpha + 1$

$= \alpha^2 + \alpha + \alpha^2 + \alpha + 1$

$= 1$

(e) $\alpha^{15} = 1$

Therefore $\alpha^i \cdot \alpha^x = \alpha^{15}$

$\alpha^{i+x} = \alpha^{15}$

$i + x = 15$

$x = 15 - i$

α^{15-i} is the inverse of α^i

Q2

$X + Y + W = 1$ ①

$X + Z + W = 0$ ②

$X + Y + Z + W = 1$ ③

$Y + Z + W = 0$ ④

③ + ④ is $X + Y + Z + W + Y + Z + W = 1 + 0$

$\longrightarrow X = 1$

① + ② + ④ $X + Y + W + X + Z + W + Y + Z + W = 1 + 0 + 0$

$\Rightarrow \underbrace{2X}_{0} + \underbrace{2Y}_{0} + \underbrace{2Z}_{0} + \underbrace{3W}_{W} = 1$

therefore $W = 1$

$X + Y + W = 1$

$1 + Y + 1 = 1$

$Y = 1$

$Y + Z + W = 0$

$1 + Z + 1 = 0$

$Z = 0$

Q 3

show that $X^5 + X^3 + 1$ is irreducible

let $p(x) = X^5 + X^3 + 1$

$p(1) = 1 + 1 + 1 = 1 \neq 0$

$p(0) = 1 = 0$

therefore not divisible by $X+1$ or X

$(X^2+1) = (X+1)(X+1)$ therefore if $p(x)$ is divisible by X^2+1 it is divisible by $X+1$

$$
\begin{array}{r|l}
 & X^3 + X^2 + X \\
\hline
X^2+X+1 & X^5 + X^3 + 1 \\
 & X^5 + X^4 + X^3 \\
\hline
 & X^4 + 1 \\
 & X^4 + X^3 + X^2 \\
\hline
 & X^3 + X^2 + 1 \\
 & X^3 + X^2 + X \\
\hline
 & X + 1
\end{array}
$$

$X+1$ ⇒ remainder

not divisible by X^2+X+1

cannot be divisible by X^2+X because that is divisible by X.

if divisible by $X^3 + \ldots + 1$ then quotient is a polynomial with degree 2 and we showed that no polynomial of degree 2 divides $X^5 + X^3 + 1$. Therefore it is irreducible.

Q4

$$X + \alpha Y = \alpha^2 \quad (1)$$
$$\alpha X + Y = 1 \quad (2)$$

multiply (1) by α

$$\alpha X + \alpha^2 Y = 1 \quad (1)$$
$$\alpha X + Y = 1 \quad (2)$$

add (1) and (2)

$$\underbrace{(\alpha + \alpha)}_{0} X + \underbrace{(\alpha^2 + 1)}_{\alpha} Y = 0$$

$$\alpha Y = 0$$
$$Y = 0$$

take (1) $X + \alpha Y = \alpha^2$

$$X + \alpha(0) = \alpha^2$$
$$X = \alpha^2$$

q5 (note using x^3+x+1 as primitive)

a) $\alpha f(x) = \alpha(1 + \alpha^3 x^2 + x^3)$
$= \alpha + \alpha^4 x^2 + \alpha x^3$

$\alpha f(x) + g(x)$

$= \alpha + \alpha^4 x^2 + \alpha x^3 + \alpha^4 x + \alpha^6 x^2 + \alpha^3 x^3 + \alpha^4 x^4$

$= \alpha + \alpha^4 x + (\alpha^4 + \alpha^6) x^2 + (\alpha + \alpha^3) x^3 + \alpha^4 x^4$

$= \alpha + \alpha^4 x + \alpha^3 x^2 + x^3 + \alpha^4 x^4$

b) $f(x) g(x)$

$= (1 + \alpha^3 x^2 + x^3)(\alpha + \alpha^4 x^2 + \alpha x^3)$
$= \alpha + \alpha^4 x^2 + \alpha x^3 + \alpha^4 x^2 + \alpha^7 x^4 + \alpha^4 x^5$
$+ \alpha x^3 + \alpha^4 x^5 + \alpha x^6$ (91)
$= \alpha + (\alpha^4 + \alpha^4) x^2 + (\alpha + \alpha) x^3 + x^4$
$+ (\alpha^4 + \alpha^4) x^5 + \alpha x^6$
$= \alpha + x^4 + \alpha x^6$

(c) $f(x)+1$

$= 1+1+a^3x^2+x^3$

$= a^3x^2+x^3$