6 Galois fields

We have seen that the mathematical framework for linear codes and cyclic codes are matrices and polynomials respectively. For each type of code, encoding and decoding can be concisely formulated in terms of their respective mathematics. This difference in mathematics signifies more than just mathematical representation, for in going from linear codes to cyclic codes there is an increase in underlying mathematical structure. Moving on, from cyclic codes to the next level of codes with greater mathematical structure are the BCH codes, considered in Chapter 7. The mathematical framework within which the BCH codes are addressed is that of Galois fields and it is these that we consider next.

6.1 Roots of equations

We have already considered fields, in particular finite fields, in Chapter 5. Here we are interested in finite fields constructed from the roots of equations. The motivation for this approach lies in the property of cyclic codes that all codeword polynomials $c(x)$ have the generator polynomial $g(x)$ as a factor. This can be restated by saying that any root of $g(x)=0$ is also a root of $c(x)=0$ and it is the exploitation of roots of equations that takes us to the BCH codes and to the finite fields relevant to the codes.

Consider the *algebraic equation* of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0 \tag{6.1}$$

where $a_0 \neq 0$. For now the coefficients $a_0, a_1, \ldots, a_n$ are taken to be real numbers but later we consider eqn 6.1 when the coefficients are binary. The simplest algebraic equation is the equation of first degree obtained by setting $n=1$, this is usually written as

$$ax + b = 0$$

where $a=a_1$, $b=a_0$ and there exists one root $x=-b/a$. The second degree (quadratic) equation, commonly expressed as

$$ax^2 + bx + c = 0$$

where now $a=a_2$, $b=a_1$ and $c=a_0$, has 2 roots given by the famous 'formula' for solving quadratic equations

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{6.2}$$

The roots of equations of third and fourth degree, with 3 and 4 roots respectively, can likewise be obtained algebraically. However, the same is not true for fifth-degree equations for it has been shown that it is not possible to solve the fifth-degree equation using a finite number of algebraic operations, in other words it is impossible to obtain the roots algebraically. This was established in the early 19th century by Abel, a Norwegian mathematician. Furthermore, it is now known that algebraic equations of degree greater than 5 cannot be solved algebraically. This though does not mean that roots for fifth and higher degree equations do not exist, it is just that expressions for giving the roots do not exist. A fifth-degree equation has 5 roots and an equation with degree n, as given by eqn 6.1, has n roots. There is, however, one slight problem regarding the nature of some of the roots. Returning to the quadratic equation $ax^2 + bx + c = 0$ and setting $a = c = 1$ and $b = 0$ gives

$$x^2 + 1 = 0. \tag{6.3}$$

Each root of eqn 6.3 has the property that when multiplied by itself it gives -1. But there are no real numbers that have this property and the only way of obtaining 2 roots for eqn 6.3 is by defining a new *imaginary* or *complex* number j, which satisfies

$$\mathrm{j}^2 + 1 = 0. \tag{6.4}$$

The number j can be combined with 2 real numbers p and q to give the complex number $p + \mathrm{j}q$. Addition and multiplication over the set of all complex numbers obey the rules described in Section 5.3 for a set of elements to form a field, and the resulting field is known as the *complex field*. It is because of the existence of the complex field that all equations of degree n have n roots. The roots to eqn 6.1 are of the form $p + \mathrm{j}q$ with real roots having $q = 0$. If we consider a quadratic equation with $b \neq 0$, for example

$$x^2 - 4x + 13 = 0$$

then using eqn 6.2 we can easily find that there are two complex roots $2 - \mathrm{j}3$ and $2 + \mathrm{j}3$. Complex roots, of an equation with real coefficients, always occur in pairs known as *complex conjugates* or *conjugates*, which take the form $p \pm \mathrm{j}q$. The complex number $p - \mathrm{j}q$ is the conjugate of $p + \mathrm{j}q$, and likewise $p + \mathrm{j}q$ is the conjugate of $p - \mathrm{j}q$. An equation can never have an odd number of complex roots, this would require a complex root without a conjugate. In a cubic equation the roots are either all real or there is one real root and two roots that are complex conjugates. For example, the roots of

$$x^3 - 6x^2 + 13x - 20 = 0$$

are 4, $1 + \mathrm{j}2$ and $1 - \mathrm{j}2$.

The complex field includes all the real numbers as they can be considered as field elements with $q = 0$. We can think of the complex field as expanding or extending the real field that we started with. In this sense, the real field is referred to as a *base field* and the complex field as an *extension field*, the complex field is an extension of the real field. The coefficients $a_0, a_1, \ldots, a_n$ in eqn 6.1 belong to the base field (i.e. the real field) whereas the roots belong to the extension field (i.e. the complex field). The occurrence of complex roots as conjugate pairs is necessary for the coefficients

to lie in the real field. To illustrate this, let's try to construct a quadratic equation with 2 roots that are not conjugate pairs. For example let $1+j2$ and $3-j4$ be roots of a quadratic equation, then the quadratic equation will be

$$(x-(1+j2))(x-(3-j4)) = x^2-(4-j2)x+(11+j2)$$

which has coefficients in the complex field. It can be easily shown that if the coefficients of a quadratic equation, with complex roots, lie in the real field then the roots must form a conjugate pair.

Example 6.1

If $p+jq$ is a root of a quadratic equation with real coefficients, show that its conjugate $p-jq$ is the other root.

Let $a+jb$ be the other root, then the quadratic equation is

$$(x-(p+jq))(x-(a+jb)) = 0$$

which gives

$$x^2-x[(a+p)+j(b+q)]+(pa-qb)+j(aq+bp) = 0.$$

If the quadratic equation is to have real coefficients then the complex terms must equal zero, and so

$$b+q = 0$$
$$aq+bp = 0$$

which give $b=-q$ and $a=p$. Hence $a+jb=p-jq$ and so the two roots are conjugates of each other. □

We next consider roots of equations of the form $p(x)=0$ where $p(x)$ is a polynomial with binary coefficients. As we have seen such polynomials are used for encoding and decoding binary cyclic codes. The trivial cases of $x+1=0$ and $x^2+1=0$ have 1 as a root, in the latter case 1 is a double root. The quadratic equation

$$x^2+x+1 = 0 \tag{6.5}$$

presents more of a problem. We cannot use eqn 6.2 for solving this because eqn 6.2 has a 2 on the denominator and $2=0$ when using modulo-2 arithmetic. Since x can only have a value of 0 or 1, we can substitute 0 and 1 directly into eqn 6.5 to see which, if any, is a root. Substituting $x=0$ into eqn 6.5 gives 1 and so 0 is not a root. Likewise $x=1$ gives 1 and therefore neither 0 or 1 are roots of eqn 6.5. As another example consider

$$x^3+x+1 = 0. \tag{6.6}$$

Substituting $x=0$ or $x=1$ into this gives 1, and so again we have a binary polynomial without any binary roots. This is analogous to the situation encountered previously where we considered a real quadratic equation without any real roots, so the complex term j is 'invented' to get around the problem. Here we proceed in the

same manner by defining a new term such that it is a root of the polynomial of interest. We will consider eqn 6.6 instead of eqn 6.5 as this proves to be more interesting. We could use j to denote a root of eqn 6.6, but this may cause confusion with the use of j in ordinary complex numbers. Instead it is conventional to use α to represent the newly defined root. Substituting $x = \alpha$ into eqn 6.6 gives

$$\alpha^3 + \alpha + 1 = 0. \tag{6.7}$$

Whilst eqn 6.7 may define the new root α it tells us little else about it and furthermore there are 2 more roots of eqn 6.6 that we need to find. We know that α does not belong to the binary field and to proceed further we need to determine the mathematical structure of the field within which α lies. The root α lies within a finite field known as $GF(2^3)$ which can be generated from eqn 6.7. Once $GF(2^3)$ has been established the other roots can be found.

6.2 The Galois field $GF(2^3)$

The field $GF(2^3)$ can be generated from the newly defined element α given by eqn 6.7. First consider addition and multiplication of α with the binary numbers 0 and 1. The binary numbers 0 and 1 form additive and multiplicative identity elements respectively, so

$$\alpha + 0 = \alpha$$
$$\alpha 1 = \alpha.$$

The additive inverse of α is α itself, as can be easily shown

$$\alpha + \alpha = 1\alpha + 1\alpha = (1 + 1)\alpha = 0\alpha = 0$$

and so

$$\alpha + \alpha = 0.$$

Furthermore rearranging this gives

$$\alpha = -\alpha$$

and therefore subtraction and addition of α are equivalent. The multiplicative inverse of α is defined as

$$\alpha^{-1} = \frac{1}{\alpha}$$

so that

$$\alpha^{-1}\alpha = \frac{1}{\alpha}\alpha = 1.$$

Table 6.1 summarizes the identity and inverse elements of α.

In eqn 6.7 it is implicit that $\alpha^3 = \alpha\alpha\alpha$ and likewise other powers of α can be defined, for example $\alpha^2 = \alpha\alpha$. Higher powers of α can be determined by rearranging

Table 6.1
Identity and inverse elements of α

Identity elements	Additive	0,	$\alpha+0=\alpha$
	Multiplicative	1,	$\alpha 1=\alpha$
Inverse elements	Additive	α,	$\alpha+\alpha=0$
	Multiplicative	α^{-1}	$\alpha\alpha^{-1}=1$

eqn 6.7 to give $\alpha^3=\alpha+1$ (recall that $-\alpha=\alpha$), repeatedly multiplying by α and substituting $\alpha+1$ for α^3 whenever α^3 appears. Starting first with α^3

$$\begin{aligned}
\alpha^3 &= \alpha+1\\
\alpha^4 &= \alpha\alpha^3=\alpha(\alpha+1)=\alpha^2+\alpha\\
\alpha^5 &= \alpha\alpha^4=\alpha(\alpha^2+\alpha)=\alpha^3+\alpha^2=\alpha^2+\alpha+1\\
\alpha^6 &= \alpha\alpha^5=\alpha(\alpha^2+\alpha+1)=\alpha^3+\alpha^2+\alpha=\alpha^2+1.
\end{aligned} \tag{6.8}$$

The four elements α^3, α^4, α^5, and α^6 differ from each other and from the four elements 0, 1, α, and α^2. Equations 6.8 are referred to as the *polynomial representations* of the elements α^3, α^4, α^5, and α^6. It may appear that other elements can be constructed by taking further powers of α. This though is not so, for the next power of α gives

$$\alpha^7=\alpha\alpha^6=\alpha(\alpha^2+1)=\alpha^3+\alpha=\alpha+1+\alpha=1$$

and therefore

$$\alpha^7=1$$

which is an existing element. Forming further powers of α always generates one of the existing nonzero elements. For example, the next three powers give

$$\begin{aligned}
\alpha^8 &= \alpha\alpha^7=\alpha 1=\alpha\\
\alpha^9 &= \alpha\alpha^8=\alpha\alpha=\alpha^2\\
\alpha^{10} &= \alpha\alpha^9=\alpha\alpha^2=\alpha^3.
\end{aligned}$$

A field element with power greater than 6 can be reduced to an element with power of 6 or less by removing factors of α^7. This is equivalent to taking the power modulo-7. For example

$$\begin{aligned}
\alpha^{12} &= \alpha^7\alpha^5=\alpha^5(12=5 \text{ modulo-7})\\
\alpha^{17} &= \alpha^7\alpha^7\alpha^3=\alpha^3(17=3 \text{ modulo-7})
\end{aligned}$$

and so forth. Taking into account 0 and 1 we see that we have constructed a set with the 8 elements

$$0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \text{and } \alpha^6.$$

Along with the operations addition and multiplication the set forms a field, namely the field $GF(2^3)$. Unlike the field of real numbers, which has an infinite number of field elements, $GF(2^3)$ has a finite number of field elements and is therefore a finite

field. Finite fields are also referred to as *Galois fields* after the mathematician Evariste Galois (1811–1832). The fields are usually expressed as $GF(p^m)$ where p is the number of elements in the base field, which is referred to as the field's *characteristic*, and m is the degree of the polynomial whose root is used to construct the field. The order of the field is given by $q = p^m$.

Table 6.2 shows the 8 elements of $GF(2^3)$ along with the polynomial representations of α^3, α^4, α^5, and α^6 in terms of 1, α, and α^2. We have already seen that $\alpha + \alpha = 0$, likewise any field element added to itself gives zero. For example

$$\alpha^3 + \alpha^3 = 1\alpha^3 + 1\alpha^3 = \alpha^3(1 + 1) = 0.$$

Two different field elements can be added together by using their polynomial representations. For example, adding α^4 and α^6 gives

$$\alpha^4 + \alpha^6 = (\alpha^2 + \alpha) + (\alpha^2 + 1) = \alpha + 1 = \alpha^3.$$

Example 6.2

Find (a) $\alpha^2 + \alpha$, (b) $\alpha^5 + \alpha + 1$, and (c) $\alpha^6 + \alpha^2 + 1$.

(a) From Table 6.2 we see that $\alpha^2 + \alpha = \alpha^4$.

(b) Here we first rewrite α^5 in terms of its polynomial representation and then cancel out equal field elements

$$\alpha^5 + \alpha + 1 = (\alpha^2 + \alpha + 1) + \alpha + 1 = \alpha^2.$$

(c) We can express α^6 as $\alpha^2 + 1$, and so

$$\alpha^6 + \alpha^2 + 1 = (\alpha^2 + 1) + \alpha^2 + 1 = 0.$$

□

Using the polynomial representation of field elements to add 2 elements together is rather tedious. It is easier to construct a table showing the results of all additions and then to refer to the table when needed. Table 6.3(a) shows addition of elements within $GF(2^3)$.

Table 6.2
The field elements of $GF(2^3)$

0
1
α
α^2
$\alpha^3 = \alpha + 1$
$\alpha^4 = \alpha^2 + \alpha$
$\alpha^5 = \alpha^2 + \alpha + 1$
$\alpha^6 = \alpha^2 + 1$

Table 6.3
Addition and multiplication in $GF(2^3)$

(a) *Addition*

+	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	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

(b) *Multiplication*

×	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	α^3	α^4	α^5	α^6
α	0	α	α^2	α^3	α^4	α^5	α^6	1
α^2	0	α^2	α^3	α^4	α^5	α^6	1	α
α^3	0	α^3	α^4	α^5	α^6	1	α	α^2
α^4	0	α^4	α^5	α^6	1	α	α^2	α^3
α^5	0	α^5	α^6	1	α	α^2	α^3	α^4
α^6	0	α^6	1	α	α^2	α^3	α^4	α^5

Multiplying two field elements together is straightforward, their powers are added together and because $\alpha^7 = 1$ factors of α^7 can be removed. For example, the product of α^3 and α^6 gives

$$\alpha^3\alpha^6 = \alpha^{3+6} = \alpha^9 = \alpha^7\alpha^2 = 1\alpha^2 = \alpha^2.$$

This is the same as taking the sum modulo-7 of the two powers. In the above case we have $3 + 6 = 2$ modulo-7 and the resulting field element is α^2 as obtained. Therefore the product of the field elements α^i and α^j in $GF(2^3)$ is

$$\alpha^i\alpha^j = \alpha^{(i+j)\text{modulo-7}}$$

Although there is no need to refer to a multiplication table when multiplying field elements, one is included for completeness (see Table 6.3b).

Example 6.3
Find (a) $\alpha\alpha^5$, (b) $\alpha^4\alpha^5$, and (c) $\alpha^5\alpha^6\alpha^4$.

(a) $\alpha\alpha^5 = \alpha^6$

(b) $\alpha^4\alpha^5 = \alpha^9 = \alpha^7\alpha^2 = \alpha^2$

(c) $\alpha^5\alpha^6\alpha^4 = \alpha^{15} = \alpha^7\alpha^7\alpha = \alpha$. □

For any field element α^i in $GF(2^3)$ we have

$$\alpha^i + \alpha^i = 1\alpha^i + 1\alpha^i = \alpha^i(1 + 1) = 0$$

and therefore each element is its own additive inverse. The multiplicative inverse of α^i is defined as the element α^{-i} such that

$$\alpha^i\alpha^{-i} = 1$$

and is given by

$$\alpha^{-i} = \alpha^{7-i}.$$

Taking the product of α^i with α^{-i} gives $\alpha^i\alpha^{-i} = \alpha^{i+7-i} = \alpha^7 = 1$ and so α^{-i} satisfies the requirement for a multiplicative inverse. Take, for instance, the multiplicative inverse of α^3

$$\alpha^{-3} = \alpha^{7-3} = \alpha^4$$

and so the multiplicative inverse of α^3 is α^4. Note that the element 1 is its own multiplicative inverse.

One of the requirements of a field is that division by nonzero elements is possible. Given α^i and α^j in $GF(2^3)$, where $\alpha^j \neq 0$, then α^i divided by α^j is

$$\frac{\alpha^i}{\alpha^j} = \alpha^i\alpha^{-j} = \alpha^{(i-j)\text{modulo-7}}$$

where α^{-j} is the multiplicative inverse of α^j. Note that if $i-j<0$ then $(i-j)$ modulo-7 is found by adding 7 to $i-j$. Also if $i=j$ then clearly $\alpha^i/\alpha^j = 1$. For example

$$\frac{\alpha^6}{\alpha^2} = \alpha^6\alpha^{-2} = \alpha^{(6-2)\text{modulo-7}} = \alpha^4.$$

The above calculation can also be thought of as follows

$$\frac{\alpha^6}{\alpha^2} = \alpha^6\alpha^{-2} = \alpha^6\alpha^5 = \alpha^{11\text{modulo-7}} = \alpha^4$$

where we have now made use of α^5 the multiplicative inverse of α^2, either way the same answer is obtained. Consider α divided by α^5, if we use the multiplicative inverse of α^5, which is α^2, we get

$$\frac{\alpha}{\alpha^5} = \alpha\alpha^{-5} = \alpha\alpha^2 = \alpha^3$$

or without using the inverse we can view the calculation as

$$\frac{\alpha}{\alpha^5} = \alpha\alpha^{-5} = \alpha^{(1-5)\text{modulo-7}} = \alpha^{(-4)\text{modulo-7}} = \alpha^3.$$

Example 6.4

Find (a) α^2/α^5, (b) $1/\alpha$, (c) α^3/α, and (d) α/α^3.

(a) The inverse of α^5 is α^2, and so $\alpha^2/\alpha^5 = \alpha^2\alpha^2 = \alpha^4$. Or we can view this as $\alpha^2/\alpha^5 = \alpha^{(2-5)\text{modulo-7}} = \alpha^4$.

(b) $1/\alpha = \alpha^6$

(c) $\alpha^3/\alpha = \alpha^2$

(d) $\alpha/\alpha^3 = \alpha^5$. □

We now return to the problem of finding the three roots of the binary equation $x^3 + x + 1 = 0$ (see Section 6.1). We have already 'found' 1 root, namely α belonging to $GF(2^3)$, and next we will use a trial-and-error method to test the other elements of $GF(2^3)$ to see if they satisfy $x^3 + x + 1 = 0$. Only 5 of the 8 elements need to be

considered as α is a root by definition and 0 and 1 are known not to be roots. Starting with $x = \alpha^2$ gives

$$\alpha^6 + \alpha^2 + 1 = 1 + 1 = 0$$

and so α^2 is a root (here we have referred to Table 6.3(a) to get $\alpha^2 + \alpha^6 = 1$). Next try $x = \alpha^3$

$$\alpha^9 + \alpha^3 + 1 = \alpha^7\alpha^2 + \alpha^3 + 1 = \alpha^2 + \alpha = \alpha^4 \neq 0$$

and so α^3 is not a root. Continuing with $x = \alpha^4$ gives

$$\alpha^{12} + \alpha^4 + 1 = \alpha^5 + \alpha^4 + 1 = 1 + 1 = 0$$

and therefore α^4 is the third root. The elements α^5 and α^6 cannot be roots because a cubic equation can only have 3 roots. As a check, substituting α^5 and α^6 into $x^3 + x + 1$ gives α^2 and α respectively, thus confirming that they are not roots. Therefore the three roots of the binary equation

$$x^3 + x + 1 = 0$$

are the field elements α, α^2, and α^4 belonging to the finite field $GF(2^3)$. Hence the original aim of finding the equation's roots has been achieved.

In Section 6.1 we considered equations with real coefficients and complex roots and the idea of base and extension fields were introduced in the context of the real and complex fields. The real field is thought of as the base field containing the equations' coefficients. The extension field contains the base field and extends it to include the complex roots. In the present case the equation of interest $x^3 + x + 1 = 0$ has its coefficients in the binary field and its roots in $GF(2^3)$. The binary field is denoted by ***GF(2)*** as it is a finite field with 2 elements. The field $GF(2^3)$ is an extension field of the binary field $GF(2)$. Note that $GF(2^3)$ is not the only extension field of $GF(2)$. The field $GF(2^3)$ has been constructed by determining the roots of the polynomial $p(x) = x^3 + x + 1$. Other extension fields can be generated using different polynomials. However, not all polynomials can generate extension fields, this is considered further in Section 6.5.

6.3 The fields $GF(2^4)$ and $GF(2^5)$

Here we are going to first construct the finite field $GF(2^4)$ and then take a brief look at $GF(2^5)$. $GF(2^4)$ is a field that the reader will encounter in most text books on error control. $GF(2^3)$ was constructed using a cubic polynomial that does not have 0 or 1 as roots. Consider the polynomial

$$p(x) = x^4 + x + 1. \tag{6.9}$$

Neither 0 or 1 are roots of $p(x) = 0$, it can be easily seen that $p(0) = p(1) = 1$. The four roots of eqn 6.9 therefore lie outside the binary field $GF(2)$. If we let α be one of

the roots, then $p(\alpha) = 0$ by definition and

$$\alpha^4 + \alpha + 1 = 0. \tag{6.10}$$

Equation 6.10 is used to generate $GF(2^4)$ in the same way as eqn 6.7 was used to generate $GF(2^3)$. The binary elements 0 and 1 are again additive and multiplicative identity elements of α respectively. To determine the elements of $GF(2^4)$ we proceed in the same manner as when constructing $GF(2^3)$, by forming successive powers of α until an existing element is generated. Rearranging 6.10 gives

$$\alpha^4 = \alpha + 1. \tag{6.11}$$

When constructing higher powers of α eqn 6.11 is used to reduce field elements to their lowest power. Starting with α^4 and successively multiplying by α gives

$$\begin{aligned}
\alpha^4 &= \alpha + 1 \\
\alpha^5 &= \alpha\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha \\
\alpha^6 &= \alpha\alpha^5 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 \\
\alpha^7 &= \alpha\alpha^6 = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1.
\end{aligned} \tag{6.12}$$

Note that at this point $\alpha^7 = 1$ in $GF(2^3)$. However, here α^7 differs from all the previous elements and we therefore continue producing higher powers of α until an existing element is obtained

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

All the elements generated so far are different, so the process is continued

$$\begin{aligned}
\alpha^{13} &= \alpha\alpha^{12} = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + 1 \\
\alpha^{14} &= \alpha\alpha^{13} = \alpha(\alpha^3 + \alpha^2 + 1) = \alpha^3 + 1
\end{aligned}$$

and finally

$$\alpha^{15} = \alpha\alpha^{14} = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = 1$$

which is an existing element. Constructing further powers of α will always give existing field elements, for example

$$\begin{aligned}
\alpha^{16} &= \alpha\alpha^{15} = \alpha 1 = \alpha \\
\alpha^{17} &= \alpha\alpha^{16} = \alpha\alpha = \alpha^2.
\end{aligned}$$

The field $GF(2^4)$ therefore has the following 16 elements

$$0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}.$$

Table 6.4 lists the elements along with their polynomial representations in terms of 1, α, α^2, and α^3. Field elements of $GF(2^4)$ can be added together by using the polynomial representation of elements given in Table 6.4 or by referring to an addition table (see Table 6.5a).

Table 6.4
The field elements of $GF(2^4)$

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

Table 6.5(a)
Addition in $GF(2^4)$

+	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
1	0	α^4	α^8	α^{14}	α	α^{10}	α^{13}	α^9	α^2	α^7	α^5	α^{12}	α^{11}	α^6	α^3
α	α^4	0	α^5	α^9	1	α^2	α^{11}	α^{14}	α^{10}	α^3	α^8	α^6	α^{13}	α^{12}	α^7
α^2	α^8	α^5	0	α^6	α^{10}	α	α^3	α^{12}	1	α^{11}	α^4	α^9	α^7	α^{14}	α^{13}
α^3	α^{14}	α^9	α^6	0	α^7	α^{11}	α^2	α^4	α^{13}	α	α^{12}	α^5	α^{10}	α^8	1
α^4	α	1	α^{10}	α^7	0	α^8	α^{12}	α^3	α^5	α^{14}	α^2	α^{13}	α^6	α^{11}	α^9
α^5	α^{10}	α^2	α	α^{11}	α^8	0	α^9	α^{13}	α^4	α^6	1	α^3	α^{14}	α^7	α^{12}
α^6	α^{13}	α^{11}	α^3	α^2	α^{12}	α^9	0	α^{10}	α^{14}	α^5	α^7	α	α^4	1	α^8
α^7	α^9	α^{14}	α^{12}	α^4	α^3	α^{13}	α^{10}	0	α^{11}	1	α^6	α^8	α^2	α^5	α
α^8	α^2	α^{10}	1	α^{13}	α^5	α^4	α^{14}	α^{11}	0	α^{12}	α	α^7	α^9	α^3	α^6
α^9	α^7	α^3	α^{11}	α	α^{14}	α^6	α^5	1	α^{12}	0	α^{13}	α^2	α^8	α^{10}	α^4
α^{10}	α^5	α^8	α^4	α^{12}	α^2	1	α^7	α^6	α	α^{13}	0	α^{14}	α^3	α^9	α^{11}
α^{11}	α^{12}	α^6	α^9	α^5	α^{13}	α^3	α	α^8	α^7	α^2	α^{14}	0	1	α^4	α^{10}
α^{12}	α^{11}	α^{13}	α^7	α^{10}	α^6	α^{14}	α^4	α^2	α^9	α^8	α^3	1	0	α	α^5
α^{13}	α^6	α^{12}	α^{14}	α^8	α^{11}	α^7	1	α^5	α^3	α^{10}	α^9	α^4	α	0	α^2
α^{14}	α^3	α^7	α^{13}	1	α^9	α^{12}	α^8	α	α^6	α^4	α^{11}	α^{10}	α^5	α^2	0

Example 6.5
Find (a) $\alpha^2+\alpha^9$ and (b) $\alpha^7+\alpha^3+\alpha^{11}$ in $GF(2^4)$.

(a) From Table 6.4, $\alpha^9=\alpha^3+\alpha$ and so $\alpha^2+\alpha^9=\alpha^2+\alpha^3+\alpha=\alpha^{11}$.

(b) Again from Table 6.4, $\alpha^7=\alpha^3+\alpha+1$ and $\alpha^{11}=\alpha^3+\alpha^2+\alpha$ and therefore

$$\begin{aligned}\alpha^7+\alpha^3+\alpha^{11} &= \alpha^3+\alpha+1+\alpha^3+\alpha^3+\alpha^2+\alpha \\ &= \alpha^3+\alpha^2+1=\alpha^{13}.\end{aligned}$$

□

When multiplying two field elements together, factors of α^{15} can be taken out and set to unity as $\alpha^{15}=1$. This is equivalent to taking the sum modulo-15 of the exponents. Given two field elements α^i and α^j in $GF(2^4)$ their product is

$$\alpha^i\alpha^j=\alpha^{(i+j)\text{modulo-15}}.$$

Table 6.5(b) show the product of elements in $GF(2^4)$.

Example 6.6
Find (a) $\alpha^2\alpha^9$, (b) $\alpha^{13}\alpha^8$, and (c) $\alpha^7\alpha^{12}\alpha^4$ in $GF(2^4)$.

(a) $\alpha^2\alpha^9=\alpha^{11}$

(b) $\alpha^{13}\alpha^8=\alpha^{21}=\alpha^{15}\alpha^6=1\alpha^6=\alpha^6$

(c) $\alpha^7\alpha^{12}\alpha^4=\alpha^{(7+12+4)\text{modulo-15}}=\alpha^8$.

□

To divide two elements in $GF(2^4)$ the difference modulo-15 in the exponents is required, and so given α^i and α^j, where $\alpha^j\neq 0$, in $GF(2^4)$ then α^i divided by α^j is

$$\frac{\alpha^i}{\alpha^j}=\alpha^{(i-j)\text{modulo-15}}.$$

Table 6.5(b)
Multiplication in $GF(2^4)$

×	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
1	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
α	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1
α^2	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α
α^3	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2
α^4	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3
α^5	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4
α^6	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5
α^7	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6
α^8	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7
α^9	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8
α^{10}	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9
α^{11}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}
α^{12}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}
α^{13}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}
α^{14}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}

Example 6.7
Find (a) α^{13}/α^2, (b) α^3/α^{10}, and (c) α/α^9 in $GF(2^4)$.

(a) $\alpha^{13}/\alpha^2 = \alpha^{(13-2)\text{modulo-}15} = \alpha^{11}$

(b) $\alpha^3/\alpha^{10} = \alpha^{(3-10)\text{modulo-}15} = \alpha^8$

(c) $\alpha/\alpha^9 = \alpha^{(1-9)\text{modulo-}15} = \alpha^7$.

□

Each element α^i in $GF(2^4)$ is its own additive inverse and has a multiplicative inverse given by $\alpha^{-i} = \alpha^{15-i}$. Note that elements that are common to $GF(2^3)$ and $GF(2^4)$ do not have the same inverse. For example in $GF(2^4)$ the inverse of α^2 is $\alpha^{-2} = \alpha^{13}$, whereas the inverse of α^2 in $GF(2^3)$ is $\alpha^{-2} = \alpha^5$.

Returning now to the polynomial $p(x) = x^4 + x + 1$ we have established that one of its roots is α belonging to $GF(2^4)$. We can now proceed to find the other 3 roots by using a trial-and-error method in which each field element α^i of $GF(2^4)$ is tested to see if it gives $p(\alpha^i) = 0$. We have already seen that 0 and 1 are not roots of $p(x)$, and so starting with $x = \alpha^2$ we find that

$$p(\alpha^2) = 0$$
$$p(\alpha^3) = \alpha^5$$
$$p(\alpha^4) = 0.$$

So far then, three of the roots are α, α^2 and α^4, recall that the same three field elements belonging to $GF(2^3)$ are roots of $x^3 + x + 1$. Another root is required and so continuing with the search gives

$$p(\alpha^5) = 1$$
$$p(\alpha^6) = \alpha^{10}$$
$$p(\alpha^7) = \alpha^{10}$$
$$p(\alpha^8) = 0$$

and α^8 is therefore the fourth root. The remaining elements need not be tested as there can be only 4 roots, the reader may wish to verify that taking $x = \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}$, and α^{14} gives $p(x) \neq 0$. The roots of the binary equation $x^4 + x + 1 = 0$ are therefore the elements α, α^2, α^4, and α^8 lying in the field $GF(2^4)$.

We now take a brief look at $GF(2^5)$ generated by

$$p(x) = x^5 + x^2 + 1.$$

Setting $p(x) = 0$ and defining an element α such that $p(\alpha) = 0$ gives

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

which can be used to generate the field $GF(2^5)$ with 32 elements and where $\alpha^{31} = 1$ (see Table 6.6). The other 4 roots of $p(x) = x^5 + x^2 + 1 = 0$ are α^2, α^4, α^8, and α^{16} belonging to $GF(2^5)$.

The fields $GF(2^3)$, $GF(2^4)$, and $GF(2^5)$ are just 3 examples of extension fields that can be constructed from the binary field $GF(2)$. Polynomials of degrees 3, 4, and 5 were used to construct $GF(2^3)$, $GF(2^4)$, and $GF(2^5)$ respectively. To construct the

Table 6.6
The field elements of $GF(2^5)$

0	$\alpha^{15} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$
1	$\alpha^{16} = \alpha^4 + \alpha^3 + \alpha + 1$
α	$\alpha^{17} = \alpha^4 + \alpha + 1$
α^2	$\alpha^{18} = \alpha + 1$
α^3	$\alpha^{19} = \alpha^2 + \alpha$
α^4	$\alpha^{20} = \alpha^3 + \alpha^2$
$\alpha^5 = \alpha^2 + 1$	$\alpha^{21} = \alpha^4 + \alpha^3$
$\alpha^6 = \alpha^3 + \alpha$	$\alpha^{22} = \alpha^4 + \alpha^2 + 1$
$\alpha^7 = \alpha^4 + \alpha^2$	$\alpha^{23} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^8 = \alpha^3 + \alpha^2 + 1$	$\alpha^{24} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
$\alpha^9 = \alpha^4 + \alpha^3 + \alpha$	$\alpha^{25} = \alpha^4 + \alpha^3 + 1$
$\alpha^{10} = \alpha^4 + 1$	$\alpha^{26} = \alpha^4 + \alpha^2 + \alpha + 1$
$\alpha^{11} = \alpha^2 + \alpha + 1$	$\alpha^{27} = \alpha^3 + \alpha + 1$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha$	$\alpha^{28} = \alpha^4 + \alpha^2 + \alpha$
$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2$	$\alpha^{29} = \alpha^3 + 1$
$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha^2 + 1$	$\alpha^{30} = \alpha^4 + \alpha$

field $GF(2^m)$ a polynomial of degree m is required. In the following sections we consider some basic properties of extension fields and field elements, along with the characteristics of polynomials that are relevant to the construction of fields.

6.4 Primitive field elements

The nonzero field elements of the Galois fields are generated by taking successive multiples of a single element α. Field elements that can generate all the nonzero elements of a field are said to be *primitive* and α is primitive in $GF(2^3)$, $GF(2^4)$, and $GF(2^5)$. It can be shown that every Galois field has at least one primitive field element. In $GF(2^3)$ α^2 is primitive as can be easily shown. For convenience arbitrary field elements are represented by β. If we let $\beta = \alpha^2$, then constructing successive powers of β gives

$$\beta = \alpha^2$$
$$\beta^2 = (\alpha^2)^2 = \alpha^4$$
$$\beta^3 = (\alpha^2)^3 = \alpha^6$$
$$\beta^4 = (\alpha^2)^4 = \alpha^8 = \alpha \quad \text{(recall that } \alpha^7 = 1 \text{ in } GF(2^3)\text{)}$$
$$\beta^5 = (\alpha^2)^5 = \alpha^{10} = \alpha^3$$
$$\beta^6 = (\alpha^2)^6 = \alpha^{12} = \alpha^5.$$

So far this has generated six different elements, taking the next power gives

$$\beta^7 = (\alpha^2)^7 = \alpha^{14} = 1$$

and so further multiples of β will produce existing elements

$$\beta^8 = \beta = \alpha^2$$
$$\beta^9 = \beta^2 = \alpha^4$$

and so forth. Hence α^2 can also generate the nonzero elements of $GF(2^3)$ and is therefore a primitive field element of $GF(2^3)$. In fact all the elements (other than 0 and 1) of $GF(2^3)$ are primitive and therefore capable of generating the other nonzero elements.

Example 6.8
Show that α^5 is a primitive element of $GF(2^3)$.

Let $\beta = \alpha^5$ then

$$\beta^2 = \alpha^{10} = \alpha^3$$
$$\beta^3 = \alpha^{15} = \alpha$$
$$\beta^4 = \alpha^{20} = \alpha^6$$
$$\beta^5 = \alpha^{25} = \alpha^4$$
$$\beta^6 = \alpha^{30} = \alpha^2$$
$$\beta^7 = \alpha^{35} = 1.$$

Hence all 7 nonzero elements have been generated and α^5 is therefore primitive in $GF(2^3)$. □

We can likewise show that α^2 is primitive in $GF(2^4)$. However, consider next α^3 in $GF(2^4)$ and let $\beta = \alpha^3$, then

$$\beta = \alpha^3$$
$$\beta^2 = \alpha^6$$
$$\beta^3 = \alpha^9$$
$$\beta^4 = \alpha^{12}.$$

So far this has generated different elements, but the next term gives

$$\beta^5 = \alpha^{15} = 1 \text{(recall that } \alpha^{15} = 1 \text{ in } GF(2^4))$$

and therefore none of the remaining nonzero elements of $GF(2^4)$ can be generated. Continuing to take further powers of β will only generate 1, α^3, α^6, α^9, and α^{12}. For example

$$\beta^6 = \alpha^{18} = \alpha^3$$
$$\beta^7 = \alpha^{21} = \alpha^6$$
$$\beta^8 = \alpha^{24} = \alpha^9$$
$$\beta^9 = \alpha^{27} = \alpha^{12}$$
$$\beta^{10} = \alpha^{30} = 1.$$

Therefore within $GF(2^4)$ the field element α^3 is not primitive. There are other elements within $GF(2^4)$ that are not primitive, for example α^5 can only generate the elements 1 and α^{10}.

Whether or not a field element is primitive can be established by determining the *order* of the element, which for an element β is defined as the smallest positive integer n such that $\beta^n = 1$. This should not be confused with the order of a field, which is the number of elements within the field. In $GF(2^3)$ all the field elements have the same order 7. For example consider α^3 this has an order of 7 because $(\alpha^3)^7 = \alpha^{21} = 1$ and no other smaller power of α^3 gives 1. In $GF(2^4)$ however, not all elements have the same order. For example the order of α^5 is 3, whereas α^2 has an order of 15. The order of an element in $GF(2^m)$ divides $2^m - 1$ and furthermore determines whether or not the element is primitive. In a field $GF(2^m)$ a nonzero field element β is primitive if the order of β is $2^m - 1$. Within $GF(2^3)$ primitive field elements therefore have an order of 7 and primitive elements within $GF(2^4)$ have an order of 15.

Example 6.9

Given that α^{12} and α^7 are field elements of $GF(2^4)$ determine their order, whether or not they are primitive and the field elements generated if they are not primitive.

The smallest power of α^{12} to give unity is 5, as this gives $(\alpha^{12})^5 = \alpha^{60} = 1$. Hence α^{12} is not primitive. The elements generated by α^{12} are $(\alpha^{12})^2 = \alpha^{24} = \alpha^9$, $(\alpha^{12})^3 = \alpha^{36} = \alpha^6$, and $(\alpha^{12})^4 = \alpha^{48} = \alpha^3$. The next power of α^{12} gives $\alpha^{60} = 1$ and therefore α^{12} only generates 1, α^3, α^6, and α^9.

The field element α^7 has order 15 as $(\alpha^7)^{15} = \alpha^{105} = 1$ and no smaller power of α^7 gives unity, it is therefore primitive and generates all the field elements of $GF(2^4)$. □

6.5 Irreducible and primitive polynomials

The polynomials $x^3 + x + 1$, $x^4 + x + 1$, and $x^5 + x^2 + 1$ used to generate $GF(2^3)$, $GF(2^4)$, and $GF(2^5)$ respectively cannot be factorized. Each polynomial is divisible only by itself and 1, such polynomials are referred to as *irreducible polynomials*. An irreducible polynomial having a primitive field element as a root is called a *primitive polynomial*. We have seen that $x^3 + x + 1$, $x^4 + x + 1$ and $x^5 + x^2 + 1$ have the primitive element α as a root and therefore the polynomials used to generate $GF(2^3)$, $GF(2^4)$, and $GF(2^5)$ are primitive.

For any positive integer m there is at least one irreducible polynomial of degree m. It can be shown that an irreducible polynomial of degree m divides $x^r + 1$ where $r = 2^m - 1$, and this can be used to establish whether or not a polynomial is irreducible. Take for example $x^3 + x + 1$, this should divide $x^7 + 1$ for it to be irreducible. Dividing $x^7 + 1$ by $x^3 + x + 1$ gives the quotient $x^4 + x^2 + x + 1$ and zero remainder, and therefore $x^3 + x + 1$ is irreducible. The reader can likewise show that $x^4 + x + 1$ and $x^5 + x^2 + 1$ are irreducible.

It is not always so easy, however, to establish whether or not an irreducible polynomial is primitive. It can be shown that an irreducible polynomial of degree m is primitive if it divides $x^r + 1$ for no r less than $2^m - 1$. Hence the polynomial must divide $x^r + 1$ but not $x^{r-1} + 1$, $x^{r-2} + 1$ and so forth. Consider again $x^3 + x + 1$, we have seen that it divides $x^7 + 1$ which shows that it is irreducible. To further show

that it is primitive we need to show that it does not divide x^6+1, x^5+1 or x^4+1 (there is no need to consider division into x^3+1, x^2+1 or $x+1$ because a polynomial of degree m cannot divide a polynomial of degree $\leq m$). Taking x^6+1 and dividing by x^3+x+1 gives

$$
\begin{array}{r}
x^3+x+1 \\
\hline
x^3+x+1\,\big)\,x^6+1 \\
\underline{x^6+x^4+x^3} \\
-\quad x^4+x^3+1 \\
\underline{x^4+x^2+x} \\
-\quad x^3+x^2+x+1 \\
\underline{x^3+x+1} \\
-\quad x^2
\end{array}
$$

resulting in a nonzero remainder. Likewise x^3+x+1 does not divide x^5+1 or x^4+1 and therefore x^3+x+1 is primitive.

The condition given for determining whether an irreducible polynomial is primitive is of limited use. However, a special case arises if 2^m-1 is prime, for an irreducible polynomial of degree m is primitive if 2^m-1 is prime. Care needs to be exercised here, because this special case means that if 2^m-1 is prime then the irreducible polynomial is primitive, but if 2^m-1 is not prime the polynomial may still be primitive. To illustrate this let's consider the polynomials used to generate $GF(2^3)$ and $GF(2^4)$. The field $GF(2^3)$ was generated using x^3+x+1 which has degree $m=3$, therefore $2^m-1=7$ is prime and so x^3+x+1 is primitive (as we have already seen). The polynomial x^4+x+1 used to generate $GF(2^4)$ has $m=4$ and $2^m-1=15$ which is not prime. However, the roots of the polynomial are α, α^2, α^4, and α^8 which are primitive elements of $GF(2^4)$ and therefore x^4+x+1 is primitive (recall that an irreducible polynomial with a primitive root is primitive).

Primitive polynomials are a special type of irreducible polynomials. With regard to generating a finite field it is the irreducible characteristic of a polynomial that is of importance. In order to generate a finite field it is not necessary for a polynomial to be primitive, it must however be irreducible. Primitive polynomials are preferred because it is easier to generate a field from a primitive polynomial than from one that is not primitive. A primitive polynomial has primitive roots and the field can be generated by taking successive powers of any primitive root. If an irreducible polynomial is not primitive then its roots are not primitive and each root generates only a limited number of field elements. To determine the remaining field elements a primitive element must first be found (recall that every finite field has at least one primitive element). To illustrate this consider the polynomial

$$p(x)=x^4+x^3+x^2+x+1. \tag{5.13}$$

The degree of $p(x)$ is $m=4$ and so for $p(x)$ to be irreducible it must divide $x^{15}+1$, which indeed it does. Hence $p(x)$ is irreducible and can be used to generate a field with 15 nonzero elements. Whether or not the polynomial is primitive cannot be determined from its degree because $2^m-1=15$ is not a prime number. To establish whether or not $p(x)$ is primitive we need to determine if it divides into $x^{14}+1$, $x^{13}+1,\ldots,$ or x^5+1. If $p(x)$ divides into any of these polynomials then it is not

primitive. It can be shown that $p(x)$ divides into x^5+1 and $p(x)$ is therefore not primitive. To construct the field generated by eqn 6.13 we let α be a root of $p(x)$ then $\alpha^4+\alpha^3+\alpha^2+\alpha+1=0$ and so

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

Proceeding as usual to take successive powers of α gives:

$$\begin{aligned}
&\alpha\\
&\alpha^2\\
&\alpha^3\\
&\alpha^4=\alpha^3+\alpha^2+\alpha+1\\
&\alpha^5=\alpha\alpha^4=\alpha(\alpha^3+\alpha^2+\alpha+1)=\alpha^4+\alpha^3+\alpha^2+\alpha=1.
\end{aligned}\tag{6.14}$$

Hence α has order 5 and is therefore not primitive and fails to generate the 15 nonzero elements of the field. To proceed further we need to find a primitive element. None of the elements α^2, α^3, or α^4 are primitive, taking any one of these will only generate the existing elements. Instead we need to consider some other element. If we let $\beta=\alpha+1$ we find that β is primitive with β, β^2, β^3, ..., β^{15} giving the 15 nonzero field elements shown in Table 6.7. We have now constructed two finite fields containing 16 elements, the field generated by $x^4+x^3+x^2+x+1$ (Table 6.7) and that generated by x^4+x+1 (Table 6.4). However the two fields are just different representations of the same field $GF(2^4)$, because two finite fields with the same number of elements differ only in the way that the elements are labelled or ordered. Two finite fields with the same number of elements are said to be *isomorphic*, whilst they may have different representations their mathematical structure is the same.

Table 6.7
$GF(2^4)$ generated by
$p(x)=x^4+x^3+x^2+x+1$

0
$\beta=\alpha+1$
$\beta^2=\alpha^2+1$
$\beta^3=\alpha^3+\alpha^2+\alpha+1$
$\beta^4=\alpha^3+\alpha^2+\alpha$
$\beta^5=\alpha^3+\alpha^2+1$
$\beta^6=\alpha^3$
$\beta^7=\alpha^2+\alpha+1$
$\beta^8=\alpha^3+1$
$\beta^9=\alpha^2$
$\beta^{10}=\alpha^3+\alpha^2$
$\beta^{11}=\alpha^3+\alpha+1$
$\beta^{12}=\alpha$
$\beta^{13}=\alpha^2+\alpha$
$\beta^{14}=\alpha^3+\alpha$
$\beta^{15}=1$

6.6 Minimal polynomials

We have seen that irreducible polynomials and primitive polynomials are used to construct finite fields. Here we consider minimal polynomials, which are used in the construction of binary codes (see Chapter 7).

Complex roots of equations with real coefficients always occur in pairs of complex conjugates. If $p+jq$ is a root of an equation with real coefficients then its complex conjugate $p-jq$ is also a root. The roots of a polynomial with binary coefficients likewise occur in conjugates, not necessarily in pairs but in groups or *sets of conjugates*. Given that β is a field element of $GF(2^m)$ then the conjugates of β are

$$\beta, \beta^2, \beta^4, \beta^8, \ldots, \beta^{2^{r-1}}$$

where r is the smallest integer such that $\beta^{2^r} = \beta$. For example consider the conjugates of α^5 in $GF(2^4)$

$$(\alpha^5)^2 = \alpha^{10}$$
$$(\alpha^5)^4 = \alpha^{20} = \alpha^5$$

therefore in $GF(2^4)$ α^5 has only one conjugate, α^{10}. The conjugates of α^7 in $GF(2^4)$ are

$$(\alpha^7)^2 = \alpha^{14}$$
$$(\alpha^7)^4 = \alpha^{28} = \alpha^{13}$$
$$(\alpha^7)^8 = \alpha^{56} = \alpha^{11}$$
$$(\alpha^7)^{16} = \alpha^{112} = \alpha^7$$

and therefore α^7 has the conjugates α^{11}, α^{13}, and α^{14}.

Example 6.10
Determine the conjugates of α^3 in $GF(2^3)$ and in $GF(2^4)$.

In $GF(2^4)$ we have:

$$(\alpha^3)^2 = \alpha^6$$
$$(\alpha^3)^4 = \alpha^{12}$$
$$(\alpha^3)^8 = \alpha^{24} = \alpha^9$$
$$(\alpha^3)^{16} = \alpha^{48} = \alpha^3$$

and therefore the conjugates of α^3 are α^6, α^9 and α^{12}. Whereas in $GF(2^3)$ the conjugates of α^3 are:

$$(\alpha^3)^2 = \alpha^6$$
$$(\alpha^3)^4 = \alpha^{12} = \alpha^5$$
$$(\alpha^3)^8 = \alpha^{24} = \alpha^3.$$

Note that the set of conjugates of α^3 in $GF(2^3)$ is different from that in $GF(2^4)$. □

Table 6.8
Conjugate elements in $GF(2^4)$ and in $GF(2^3)$

(a) $GF(2^4)$ *Conjugates*	*Order*	(b) $GF(2^3)$ *Conjugates*	*Order*
1	1	1	1
$\alpha, \alpha^2, \alpha^4, \alpha^8$	15	$\alpha, \alpha^2, \alpha^4$	7
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	5	$\alpha^3, \alpha^5, \alpha^6$	7
α^5, α^{10}	3		
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	15		

Table 6.8 shows the sets of conjugate elements in $GF(2^3)$ and $GF(2^4)$ along with the order of elements in the same conjugate set. Note that conjugate elements have the same order and therefore if an element β of $GF(2^m)$ is primitive then its conjugates are also primitive. Recall that the order of an element divides $2^m - 1$ and therefore if $2^m - 1$ is prime the field elements will have order $2^m - 1$ and be primitive. If $2^m - 1$ is not prime, then some elements will be nonprimitive with order less than $2^m - 1$ but there will be at least 1 primitive element. In $GF(2^3)$ $2^3 - 1 = 7$ is prime and therefore the field elements have order 7 and are primitive. $GF(2^4)$ has $2^4 - 1 = 15$ which is not prime and therefore the field has some nonprimitive elements with order less than 15.

One of the properties of conjugates is that they provide a mechanism for going from an extension field to its base field. Consider the pair of complex conjugates $z = p + jq$ and $z^* = p - jq$, their product gives the real number

$$zz^* = p^2 + q^2.$$

Taking the product of the two factors $(x - z)$ and $(x - z^*)$ likewise gives a real expression

$$(x - z)(x - z^*) = x^2 - 2px + p^2 + q^2.$$

In finite fields sets of conjugate elements perform the same function. Consider α^7, belonging to $GF(2^4)$, and its conjugates α^{11}, α^{13}, and α^{14}. Let

$$m(x) = (x + \alpha^7)(x + \alpha^{11})(x + \alpha^{13})(x + \alpha^{14})$$

then

$$\begin{aligned} m(x) &= (x^2 + x(\alpha^7 + \alpha^{11}) + \alpha^{18})(x^2 + x(\alpha^{13} + \alpha^{14}) + \alpha^{27}) \\ &= (x^2 + \alpha^8 x + \alpha^3)(x^2 + \alpha^2 x + \alpha^{12}) \\ &= x^4 + x^3(\alpha^2 + \alpha^8) + x^2(\alpha^{12} + \alpha^{10} + \alpha^3) + x(\alpha^{20} + \alpha^5) + \alpha^{15} \\ &= x^4 + x^3 + 1 \end{aligned}$$

which is a polynomial in the base field $GF(2)$. The polynomial $m(x)$ is referred to as the *minimal polynomial* of α^7, α^{11}, α^{13}, and α^{14}. It is the binary polynomial of smallest degree that has α^7, α^{11}, α^{13}, and α^{14} as roots. Let $m_i(x)$ denote the minimal polynomial of α^i, then $m_i(x)$ is defined to be the smallest degree polynomial in $GF(2)$

that has α^i as a root, and so

$$m_i(\alpha^i) = 0. \tag{6.15}$$

The minimal polynomial $m_i(x)$ is also the minimal polynomial of the conjugates of α and therefore

$$m_7(x) = m_{11}(x) = m_{13}(x) = m_{14}(x) = x^4 + x^3 + 1$$

where $m_7(x)$, $m_{11}(x)$, $m_{13}(x)$, and $m_{14}(x)$ are the minimal polynomials of α^7, α^{11}, α^{13}, and α^{14} respectively.

To determine the minimal polynomial $m(x)$ of an element β, a factor $(x+\beta^*)$ is required for each conjugate β^* of β. This ensures that the conjugate β^* is a root of $m(x)$. The minimal polynomial is then given by the product of all such factors, so that

$$m(x) = (x+\beta)(x+\beta^2)(x+\beta^4)\ldots(x+\beta^{2^{r-1}}) \tag{6.16}$$

where r is the smallest integer such that $\beta^{2^r} = \beta$. In $GF(2^4)$ the conjugates of α are α^2, α^4, α^8 and the minimal polynomial of α is therefore

$$\begin{aligned} m_1(x) &= (x+\alpha)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8) \\ &= (x^2+\alpha^5 x+\alpha^3)(x^2+\alpha^5 x+\alpha^{12}) \\ &= x^4+x+1. \end{aligned}$$

The minimal polynomials of α^2, α^4, and α^8 are all equal to $m_1(x)$

$$m_2(x) = m_4(x) = m_8(x) = m_1(x) = x^4 + x + 1.$$

Table 6.9 gives the minimal polynomials of field elements in $GF(2^3)$ and $GF(2^4)$.

Table 6.9
Minimal polynomials in $GF(2^3)$ and $GF(2^4)$

Field elements	*Minimal polynomials*
(a) $GF(2^3)$	
0	x
1	$x+1$
$\alpha, \alpha^2, \alpha^4$	x^3+x+1
$\alpha^3, \alpha^5, \alpha^6$	x^3+x^2+1
(b) $GF(2^4)$	
0	x
1	$x+1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	x^4+x+1
α^5, α^{10}	x^2+x+1
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$x^4+x^3+x^2+x+1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	x^4+x^3+1

Example 6.11
Find the minimal polynomial of α^5 in $GF(2^3)$.

The conjugates of α^5 are $(\alpha^5)^2 = \alpha^3$ and $(\alpha^5)^4 = \alpha^6$. The minimal polynomial of α^5 is therefore

$$\begin{aligned} m_5(x) &= (x+\alpha^5)(x+\alpha^3)(x+\alpha^6) \\ &= (x^2+\alpha^2 x+\alpha)(x+\alpha^6) \\ &= x^3+x^2(\alpha^6+\alpha^2)+x(\alpha^8+\alpha)+\alpha^7 \\ &= x^3+x^2+1. \end{aligned}$$

This is also the minimal polynomial of α^3 and α^6. □

Consider the field element α^i and its conjugate α^{2i}, conjugate elements have the same minimal polynomial and therefore $m_{2i} = m_i$. Furthermore given that any even integer can be expressed as $2i$ where i is a smaller odd integer, we see therefore that the minimal polynomial of an even power of a field element is always equal to the minimal polynomial of some odd lower power of the field element.

6.7 Solution of equations in $GF(2^4)$ and $GF(2^3)$

We have seen that addition and multiplication of field elements can be carried out in finite fields. The finite fields though are not restricted to just addition and multiplication of field elements, for much of the mathematics that can be performed in the real and complex fields can also be performed in finite fields. Indeed it is often easier to carry out a mathematical operation in a finite field than in the real or complex fields due to the finite number of elements. Here we consider various characteristics of Galois fields, with particular reference to the solution of equations within the fields.

Consider first the linear equation

$$\alpha^3 x + \alpha^{11} = 0$$

defined in $GF(2^4)$. This differs from the equations previously considered in that its coefficients belong to an extension field. In the previous sections the coefficients of equations were real or binary, only the roots of equations were in extension fields. Nevertheless there is no reason why we cannot construct an equation whose coefficients belong to an extension field. We can easily solve the above equation, taking α^{11} over to the right-hand side gives $\alpha^3 x = \alpha^{11}$ and dividing through by α^3 gives $x = \alpha^{11}/\alpha^3 = \alpha^8$.

Every element in the field $GF(2^m)$ has a square root within $GF(2^m)$. Consider α^4 in $GF(2^4)$, its square root is $\sqrt{\alpha^4} = \alpha^2$. Likewise in $GF(2^3)$ the square root of α^4 is α^2. However the square root of α^5 in $GF(2^4)$ is not so obvious. To deal with this we multiply α^5 by α^{15} and then take the square root, so giving

$$\sqrt{\alpha^5} = \sqrt{(\alpha^5\alpha^{15})} = \sqrt{\alpha^{20}} = \alpha^{10}.$$

Note, however, that in $GF(2^3)$ the square root of α^5 is

$$\sqrt{\alpha^5} = \sqrt{(\alpha^5\alpha^7)} = \sqrt{\alpha^{12}} = \alpha^6.$$

Hence the square root of α^5 in $GF(2^3)$ differs from its square root in $GF(2^4)$.

Next consider the roots of the quadratic equation

$$x^2 + \alpha^{12}x + \alpha^9 = 0$$

defined over $GF(2^4)$. Here again we have an equation whose coefficients belong to an extension field. We can factorize the above equation by using the standard approach of establishing two terms whose sum and product give the required coefficients. If β_1 and β_2 are the required roots then

$$(x + \beta_1)(x + \beta_2) = 0$$

and expanding this gives

$$x^2 + x(\beta_1 + \beta_2) + \beta_1\beta_2 = 0$$

and therefore we need to find the field elements β_1 and β_2 that satisfy

$$\beta_1 + \beta_2 = \alpha^{12}$$
$$\beta_1\beta_2 = \alpha^9.$$

Referring to Table 6.5 we see that the field elements α^2 and α^7 meet this requirement, since

$$\alpha^2\alpha^7 = \alpha^9$$
$$\alpha^2 + \alpha^7 = \alpha^{12}$$

and therefore

$$(x + \alpha^2)(x + \alpha^7) = x^2 + \alpha^{12}x + \alpha^9 = 0$$

so giving α^2 and α^7 as the roots. The solution of equations in a finite field can be achieved by a trial-and-error method in which field elements are systematically tested to see if they are roots. Such an approach of searching for roots is referred to as a *Chien search*. For example consider the roots of $p(x) = x^3 + \alpha^9x^2 + \alpha^6x + \alpha^2$ over $GF(2^4)$. Starting with $x = 0$ gives

$$p(0) = \alpha^2$$
$$p(1) = \alpha^4$$
$$p(\alpha) = \alpha^{14}$$
$$p(\alpha^2) = 0$$

and so $x = \alpha^2$ is one of the roots.Continuing with the search shows that the other roots are α^7 and α^8. Note that within an extension field polynomials can exist that do not have roots within the field but lie within some other field. Consider for example

$$p(x) = x^2 + \alpha^2x + \alpha^{10}$$

in $GF(2^4)$. A search fails to find any roots and therefore $p(x)$ is irreducible over $GF(2^4)$.

A useful property of the field $GF(2^m)$ is that the square of a series of terms added together is equal to sum of the individual terms squared. Consider $x_1 + x_2$ squared

$$(x_1 + x_2)^2 = x_1^2 + x_1x_2 + x_2x_1 + x_2^2$$

and because $x_1x_2 + x_2x_1 = 2x_1x_2 = 0$ we see that

$$(x_1 + x_2)^2 = x_1^2 + x_2^2.$$

Squaring this again gives

$$\{(x_1 + x_2)^2\}^2 = \{(x_1^2 + x_2^2)\}^2 = x_1^4 + x_2^4$$

and so

$$(x_1 + x_2)^4 = x_1^4 + x_2^4.$$

This can be extended to all powers 2^i, where i is a positive integer, of $(x_1 + x_2)$ so giving

$$(x_1 + x_2)^{2^i} = x_1^{2^i} + x_2^{2^i}. \tag{6.17}$$

For example in $GF(2^4)$

$$\begin{aligned}(x + \alpha^7)^8 &= x^8 + (\alpha^7)^8 \\ &= x^8 + \alpha^{56} \\ &= x^8 + \alpha^{11}.\end{aligned}$$

Care must be taken not to incorrectly apply eqn 6.17, for instance $(x_1 + x_2)^6 \neq (x_1^6 + x_2^6)$. Equation 6.17 can, though, still be used to expand such an expression

$$\begin{aligned}(x_1 + x_2)^6 &= (x_1 + x_2)^4(x_1 + x_2)^2 \\ &= (x_1^4 + x_2^4)(x_1^2 + x_2^2) \\ &= x_1^6 + x_2^2x_1^4 + x_2^4x_1^2 + x_2^6.\end{aligned}$$

Example 6.12
Expand (a) $(x + \alpha^4)^2$ in $GF(2^3)$ and (b) $(x + \alpha^3)^5 (x + \alpha^{10})$ in $GF(2^4)$.

(a) In $GF(2^3)$ we have $(x + \alpha^4)^2 = x^2 + \alpha^8 = x^2 + \alpha$.

(b) In $GF(2^4)$

$$\begin{aligned}(x + \alpha^3)^5(x + \alpha^{10}) &= (x + \alpha^3)^4(x + \alpha^3)(x + \alpha^{10}) \\ &= (x^4 + \alpha^{12})(x^2 + \alpha^{12}x + \alpha^{13}) \\ &= x^6 + \alpha^{12}x^5 + \alpha^{13}x^4 + \alpha^{12}x^2 + \alpha^9x + \alpha^{10}.\end{aligned}$$ □

Equation 6.17 can be applied to a series of r terms, given $x_1 + x_2 + \cdots + x_r$ in $GF(2^m)$ then

$$(x_1 + x_2 + \cdots + x_r)^{2^i} = x_1^{2^i} + x_2^{2^i} + \cdots + x_r^{2^i} \tag{6.18}$$

where i is a positive integer.

Matrices and determinants of field elements can be constructed and are subject to the same algebraic rules as when constructed with real or complex numbers, obviously though using the additive and multiplicative rules of the finite field within which the field elements exist. Over a field $GF(2^m)$ the matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rn} \end{bmatrix}$$

can be defined where r and n are positive integers, and where a_{ij} are field elements with $i = 1, 2, \dots, r$ and $j = 1, 2, \dots, n$. Consider the 3 by 3 matrix defined in $GF(2^4)$

$$A_1 = \begin{bmatrix} \alpha^2 & \alpha & \alpha^{13} \\ 0 & \alpha^{10} & \alpha \\ \alpha^7 & \alpha^3 & 1 \end{bmatrix}.$$

The determinant of A_1 is

$$\begin{aligned} \det A_1 &= \alpha^2 \begin{vmatrix} \alpha^{10} & \alpha \\ \alpha^3 & 1 \end{vmatrix} + \alpha \begin{vmatrix} 0 & \alpha \\ \alpha^7 & 1 \end{vmatrix} + \alpha^{13} \begin{vmatrix} 0 & \alpha^{10} \\ \alpha^7 & \alpha^3 \end{vmatrix} \\ &= \alpha^2(\alpha^{10} + \alpha^4) + \alpha(0 + \alpha^8) + \alpha^{13}(0 + \alpha^{17}) \\ &= \alpha^2\alpha^2 + \alpha\alpha^8 + \alpha^{13}\alpha^2 = \alpha^4 + \alpha^9 + 1 = \alpha^3. \end{aligned}$$

Note that $\det A_1$ is a field element of $GF(2^4)$. As $\det A_1$ is nonzero we can determine the inverse of A_1. The inverse A^{-1} of a square matrix A is given by $\text{adj } A / \det A$ where $\text{adj } A$ is the adjoint of A and $\det A \neq 0$. The adjoint of a matrix is the transpose of the matrix formed from the cofactors of A and so

$$\text{adj } A = \begin{bmatrix} A_{11} & A_{21} & \dots & A_{r1} \\ A_{12} & A_{22} & \dots & A_{r2} \\ \vdots & & & \vdots \\ A_{1r} & A_{2r} & \dots & A_{rr} \end{bmatrix}$$

where the cofactor A_{ij} is the determinant constructed by excluding the row and column that a_{ij} lies in. A plus or minus sign is normally attached to the cofactor, however as the base field is $GF(2)$ there is no need for this. To find the inverse of A_1 we first determine the cofactors

$$A_{11} = \begin{vmatrix} \alpha^{10} & \alpha \\ \alpha^3 & 1 \end{vmatrix} = \alpha^{10}1 + \alpha\alpha^3 = \alpha^{10} + \alpha^4 = \alpha^2$$

$$A_{21} = \begin{vmatrix} \alpha & \alpha^{13} \\ \alpha^3 & 1 \end{vmatrix} = \alpha 1 + \alpha^{13}\alpha^3 = \alpha + \alpha = 0$$