S-72.341 CODING METHODS

Tutorial 2, Solutions

1. The orders of the elements in GF(125) must divide 124. Since $124 = 2 \times 2 \times 31$, the possible orders are 1, 2, 4, 31, 62, 124. The number of elements that are relative primes with given orders can be calculated by Euler totient function defined as

   $$\phi(t) = |\{1 \le i < t | \mathrm{GCD}(i,t) = 1\}| = t \prod_{p|t} \left(1 - \frac{1}{p}\right).$$

   The amount of relative prime elements are given in the following table:

Order	**# of elements**
1	$\phi(1) = 1$
2	$\phi(2) = 1$
4	$\phi(4) = 2$
31	$\phi(31) = 30$
62	$\phi(62) = 30$
124	$\phi(124) = 60$

   The number of elements of order t is $\phi(t)$.

2.

   a) Let α be a primitive element of GF(q^m). The nonzero elements of GF(q) are the powers of $\alpha^{(q^m-1)/(q-1)}$ or in other words satisfy relationship $j \cdot q \equiv j \,\mathrm{modulo}\,(q^m - 1)$. In particular, the subfields GF(2), GF(4) and GF(32) are generated by $\alpha^{1023} = 1$, $\alpha^{1023/3} = \alpha^{341}$ and $\alpha^{1023/31} = \alpha^{33}$, respectively. The elements in the subfields are: GF(2)=$\{0,1\}$, GF(4)= $\left\{0,1,\alpha^{341},\alpha^{682}\right\}$, GF(32)= $\left\{0,1,\alpha^{33},\alpha^{66},\alpha^{99},\alpha^{132},\ldots,\alpha^{990}\right\}$.

   b) The conjugates of α over GF(q) are defined as $\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$. Over the subfields GF(2), GF(4), and GF(32), the primitive element $\alpha \in$ GF(1024) has 10, 5, 2 conjugates, respectively. The conjugates of α over GF(2) are $\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}, \alpha^{256}, \alpha^{512}$. Conjugates over GF(4) are $\alpha, \alpha^4, \alpha^{16}, \alpha^{64}, \alpha^{256}$. Conjugates over GF(32) are α, α^{32}.

3. By polynomial division we get

a) $x^8 + 1 = (x^4 + 1)(x^4 + 1)$

b) $x^8 + 1 = (x^4 + x)(x^4 + x) + x^2 + 1$

c) $x^{10} + x^9 + x^5 + x^4 = (x^9 + x^4)(x + 1)$

d) $x^5 + x^3 + 1 = (x^3 + x^2 + x)(x^2 + x + 1) + x + 1$.

4. We are given the order of the roots of unity and are asked to find the minimum extension field where we can find root with this order. Let the degree of the minimal polynomial $f(x) \in \mathrm{GF}(q)[x]$ of an element β be m. We are searching for the smallest field $\mathrm{GF}(q^m)$ that contains β. By Theorem 2-10 $\mathrm{ord}(\beta) | (q^m - 1)$. By trial and error we find the smallest m for the given orders. In our case $q = 2$. The results are given in the following table.

$\mathrm{ord}(\beta)$	9	13	21	1023
m (=degree)	6	12	6	10
$2^m - 1$	63	4095	63	1023

5. Since α is a root of $f(x)$, $\alpha^2 + \alpha + 1 = 0$. Below are exponential and polynomial representations of GF(4).

exponential	**polynomial**
$\alpha^0 = 1$	1
α	α
α^2	$\alpha + 1$
0	0

Addition table (using the exponential representation):

$\oplus$	0	1	α	α^2
0	0	1	α	α^2
1		0	α^2	α
α			0	1
α^2				0

Multiplication table:

$\otimes$	0	1	α	α^2
0	0	0	0	0
1		1	α	α^2
α			α^2	1
α^2				α

Operation tables are symmetric, since operations in a field are by definition commutative.

6. We construct GF(8) by using the primitive polynomial $p(x) = x^3 + x + 1$. The other 3^{rd} degree primitive polynomial, $p(x) = x^3 + x^2 + 1$, could also be used. Exponential and polynomial representations for GF(8) have been given in Example 2-23 of the book.

   Addition table:

$\oplus$	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1		0	α^3	α^6	α	α^5	α^4	α^2
α			0	α^4	1	α^2	α^6	α^5
α^2				0	α^5	α	α^3	1
α^3					0	α^6	α^2	α^4
α^4						0	1	α^3
α^5							0	α
α^6								0

   Multiplication table:

$\otimes$	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
1		1	α	α^2	α^3	α^4	α^5	α^6
α			α^2	α^3	α^4	α^5	α^6	1
α^2				α^4	α^5	α^6	1	α
α^3					α^6	1	α	α^2
α^4						α	α^2	α^3
α^5							α^3	α^4
α^6								α^5

7.

a) Denote $f(x) = x^3 + 1$. Since $f(1) = 0$, the polynomial has factor $x - 1$. By polynomial division we get $f(x) = (x+1)\left(x^2 + x + 1\right)$. The second degree factor cannot be factored in GF(2). It is actually a primitive polynomial.

b) The product of the two polynomials $g(x) = x^4 + 2x^3 + x^2 + 2$. To find representation in $\mathrm{GF}(3)[x]/\left(x^3 - 1\right)$ we do the polynomial division and get $g(x) \equiv x^2 + x + 1 \bmod \left(x^3 - 1\right)$.

8. In order to factor the given polynomials we need to divide the field elements to conjugacy classes. The first two parts are solved in detail; for the remaining one only result is given.

a) All nonzero elements (except 1) in GF(8) are primitive. The conjugacy classes of GF(8) wrt GF(2) may have 1 or 3 elements. The conjugacy classes are $\left\{\alpha, \alpha^2, \alpha^4\right\}$, $\left\{\alpha^3, \alpha^6, \alpha^{12} = \alpha^5\right\}$, $\{1\}$. Operation tables for GF(8) using primitive polynomial $f(x) = x^3 + x + 1$ were computed in problem 7.

Minimal polynomial #1:

$$\begin{aligned} g_1(x) &= (x - \alpha)\left(x - \alpha^2\right)\left(x - \alpha^4\right) \\ &= \left[x^2 + \left(\alpha^2 + \alpha\right)x + \alpha^3\right]\left(x + \alpha^4\right) \\ &= x^3 + \alpha^4 x^2 + \alpha^4 x^2 + \alpha x + \alpha^3 x + 1 \\ &= x^3 + x + 1 \end{aligned}$$

Minimal polynomial #2:

$$\begin{aligned} g_2(x) &= \left(x-\alpha^3\right)\left(x-\alpha^5\right)\left(x-\alpha^6\right) \\ &= \left[x^2+\left(\alpha^3+\alpha^5\right)x+\alpha^8\right]\left(x+\alpha^6\right) \\ &= x^3+\alpha^6x^2+\alpha^2x^2+\alpha^8x+\alpha^8x+1 \\ &= x^3+x^2+1 \end{aligned}$$

Minimal polynomial #3:

$$g_3(x) = x+1$$

The factorization is $x^7+1=(x+1)\left(x^3+x+1\right)\left(x^3+x^2+1\right)$.

b) Nonzero elements in GF(16) may have order 1, 3, 5, or 15. (The numbers of elements with these orders are $\phi(1)=1$, $\phi(3)=2$, $\phi(5)=4$, and $\phi(15)=8$, respectively.) Conjugacy classes wrt GF(2) may have 1, 2, or 4 elements. Let α be a primitive element in GF(16), i.e. $\mathrm{ord}(\alpha)=15$. First we find the conjugacy classes of GF(16) wrt GF(2) using α. They are $\left\{\alpha,\alpha^2,\alpha^4,\alpha^8\right\}$, $\left\{\alpha^3,\alpha^6,\alpha^{12},\alpha^{24}=\alpha^9\right\}$, $\left\{\alpha^5,\alpha^{10}\right\}$, $\left\{\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}\right\}$, $\left\{\alpha^0=1\right\}$. These are the roots of the minimal polynomials. To puncture the dreariness of the ensuing algebra, let's construct the exponential and polynomial representations for GF(16). We use the primitive polynomial $f(x)=x^4+x+1$.

exponential	**polynomial**	**exponential**	**polynomial**
0	0	α^7	$\alpha^3+\alpha+1$
$\alpha^0=1$	1	α^8	α^2+1
α	α	α^9	$\alpha^3+\alpha$
α^2	α^2	α^{10}	$\alpha^2+\alpha+1$
α^3	α^3	α^{11}	$\alpha^3+\alpha^2+\alpha$
α^4	$\alpha+1$	α^{12}	$\alpha^3+\alpha^2+\alpha+1$
α^5	$\alpha^2+\alpha$	α^{13}	$\alpha^3+\alpha^2+1$
α^6	$\alpha^3+\alpha^2$	α^{14}	α^3+1

Minimal polynomial #1:

$$\begin{aligned}
g_1(x) &= (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right)\left(x-\alpha^8\right) \\
&= \left[x^2+\left(\alpha^2+\alpha\right)x+\alpha^3\right]\left[x^2+\left(\alpha^8+\alpha^4\right)x+\alpha^{12}\right] \\
&= \left[x^2+\alpha^5x+\alpha^3\right]\left[x^2+\alpha^5x+\alpha^{12}\right] \\
&= x^4+\alpha^5x^3+\alpha^{12}x^2+\alpha^5x^3+\alpha^{10}x^2+\alpha^2x+\alpha^3x^2+\alpha^8x+1 \\
&= x^4+\underbrace{\left(\alpha^{12}+\alpha^{10}+\alpha^3\right)}_{0}x^2+\underbrace{\left(\alpha^8+\alpha^2\right)}_{1}x+1 \\
&= x^4+x+1
\end{aligned}$$

This is actually the primitive polynomial used to construct the field.

Minimal polynomial #2:

$$\begin{aligned}
g_2(x) &= \left(x-\alpha^3\right)\left(x-\alpha^6\right)\left(x-\alpha^9\right)\left(x-\alpha^{12}\right) \\
&= \left[x^2+\left(\alpha^3+\alpha^6\right)x+\alpha^9\right]\left[x^2+\left(\alpha^9+\alpha^{12}\right)x+\alpha^6\right] \\
&= \left[x^2+\alpha^2x+\alpha^9\right]\left[x^2+\alpha^8x+\alpha^6\right] \\
&= x^4+\alpha^8x^3+\alpha^6x^2+\alpha^2x^3+\alpha^{10}x^2+\alpha^8x+\alpha^9x^2+\alpha^2x+1 \\
&= x^4+\underbrace{\left(\alpha^8+\alpha^2\right)}_{1}x^3+\underbrace{\left[\alpha^6+\alpha^{10}+\alpha^9\right]}_{1}x^2+\underbrace{\left[\alpha^8+\alpha^2\right]}_{1}x+1 \\
&= x^4+x^3+x^2+x+1
\end{aligned}$$

Minimal polynomial #3:

$$
\begin{aligned}
g_3(x) &= \big(x-\alpha^7\big)\big(x-\alpha^{14}\big)\big(x-\alpha^{13}\big)\big(x-\alpha^{11}\big) \\
&= \big[x^2+\big(\alpha^7+\alpha^{14}\big)x+\alpha^6\big]\big[x^2+\big(\alpha^{13}+\alpha^{11}\big)x+\alpha^9\big] \\
&= \big[x^2+\alpha x+\alpha^6\big]\big[x^2+\alpha^4 x+\alpha^9\big] \\
&= x^4+\alpha^4x^3+\alpha^9x^2+\alpha x^3+\alpha^5x^2+\alpha^{10}x+\alpha^6x^2+\alpha^{10}x+1 \\
&= x^4+\underbrace{\big(\alpha^4+\alpha\big)}_{1}x^3+\underbrace{\big[\alpha^9+\alpha^5+\alpha^6\big]}_{0}x^2+1 \\
&= x^4+x^3+1
\end{aligned}
$$

Minimal polynomial #4:

$$
\begin{aligned}
g_4(x) &= \big(x-\alpha^5\big)\big(x-\alpha^{10}\big) \\
&= x^2+\big(\alpha^5+\alpha^{10}\big)x+1 \\
&= x^2+x+1
\end{aligned}
$$

Minimal polynomial #5:

$$
g_5(x) = x+1
$$

The factorization is

$$
\begin{aligned}
x^{15}+1 &= (x+1)\big(x^4+x+1\big) \\
&\quad\cdot\big(x^4+x^3+1\big)\big(x^4+x^3+x^2+x+1\big)\big(x^2+x+1\big).
\end{aligned}
$$

c) The smallest field containing an element of order 21 is GF(64). The factorization is (work through it…):

$$
\begin{aligned}
x^{21}+1 = \;& (x+1)(x^6+x^5+x^4+x^2+1)(x^6+x^4+x^2+x+1) \\
&\cdot(x^3+x^2+1)(x^3+x+1)(x^2+x+1).
\end{aligned}
$$