For every y_i, $1 \le i \le m$, there exist elements $a_{ij} \in F$, $1 \le j \le n$, such that

$$y_i = \sum_{j=1}^{n} a_{ij}\alpha_j$$

Substituting these values of y_i in the expression for x, we find that x can be expressed as a linear combination of the elements $\alpha_j\beta_i$, $1 \le i \le m$, $1 \le j \le n$, with coefficients in F. Thus, the elements $\{\alpha_j \beta_i\}$ $1 \le i \le m$, $1 \le j \le n$, generate L over F.

Suppose that elements $a_{ij} \in F$, $1 \le i \le m$, $1 \le j \le n$ are such that

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}\alpha_j\beta_i = 0$$

Then

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij}\alpha_j \right) \beta_i = 0$$

and $\{\beta_i\}$, $1 \le i \le m$, being a basis of L over K, we have

$$\sum_{j=1}^{n} a_{ij}\alpha_j = 0 \quad \forall i, 1 \le i \le m$$

But then $\{\alpha_j\}$, $1 \le j \le n$ being a basis of K over F, we have $a_{ij} = 0 \forall j$, $1 \le j \le n$ and $\forall i$, $1 \le i \le m$. This proves that $\{\alpha_j\beta_i\}$, $1 \le i \le m$, $1 \le j \le n$ is a basis of L over F and

$$[L{:}F] = mn = [L{:}K][K{:}F] \qquad \blacksquare$$

Let F be a prime field of characteristic $p \ne 0$, $f(X) \in F[X]$ be an irreducible polynomial of degree n and $I = \langle f(X) \rangle$ be the ideal generated by $f(X)$. Then $K = F[X]/I$ is a field and clearly an arbitrary element of K is of form $g(X) + I$, where $g(X) \in F[X]$ is a polynomial of degree at most $n - 1$. Also it follows that such an expression of an element of K is uniquely determined. Therefore $\mathrm{O}(K) = p^n$. Thus, in order to construct a field K of order p^n, p a prime and n a positive integer, we need to find an irreducible polynomial $f(X)$ of degree n over the field of p elements. Also, observe that every element of $K = F[X]/I$ is a root of the polynomial

$$X^{p^n} - X$$

and, so, the irreducible polynomial $f(X)$ must be a divisor of $X^{p^n} - X$.

Proposition 4.4

Let $f(X)$ be a polynomial of degree 2 or 3 over a field F. Then $f(X)$ is irreducible iff none of the elements of F is a root of $f(X)$.

Proof

Suppose that $f(X)$ is reducible. Then $f(X)$ has a linear factor $aX + b$, say, where $a, b \in F$, $a \ne 0$. Then $-b/a \in F$ is a root of $f(X)$. Conversely, suppose that

$\alpha \in F$ is a root of $f(X)$. Then $X - \alpha \mid f(X)$. For example, if

$$f(X) = aX^3 + bX^2 + cX + d \qquad a, b, c, d \in F$$

then

$$\begin{aligned} f(X) &= aX^3 + bX^2 + cX + d - (a\alpha^3 + b\alpha^2 + c\alpha + d) \\ &= (X - \alpha)[a(X^2 + \alpha X + \alpha^2) + b(X + \alpha) + c] \end{aligned}$$

and

$$a(X^2 + \alpha X + \alpha^2) + b(X + \alpha) + c \in F[X]$$

This proves that $f(X)$ is reducible.

Example 4.1

Let F be the field of 5 elements. None of the elements of F is a root of the polynomial $f(X) = X^2 + 2$ and so $f(X)$ is irreducible in $F[X]$. Hence

$$K = F[X]/\langle f(X) \rangle$$

is a field of order 25. An arbitrary element of K is of the form

$$aX + b + \langle f(X) \rangle \quad a, b \in F$$

Write $X + \langle f(X) \rangle = \alpha$. The powers of α are then determined as follows: $\alpha^2 = 3$, $\alpha^3 = 3\alpha$, $\alpha^4 = 4$, $\alpha^5 = 4\alpha$, $\alpha^6 = 2$, $\alpha^7 = 2\alpha$ and $\alpha^8 = 1$. Thus α is not a primitive element of K.

Taking $\beta = \alpha + 4$ gives

$$\begin{aligned} \beta^2 &= \alpha^2 + 3\alpha + 1 = 3\alpha + 4 \\ \beta^3 &= (3\alpha + 4)(\alpha + 4) = \alpha \\ \beta^4 &= 4\alpha + \alpha^2 = 4\alpha + 3 \\ \beta^5 &= (\alpha + 4)(4\alpha + 3) = 4\alpha + 4 \\ \beta^6 &= (4\alpha + 4)(\alpha + 4) = 3 \\ \beta^7 &= 3\alpha + 2 \\ \beta^8 &= (3\alpha + 2)(\alpha + 4) = 4\alpha + 2 \\ \beta^9 &= (4\alpha + 2)(\alpha + 4) = 3\alpha \\ \beta^{10} &= 3\alpha^2 + 2\alpha = 2\alpha + 4 \\ \beta^{11} &= (2\alpha + 4)(\alpha + 4) = 2\alpha + 2 \\ \beta^{12} &= (2\alpha + 2)(\alpha + 4) = 4 \end{aligned}$$

Thus the order of β in the multiplicative group of K is greater than 12 and hence β is a primitive element of K.

Example 4.2

Let F be the field of 3 elements. None of the elements of F is a root of the polynomial $X^3 + 2X + 2 \in F[X]$ and so it is irreducible in $F[X]$. Therefore

$$K = F[X]/\langle X^3 + 2X + 2 \rangle$$

is a field of order $3^3 = 27$. Let the element $X + \langle X^3 + 2X + 2\rangle$ be denoted by α. Then

$$\begin{aligned}
\alpha^3 &= \alpha + 1 \\
\alpha^6 &= \alpha^2 + 2\alpha + 1 \\
\alpha^{12} &= \alpha^4 + 4\alpha^2 + 1 + 4\alpha^3 + 2\alpha^2 + 4\alpha \\
&= \alpha^4 + \alpha^3 + \alpha + 1 \\
&= \alpha^2 + \alpha + \alpha + 1 + \alpha + 1 \\
&= \alpha^2 + 2
\end{aligned}$$

and then

$$\alpha^{13} = \alpha^3 + 2\alpha = \alpha + 1 + 2\alpha = 1$$

Thus α is not a primitive element of K. Taking $\beta = \alpha^2 + 1$, we find that

$$\begin{aligned}
\beta^2 &= \alpha + 1 \neq 1 \\
\beta^3 &= \alpha^6 + 1 = (\alpha + 1)^2 + 1 = \alpha^2 + 2\alpha + 2 \\
\beta^6 &= \alpha^4 + \alpha^2 + 1 + \alpha^3 + \alpha^2 + 2\alpha = \alpha^2 + \alpha + \alpha^2 + 1 + \alpha + 1 + \alpha^2 + 2\alpha = \alpha + 2 \\
\beta^{12} &= \alpha^2 + \alpha + 1 \\
\beta^{13} &= (\alpha^2 + \alpha + 1)(\alpha^2 + 1) = \alpha^4 + \alpha^3 + 2\alpha^2 + \alpha + 1 = 2 \neq 1
\end{aligned}$$

Hence β is a primitive element of K.

Example 4.3

As in Chapter 1, let $\mathbb{B}$ be the field of 2 elements.

Case (i)

Neither of the two elements of $\mathbb{B}$ is a root of the polynomial $X^3 + X + 1 \in \mathbb{B}[X]$ and, so, the polynomial $X^3 + X + 1$ is irreducible over $\mathbb{B}$. Therefore,

$$K = \mathbb{B}[X]/\langle X^3 + X + 1\rangle$$

is a field of order 8. Let the element $X + \langle X^3 + X + 1\rangle$ be denoted by α. The multiplicative group of K is of order 7 and, so, any non-zero, non-identity element of K is primitive. In particular, so is the element α.

Case (ii)

Consider the polynomial $X^4 + X + 1 \in \mathbb{B}[X]$. Neither of the elements of $\mathbb{B}$ is a root of this polynomial and, so, $f(X) = X^4 + X + 1$ does not have a linear factor in $\mathbb{B}[X]$. Therefore, if $f(X)$ is reducible in $\mathbb{B}[X]$, it must be a product of only quadratic polynomials. But the only polynomial in $\mathbb{B}[X]$ of degree 2 which is irreducible is $X^2 + X + 1$ and

$$(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq X^4 + X + 1$$

Thus $f(X)$ is an irreducible polynomial and $K = \mathbb{B}[X]/\langle f(X)\rangle$ is a field of order 16. Let

$$\alpha = X + \langle f(X)\rangle$$

Then

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

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

and since $\mathrm{O}(\alpha)$ as an element of the multiplicative group of K divides 15, α is a primitive element of K. All the elements of K then are 0, 1, α, α^2, α^3, $\alpha + 1$, $\alpha^2 + \alpha$, $\alpha^3 + \alpha^2$, $\alpha^3 + \alpha + 1$, $\alpha^2 + 1$, $\alpha^3 + \alpha$, $\alpha^2 + \alpha + 1$, $\alpha^3 + \alpha^2 + \alpha$, $\alpha^3 + \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + 1, \alpha^3 + 1$. These non-zero elements are the powers of α in order.

Case (iii)

We can prove as in Case (ii) above that $X^4 + X^3 + 1$ is another polynomial of degree 4 which is irreducible over $\mathbb{B}$. Hence

$$K = \mathbb{B}[X]/\langle X^4 + X^3 + 1\rangle$$

is a field of order 16. Setting

$$\alpha = X + \langle X^4 + X^3 + 1\rangle$$

we find that $\alpha^4 = \alpha^3 + 1$. Then

$$\alpha^5 = \alpha^3 + \alpha + 1 \quad \alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1 \quad \alpha^7 = \alpha^2 + \alpha + 1$$

$$\alpha^8 = \alpha^3 + \alpha^2 + \alpha \quad \alpha^9 = \alpha^2 + 1 \quad \alpha^{10} = \alpha^3 + \alpha \quad \alpha^{11} = \alpha^3 + \alpha^2 + 1$$

$$\alpha^{12} = \alpha + 1 \quad \alpha^{13} = \alpha^2 + \alpha \quad \alpha^{14} = \alpha^3 + \alpha^2 \quad \alpha^{15} = 1$$

Thus α is a primitive element of K (this could have been concluded from $\alpha^3 \neq 1$, $\alpha^5 \neq 1$ but the above illustrates all the powers of α).

Case (iv)

Yet another polynomial of degree 4 which is irreducible over $\mathbb{B}$ is

$$X^4 + X^3 + X^2 + X + 1$$

Thus

$$\mathbb{B}[X]/\langle X^4 + X^3 + X^2 + X + 1\rangle$$

is a field of order 16. However, in this case, the element

$$\alpha = X + \langle X^4 + X^3 + X^2 + X + 1\rangle$$

is not a primitive element of the field because

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

and then

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

Case (v)

Next consider the polynomial $X^6 + X^5 + 1$ over $\mathbb{B}$. It is clear that neither 0 nor 1 is a root of this polynomial. Therefore a possible factor of degree 2 of this polynomial is $X^2 + X + 1$. Let

$$X^6 + X^5 + 1 = (X^2 + X + 1)(X^4 + aX^3 + bX^2 + cX + 1)$$

Comparing the coefficients of various powers of X, gives

$$a + 1 = 1 \quad a + b + 1 = 0 \quad a + b + c = 0 \quad b + c + 1 = 0$$

The first three equations imply that $a = 0$, $b = c = 1$ and then the fourth gives $1 = 0$ – a contradiction. Thus the polynomial can have only cubic factors. Irreducible polynomials of degree 3 are

$$X^3 + X + 1 \qquad \text{and} \qquad X^3 + X^2 + 1$$

Now

$$(X^3 + X + 1)^2 = X^6 + X^2 + 1$$
$$(X^3 + X^2 + 1)^2 = X^6 + X^4 + 1$$

and

$$(X^3 + X^2 + 1)(X^3 + X + 1) = X^6 + X^5 + X^4 + X^2 + X + 1$$

This proves that $X^6 + X^5 + 1$ is irreducible over $\mathbb{B}$. Then

$$K = \mathbb{B}[X]/\langle X^6 + X^5 + 1\rangle$$

is a field of order $2^6 = 64$. Let

$$\alpha = X + \langle X^6 + X^5 + 1\rangle$$

Then

$$\alpha^6 = \alpha^5 + 1 \quad \alpha^7 = \alpha^5 + \alpha + 1 \quad \alpha^8 = \alpha^5 + \alpha^2 + \alpha + 1$$
$$\alpha^9 = \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1 \quad \alpha^{10} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$$
$$\alpha^{11} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 \quad \alpha^{12} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$$
$$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + 1 \quad \alpha^{14} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha \quad \alpha^{15} = \alpha^4 + \alpha^2 + 1$$
$$\alpha^{16} = \alpha^5 + \alpha^3 + \alpha \quad \alpha^{17} = \alpha^5 + \alpha^4 + \alpha^2 + 1 \quad \alpha^{18} = \alpha^3 + \alpha + 1$$
$$\alpha^{19} = \alpha^4 + \alpha^2 + \alpha \quad \alpha^{20} = \alpha^5 + \alpha^3 + \alpha^2 \quad \alpha^{21} = \alpha^5 + \alpha^4 + \alpha^3 + 1$$

Since the order of α divides 63 – the order of the multiplicative group K^* of K – it follows from the above computations that $O(\alpha) = 63$ and α is a primitive element of K.

Recall that a polynomial

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

with integer coefficients $a_0, a_1, \ldots, a_n$ is called **primitive** if

$$\mathrm{GCD}(a_0, a_1, \ldots, a_n) = 1$$

However, while working with polynomials over a field of p elements (p a prime), we deviate from this accepted terminology and call an irreducible polynomial $f(X) \in F_p[X]$ of degree n, where F_p is the field of p elements, primitive if:

(i) $f(X)$ divides $X^{p^n-1} - 1$; and
(ii) $f(X)$ does not divide $X^k - 1$ for any $k < p^n - 1$.

In our applications of finite fields to coding theory we are concerned with:

(i) the construction of a field K of order p^n for a given prime p and natural number n; and
(ii) finding a primitive element in K.

We have already proved above that if $f(X) \in F_p[X]$, where F_p is a field of p elements, is an irreducible polynomial of degree n, then $F_p[X]/\langle f(X)\rangle$ is a field of order p^n. Also as seen in Examples 4.3 Cases (i), (ii), (iii) and (v) there are situations in which $X + \langle f(X)\rangle$ is a primitive element of $K = F_p[X]/\langle f(X)\rangle$. That this is not always the case is shown by the Examples 4.1, 4.2 and 4.3 Case (iv). In fact we have the following proposition.

Proposition 4.5
Given an irreducible polynomial $f(X) \in F_p[X]$, the element

$$\alpha = X + \langle f(X)\rangle \in F_p[X]/\langle f(X)\rangle$$

($= K$, say) is primitive iff $f(X)$ is a primitive polynomial.

Proof
Let $\deg f(X) = n$. Then $\mathrm{O}(K) = p^n = m$ (say) and $\mathrm{O}(\alpha) = t \leq m - 1$. Therefore

$$X^{m-1} - 1 + \langle f(X)\rangle = 0$$

i.e. $f(X) | X^{m-1} - 1$.

Observe that

$$f(X) | X^r - 1 \quad \text{iff} \quad \mathrm{O}(\alpha) | r$$

Thus $t = \mathrm{O}(\alpha)$ is the smallest value of r for which $f(X) | X^r - 1$. This proves that α is primitive iff the smallest value of r for which $f(X) | X^r - 1$ is $m - 1$, i.e. iff $f(X)$ is a primitive polynomial.

Deciding whether a given irreducible polynomial over F_p is primitive is not an easy problem. More information on this problem is found when we