

1. The codewords in the first order Reed-Muller code $R(1, 3)$ are of the form

$$x_1x_2 \dots x_7x_8 = [a_3 \ a_2 \ a_1 \ a_0] G(1, 3)$$

- (a) Find the parity check sums for a_1 , a_2 and a_3 .
 (b) Decode 1000011.
 (c) Decode 10101010.

Solution : (a) We have that

$$x_1x_2 \dots x_7x_8 = [a_3 \ a_2 \ a_1 \ a_0] \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

So

$$\begin{cases} x_1 = a_0 \\ x_2 = a_1 + a_0 \\ x_3 = a_2 + a_0 \\ x_4 = a_2 + a_1 + a_0 \\ x_5 = a_3 + a_0 \\ x_6 = a_3 + a_1 + a_0 \\ x_7 = a_3 + a_2 + a_0 \\ x_8 = a_3 + a_2 + a_1 + a_0 \end{cases}$$

Hence we get the following parity check sums :

$$\begin{aligned} a_1 &= x_1 + x_2 = x_3 + x_4 = x_5 + x_6 = x_7 + x_8 \\ a_2 &= x_1 + x_3 = x_2 + x_4 = x_5 + x_7 = x_6 + x_8 \\ a_3 &= x_1 + x_5 = x_2 + x_6 = x_3 + x_7 = x_4 + x_8 \end{aligned}$$

(b) We calculate the parity check sums for a_1 , a_2 and a_3 :

$$\begin{aligned} a_1 &: \{1, 0, 0, 0\} \quad \text{so } a_1 = 0 \\ a_2 &: \{1, 0, 1, 1\} \quad \text{so } a_2 = 1 \\ a_3 &: \{1, 0, 1, 1\} \quad \text{so } a_3 = 1 \end{aligned}$$

We easily get that

$$[a_3 \ a_2 \ a_1 \ 0] G(1, 3) = [1 \ 1 \ 0 \ 0] \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = 00111100$$

Since $1000011 - 00111100 = 10111111$, we get that $a_0 = 1$. So we decode 1000011 as

$$00111100 + 11111111 = 1100011$$

(c) We proceed as in (b). The parity check sums for a_1 , a_2 and a_3 are :

$$\begin{aligned} a_1 &: \{1, 1, 1, 1\} \quad \text{so } a_1 = 1 \\ a_2 &: \{0, 0, 0, 0\} \quad \text{so } a_2 = 0 \\ a_3 &: \{0, 0, 0, 0\} \quad \text{so } a_3 = 0 \end{aligned}$$

We easily get that

$$[a_3 \ a_2 \ a_1 \ 0] G(1,3) = [0 \ 0 \ 1 \ 0] \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = 01010101$$

Since $10101010 - 01010101 = 11111111$, we get that $a_0 = 1$. So we decode 10101010 as

$$01010101 + 11111111 = 10101010$$

Note that this implies that the received word is a codeword. □

2. Consider the binary matrix

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

Show that G is a generator matrix for the second order Reed-Muller code $R(2,3)$.

Proof : It follows from the definition of the Reed-Muller codes that

$$R(2,3) = R(2,2) \otimes R(1,2)$$

We know that $G(1,2) = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$ is a generator matrix for $R(1,2)$. Note that $R(2,2)$ is the set of all binary words of length four. We claim that

$$G(2,2) := \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is a generator matrix for $R(2,2)$. The only thing we have to show is that the rank of $G(2,2)$ is four, but this is obvious since $G(2,2)$ is an upper uni-triangular matrix.

Hence it follows from Theorem 4.2 that $G' := \begin{bmatrix} 0_{3 \times 4} & G(1,2) \\ G(2,2) & G(2,2) \end{bmatrix}$ is a generator matrix for $R(2,3)$. So

$$G' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Thus the rows of G' form a basis for $R(2,3)$. Since the rows of G are the same as the rows of G' , we get that the rows of G form a basis for $R(2,3)$. Hence G is a generator matrix for $R(2,3)$. □

3. Explain the probabilities on page 33 in the notes. First write your answers in terms of a general symbol-error-probability p . Then evaluate your answers (you will need a computer to find 99.99%).

Solution : Let p be the probability that one digit is received incorrectly.

- **No error correction**

A pixel (or grayscale) is now a message with six digits : $a_1a_2a_3a_4a_5a_6$. If an error occurs during transmission, we will not be able to recover. The probability that one digit is received correctly is $1-p$. So the probability that we receive a pixel correctly is $(1-p)^6$. Hence the probability that a pixel is received incorrectly is

$$1 - (1-p)^6 \quad ; \quad \text{for } p = 5\% : 26.49\%$$

- **Repeating every digit five times**

A pixel had six digits $a_1a_2a_3a_4a_5a_6$. We send each digit of this pixel five times. So we are using the repetition code $\{00000, 11111\}$ for each digit of the pixel. We will decode a digit of the pixel correctly if at most two errors occur during transmission. The probability of at most two errors occurring during the transmission of say $a_1a_1a_1a_1a_1$ is

$$(1-p)^5 + \binom{5}{1}p(1-p)^4 + \binom{5}{2}p^2(1-p)^3 \quad \text{or} \quad \sum_{i=0}^2 \binom{5}{i}p^i(1-p)^i$$

So the probability we decode correctly all six digits of the pixel is

$$\left(\sum_{i=0}^2 \binom{5}{i}p^i(1-p)^i \right)^6$$

Hence the probability that a pixel is decoded incorrectly now drops to

$$1 - \left(\sum_{i=0}^2 \binom{5}{i}p^i(1-p)^i \right)^6 \quad ; \quad \text{for } p = 5\% : 0.6929\%$$

- **Using $R(1, 5)$**

A pixel is now a binary word of length 32. Since $R(1, 5)$ is seven-error correcting, we will decode a pixel correctly if at most seven errors occur during transmission. The probability that at most seven errors occur during transmission is

$$\sum_{i=0}^7 \binom{32}{i}p^i(1-p)^i$$

So the probability that a pixel is decoded incorrectly drops even further down to

$$P := 1 - \sum_{i=0}^7 \binom{32}{i}p^i(1-p)^i \quad ; \quad \text{for } p = 5\% : 0.0139\%$$

- **Whole picture using $R(1, 5)$**

Since a picture is 832×700 , we get that a picture contains $M := 832 \cdot 700 = 582,400$ pixels. We just showed that the probability that a pixel is decoded incorrectly is $P = 1 - \sum_{i=0}^7 \binom{32}{i}p^i(1-p)^i$. Hence the probability that (after decoding) the whole picture contains at most 116 incorrect pixels is

$$\sum_{i=0}^{116} \binom{M}{i}P^i(1-P)^{M-i} \quad ; \quad \text{for } p = 5\% : 99.9899\%$$

4. It is given that $f(x) = x^4 + x + 1$ is irreducible and primitive over $GF(2)$. Define α by $f(\alpha) = 0$.

- (a) Set up a table for $GF(16)$ containing the binary, exponential and polynomial representation of every element in $GF(16)$.
- (b) Solve for x and y : $\begin{cases} x + \alpha^7 y = \alpha^{10} \\ \alpha^2 x + y = \alpha^5 \end{cases}$. Write all elements of $GF(16)$ in exponential form.
- (c) Find the quotient and remainder of $x^5 + \alpha^2 x^4$ divided by $x^2 + \alpha x + \alpha^2$. Write all elements of $GF(16)$ in exponential form.

Solution : (a) We know that $\alpha^4 + \alpha + 1 = 0$. So

$$\begin{aligned} \alpha^4 &= \alpha + 1 = 0011 \\ \alpha^5 &= \alpha\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 0110 \\ \alpha^6 &= \alpha\alpha^5 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = 1100 \\ \alpha^7 &= \alpha\alpha^6 = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha + 1 + \alpha^3 = \alpha^3 + \alpha + 1 = 1011 \\ \alpha^8 &= \alpha\alpha^7 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1 = 0101 \\ \alpha^9 &= \alpha\alpha^8 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = 1010 \\ \alpha^{10} &= \alpha\alpha^9 = \alpha(\alpha^3 + \alpha) = \alpha^4 + \alpha^2 = \alpha + 1 + \alpha^2 = \alpha^2 + \alpha + 1 = 0111 \\ \alpha^{11} &= \alpha\alpha^{10} = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = 1110 \\ \alpha^{12} &= \alpha\alpha^{11} = \alpha(\alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1 = 1111 \\ \alpha^{13} &= \alpha\alpha^{12} = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1 = 1101 \\ \alpha^{14} &= \alpha\alpha^{13} = \alpha(\alpha^3 + \alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha = \alpha + 1 + \alpha^3 + \alpha = \alpha^3 + 1 = 1001 \\ \alpha^{15} &= \alpha\alpha^{14} = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha + 1 + \alpha = 1 \end{aligned}$$

Hence we get the following table :

binary	$GF(16)$	Polynomial in α
0000	0	0
0001	1	1
0010	α	α
0100	α^2	α^2
1000	α^3	α^3
0011	α^4	$\alpha + 1$
0110	α^5	$\alpha^2 + \alpha$
1100	α^6	$\alpha^3 + \alpha^2$
1011	α^7	$\alpha^3 + \alpha + 1$
0101	α^8	$\alpha^2 + 1$
1010	α^9	$\alpha^3 + \alpha$
0111	α^{10}	$\alpha^2 + \alpha + 1$
1110	α^{11}	$\alpha^3 + \alpha^2 + \alpha$
1111	α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
1101	α^{13}	$\alpha^3 + \alpha^2 + 1$
1001	α^{14}	$\alpha^3 + 1$

(b) There are several methods of solving this system of linear equations : Cramer's rule, substitution method, elimination method. We illustrate the elimination method.

$$\begin{cases} x + \alpha^7 y = \alpha^{10} & \left| \begin{array}{c} \alpha^2 \\ 1 \end{array} \right| \begin{array}{c} 1 \\ \alpha^7 \end{array} \end{cases}$$

This means that we get the first new equation by multiplying the first equation by α^2 and adding the second equation; we get the second new equation by multiplying the second equation by α^7 and adding the first equation. Hence we find

$$\begin{cases} (\alpha^9 + 1)y = \alpha^{12} + \alpha^5 \\ (1 + \alpha^9)x = \alpha^{10} + \alpha^{12} \end{cases}$$

Using the table, we find

$$\begin{aligned} \alpha^9 + 1 &= 1010 + 0001 = 1011 = \alpha^7 \\ \alpha^{12} + \alpha^5 &= 1111 + 0110 = 1001 = \alpha^{14} \\ \alpha^{10} + \alpha^{12} &= 0111 + 1111 = 1000 = \alpha^3 \end{aligned}$$

So

$$\begin{cases} \alpha^7 y = \alpha^{14} \\ \alpha^7 x = \alpha^3 \end{cases}$$

Hence

$$y = \frac{\alpha^{14}}{\alpha^7} = \alpha^7$$

and

$$x = \frac{\alpha^3}{\alpha^7} = \alpha^{-4} = \alpha^{11}$$

$$\boxed{(x, y) = (\alpha^{11}, \alpha^7)}$$

(c) Using the table and standard long division, we find

$$\begin{array}{r} x^2 + \alpha x + \alpha^2 \quad \left(\begin{array}{r} x^5 + \alpha^2 x^4 \\ \underline{x^5 + \alpha x^4 + \alpha^2 x^3} \\ \alpha^5 x^4 + \alpha^2 x^3 \\ \underline{\alpha^5 x^4 + \alpha^6 x^3 + \alpha^7 x^2} \\ \alpha^3 x^3 + \alpha^7 x^2 \\ \underline{\alpha^3 x^3 + \alpha^4 x^2 + \alpha^5 x} \\ \alpha^3 x^2 + \alpha^5 x \\ \underline{\alpha^3 x^2 + \alpha^4 x + \alpha^5} \\ \alpha^8 x + \alpha^5 \end{array} \right. \end{array}$$

since

$$\begin{aligned} \alpha^2 + \alpha &= 0100 + 0010 = 0110 = \alpha^5 \\ \alpha^2 + \alpha^6 &= 0100 + 1100 = 1000 = \alpha^3 \\ \alpha^7 + \alpha^4 &= 1011 + 0011 = 1000 = \alpha^3 \\ \alpha^5 + \alpha^4 &= 0110 + 0011 = 0101 = \alpha^8 \end{aligned}$$

So

$$\boxed{x^5 + \alpha^2 x^4 = (x^2 + \alpha x + \alpha^2) \underbrace{(x^3 + \alpha^5 x^2 + \alpha^3 x + \alpha^3)}_{\text{quotient}} + \underbrace{(\alpha^8 x + \alpha^5)}_{\text{remainder}}}$$

5. Let β be a primitive 5-th root of unity in $GF(16)$. Then over $GF(16)$, we can factor $x^5 - 1$ as

$$x^5 - 1 = (x - 1)(x - \beta)(x - \beta^2)(x - \beta^3)(x - \beta^4)$$

Let α be defined as in Exercise 4. Write all elements of $GF(16)$ in exponential form.

- What are the choices for β in terms of α ?
- Use cyclotomic cosets to find the degrees of the irreducible factors of $x^5 - 1$ over $GF(2)$.
- Use the table from Exercise 4 to expand the appropriate combinations of $x - 1$, $x - \beta$, $x - \beta^2$, $x - \beta^3$ and $x - \beta^4$ to get the irreducible factors of $x^5 - 1$ over $GF(2)$.
- We can view $GF(4)$ as a subfield of $GF(16)$. Which elements of $GF(16)$ form $GF(4)$?
- Use cyclotomic cosets to find the degrees of the irreducible factors of $x^5 - 1$ over $GF(4)$.
- Use the table from Exercise 4 to expand the appropriate combinations of $x - 1$, $x - \beta$, $x - \beta^2$, $x - \beta^3$ and $x - \beta^4$ to get the irreducible factors of $x^5 - 1$ over $GF(4)$.

Solution : (a) Recall that if G is a group then for all $g \in G$ and all $k \in \mathbb{N}$, we have that $|g^k| = \frac{|g|}{\gcd(k, |g|)}$.

Here we know that $|\alpha| = 15$. So for which $1 \leq k \leq 15$ is $|\alpha^k| = 5$? This is equivalent with $\gcd(k, 15) = 3$. Hence $k \in \{3, 6, 9, 12\}$. So

$$\beta \in \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$$

(b) We easily find that the cyclotomic cosets depending on $n = 5$ and $q = 2$ are

$$\{0\} \quad \text{and} \quad \{1, 2, 4, 3\}$$

Hence the irreducible factors over $GF(2)$ are

$$x - \beta^0 \quad \text{and} \quad (x - \beta^1)(x - \beta^2)(x - \beta^3)(x - \beta^4)$$

So the degrees of the irreducible factors of $x^5 - 1$ over $GF(2)$ are one and four.

(c) Note that we can find the irreducible factors of $x^5 - 1$ over $GF(2)$ without using any tables. Since

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

and since we know there are two irreducible factors over $GF(2)$ (one of degree one and one of degree four), we must have that the irreducible factors are

$$x - 1 \quad \text{and} \quad (x - \beta^1)(x - \beta^2)(x - \beta^3)(x - \beta^4) = x^4 + x^3 + x^2 + x + 1$$

But we check this using the table from Ex.#4. We choose $\beta = \alpha^3$. Then

$$\begin{aligned} (x - \beta^1)(x - \beta^2)(x - \beta^3)(x - \beta^4) &= (x + \alpha^3)(x + \alpha^6)(x + \alpha^9)(x + \alpha^{12}) \\ &= [x^2 + (\alpha^3 + \alpha^6)x + \alpha^9] [x^2 + (\alpha^9 + \alpha^{12})x + \alpha^{21}] \\ &= [x^2 + \alpha^2 x + \alpha^9] [x^2 + \alpha^8 x + \alpha^6] \\ &= x^4 + (\alpha^2 + \alpha^8)x^3 + (\alpha^6 + \alpha^{10} + \alpha^9)x^2 + (\alpha^8 + \alpha^{17})x + \alpha^{15} \\ &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

Since

$$\begin{aligned}
\alpha^3 + \alpha^6 &= 1000 + 1100 = 0100 = \alpha^2 \\
\alpha^9 + \alpha^{12} &= 1010 + 1111 = 0101 = \alpha^8 \\
\alpha^2 + \alpha^8 &= 0100 + 0101 = 0001 = 1 \\
\alpha^6 + \alpha^{10} + \alpha^9 &= 1100 + 0111 + 1010 = 0001 = 1 \\
\alpha^8 + \alpha^{17} &= \alpha^8 + \alpha^2 = 1
\end{aligned}$$

The irreducible factors of $x^5 - 1$ over $GF(2)$ are $x + 1$ and $x^4 + x^3 + x^2 + x + 1$.

(d) We know that the multiplicative group of $GF(4)$ is a cyclic group of order 3. So if $\gamma \in GF(16)$ has order 3, then $GF(4) = \{0, 1, \gamma, \gamma^2\}$. Similarly as in (a), we are looking for $1 \leq k \leq 15$ with $\gcd(k, 15) = 5$. So we can choose $\gamma = \alpha^5$. Then

$$GF(4) = \{0, 1, \alpha^5, \alpha^{10}\}$$

(e) We easily find that the cyclotomic cosets depending on $n = 5$ and $q = 4$ are

$$\{0\}, \{1, 4\} \text{ and } \{2, 3\}$$

Hence the irreducible factors over $GF(4)$ are

$$x - \beta^0, (x - \beta^1)(x - \beta^4) \text{ and } (x - \beta^2)(x - \beta^3)$$

So the degrees of the irreducible factors of $x^5 - 1$ over $GF(4)$ are one, two and two.

(f) The irreducible factors of $x^5 - 1$ over $GF(4)$ are (where we choose $\beta = \alpha^3$) :

$$\begin{aligned}
x - \beta^0 &= x + 1 \\
(x - \beta^1)(x - \beta^4) &= (x + \alpha^3)(x + \alpha^{12}) \\
&= x^2 + (\alpha^3 + \alpha^{12})x + \alpha^{15} \\
&= x^2 + \alpha^{10}x + 1 \\
(x - \beta^2)(x - \beta^3) &= (x + \alpha^6)(x + \alpha^9) \\
&= x^2 + (\alpha^6 + \alpha^9)x + \alpha^{15} \\
&= x^2 + \alpha^5x + 1
\end{aligned}$$

since

$$\begin{aligned}
\alpha^3 + \alpha^{12} &= 1000 + 1111 = 0111 = \alpha^{10} \\
\alpha^6 + \alpha^9 &= 1100 + 1010 = 0110 = \alpha^5
\end{aligned}$$

The irreducible factors of $x^5 - 1$ over $GF(4)$ are $x + 1$, $x^2 + \alpha^5x + 1$ and $x^2 + \alpha^{10}x + 1$.

6. Let \mathbb{F}, \mathbb{K} be fields such that $\mathbb{F} \subseteq \mathbb{K}$ and $\dim_{\mathbb{F}} \mathbb{K}$ is finite. Let $\alpha \in \mathbb{K}$.

- (a) Prove that there exists a monic non-zero polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\alpha) = 0$.
- (b) Let $m(x)$ be a monic non-zero polynomial in $\mathbb{F}[x]$ with $m(\alpha) = 0$ of smallest degree. Why does $m(x)$ exist? Prove that $m(x)$ is unique and irreducible.
- (c) Let $f(x) \in \mathbb{F}[x]$ with $f(\alpha) = 0$. Prove that $m(x)$ divides $f(x)$.

Proof : We view \mathbb{K} as a vector space over the field \mathbb{F} . Put $\dim_{\mathbb{F}} \mathbb{K} = k$. Then $1, \alpha, \alpha^2, \dots, \alpha^k$ are $k + 1$ vectors in a k -dimensional vector space. Hence they are linearly dependent over \mathbb{F} . So

$$a_0 \cdot 1 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \dots + a_k \cdot \alpha^k = \vec{0} = 0$$

for some $a_0, a_1, \dots, a_k \in \mathbb{F}$, not all zero. Thus $0 \neq f(x) := a_0 + a_1x + a_2x^2 + \dots + a_kx^k \in \mathbb{F}[x]$ and $f(\alpha) = 0$. Note that it is possible that $a_k = 0$. Dividing $f(x)$ by its leading coefficient, we get a monic non-zero polynomial in $\mathbb{F}[x]$ that has α as a root.

(b) Put

$$S = \{f(x) \in \mathbb{F}[x] : f(x) \neq 0, f(\alpha) = 0 \text{ and } f(x) \text{ is monic}\}$$

We proved in (a) that $S \neq \emptyset$. Since the degree of a polynomial is a natural number, it follows that S has an element of smallest degree, say $m(x)$. Let $n(x)$ also be an element of S of smallest degree and suppose that $m(x) \neq n(x)$. Put $k(x) = m(x) - n(x)$. Then $k(x) \in \mathbb{F}[x]$, $k(x) \neq 0$ and $k(\alpha) = m(\alpha) - n(\alpha) = 0$. Since $\deg(m(x)) = \deg(n(x))$, we get that $\deg(k(x)) < \deg(m(x))$. Dividing $k(x)$ by its leading coefficient, we get a monic non-zero polynomial in $\mathbb{F}[x]$ of degree less than $\deg(m(x))$ with α as a root, a contradiction to the choice of $m(x)$. Hence $n(x) = m(x)$ and so $m(x)$ is unique.

Suppose that $m(x)$ is reducible. Since $m(x)$ is monic, we have that $m(x) = a(x)b(x)$ where $a(x), b(x)$ are monic non-constant polynomials in $\mathbb{F}[x]$. So $0 = m(\alpha) = a(\alpha)b(\alpha)$. Since we are working over the field \mathbb{F} , we have that either $a(\alpha) = 0$ or $b(\alpha) = 0$, say $a(\alpha) = 0$. As $b(x)$ is not a constant polynomial and $\deg(m(x)) = \deg(a(x)) + \deg(b(x))$, we have that $\deg(a(x)) < \deg(m(x))$, a contradiction to the choice of $m(x)$. Hence $m(x)$ is irreducible.

(c) Using the Division Algorithm, we can write

$$f(x) = m(x)q(x) + r(x) \quad \text{where } q(x), r(x) \in \mathbb{F}[x] \text{ and } \deg(r(x)) < \deg(m(x))$$

Suppose that $r(x) \neq 0$. We get that

$$r(\alpha) = f(\alpha) - m(\alpha)q(\alpha) = 0 - 0 \cdot q(\alpha) = 0$$

Dividing $r(x)$ by its leading coefficient, we get a monic non-zero polynomial in $\mathbb{F}[x]$ of degree less than $\deg(m(x))$ with α as a root, a contradiction to the choice of $m(x)$. Hence $r(x) = 0$. So $f(x) = m(x)q(x)$. Thus $m(x)$ divides $f(x)$. \square