Finite Field Arithmetic

(Galois field)

Introduction:

A finite field is also often known as a Galois field, after the French mathematician Pierre Galois. A Galois field in which the elements can take q different values is referred to as $GF(\mathrm{q})$. The formal properties of a finite field are:

(a) There are two defined operations, namely addition and multiplication.
(b) The result of adding or multiplying two elements from the field is always an element in the field.
(c) One element of the field is the element zero, such that $a + 0 = a$ for any element a in the field.
(d) One element of the field is unity, such that $a \bullet 1 = a$ for any element a in the field.
(e) For every element a in the field, there is an additive inverse element $-a$, such that $a + (-a) = 0$. This allows the operation of subtraction to be defined as addition of the inverse.
(f) For every non-zero element b in the field there is a multiplicative inverse element b^{-1} such that $\mathrm{b}\,\mathrm{b}^{-1} = 1$. This allows the operation of division to be defined as multiplication by the inverse.
(g) The associative $[a + (b + c) = (a + b) + c, a \bullet (b \bullet c) = [(a \bullet b) \bullet \mathrm{c}]$, commutative $[a + b = b + a, a \bullet b = b \bullet a]$, and distributive $[a \bullet (b + c) = a \bullet b + a \bullet c]$ laws apply.

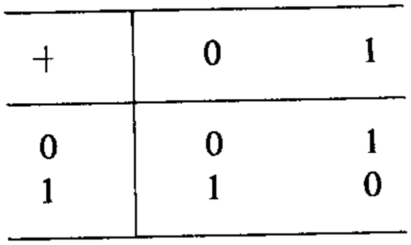
These properties cannot be satisfied for all possible field sizes. They can, however, be satisfied if the field size is any prime number or any integer power of a prime.

2. PRIME SIZE FINITE FIELD *GF(p)*

The rules for a finite field with a prime number *(p)* of elements can be satisfied by carrying out the arithmetic modulo-*p*. If we take any two elements in the range 0 to *p* — 1, and either add or multiply them, we should take the result modulo-p.

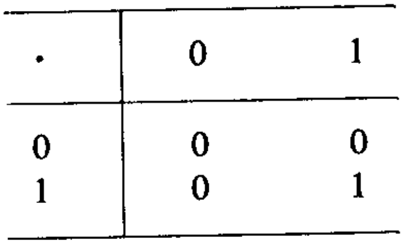
Example 1: Table 1 and 2 shows MODULE-2 addition and multiplication respectively for GF(2) , here p equals 2:-

TABLE 1
MODULO-2 ADDITION



+	0	1
0	0	1
1	1	0

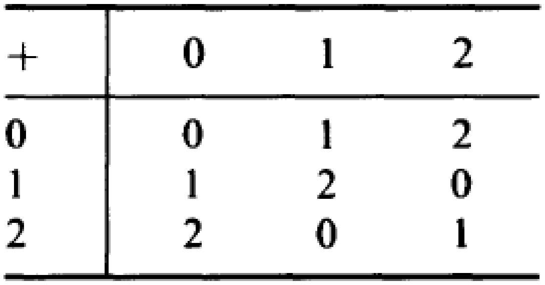
TABLE 2
MODULO-2 MULTIPLICATION



•	0	1
0	0	0
1	0	1

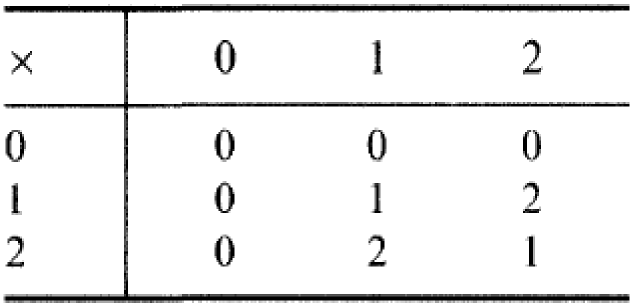
Example 2: The results for GF(3) are shown in Tables 3 and 4 where p here is equal to 3.

TABLE. 3 **Addition in GF(3)**



+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

TABLE.4 Multiplication in GF(3)



×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Thus in GF(3), the additive inverse of 0 is 0, and the additive inverse of 1 is 2 and vice versa. The multiplicative inverse can in principle be found by identifying from the table pairs of elements whose product is 1 . In the case of GF(3), we see that the multiplicative inverse of 1 is 1 and the multiplicative inverse of 2 is 2.

Another approach can be adopted to finding the multiplicative inverse that will be more generally useful and will lead towards the method for constructing other field sizes. In any prime size field, it can be proved that there is always at least one element whose powers constitute all the nonzero elements of the field. This element is said to be primitive. For example, in the field GF(7), the number 3 is primitive as

$$3^0 = 1$$

$$3^1 = 3$$

$$3^2 = 2$$

$$3^3 = 6$$

$$3^4 = 4$$

$$3^5 = 5$$

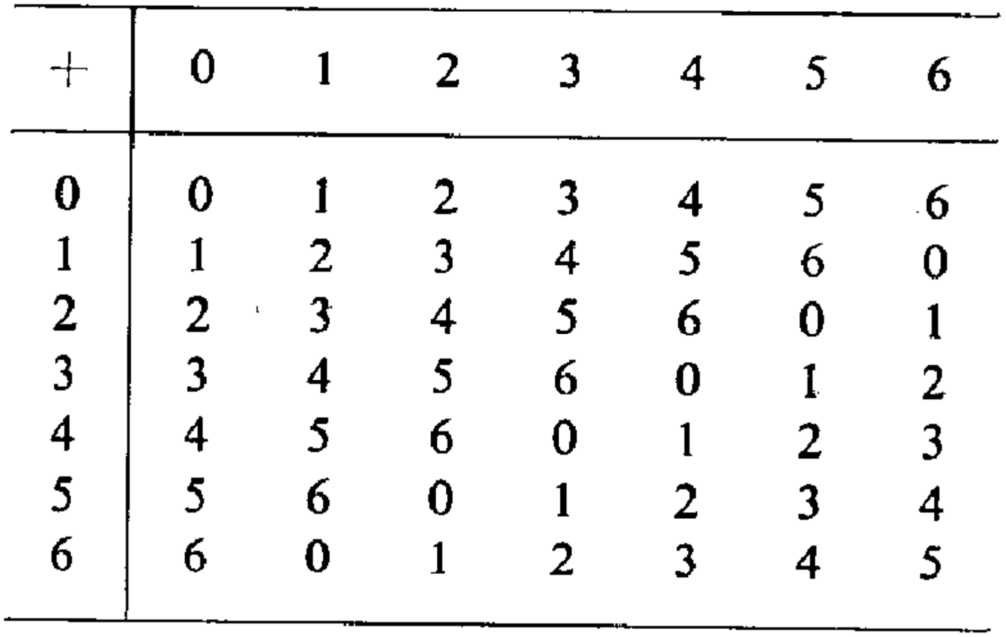
Higher powers of 3 just repeat the pattern as $3^6 = 1$. Note that we can carry out multiplication by adding the powers of

3, thus 6 x 2 = 3^3 x 3^2 = 3^5 = 5. Hence we can find the multiplicative inverse of any element as 3^i as $3^{-i} = 3^{6-i}$. Thus in GF(7) the multiplicative inverse of 6 (33) is 6 (33), the multiplicative inverse of 4 (3^4) is 2 (3^2) and the multiplicative inverse of 5 (3^5) is 3 (3^1).

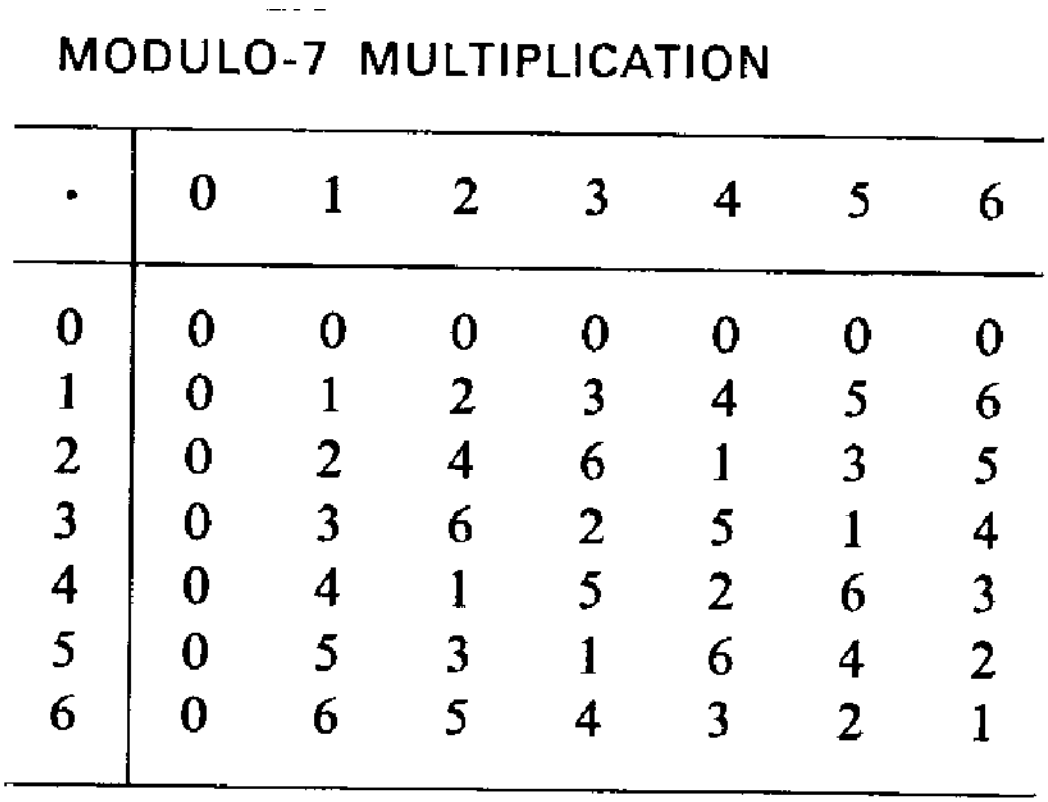
Example 3:- Construct addition and multiplication tables over GF(7), then show how you can make subtraction and division operations over this field?

Sol:- Here p equals to 7 , therefore the elements of this GF are (0,1,2,3,4,5,6). The addition and multiplication over GF(7) will be modulo-7 as shown below:-

MODULO-7 ADDITION



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



MODULO-7 MULTIPLICATION

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

The addition table shown above is used also for subtraction. For example , if we want to subtract 6 from 3 , we first use the addition table to find the additive inverse of 6, which is 1. Then we add 1 to 3 to obtain the result [i.e., 3-6=3+(-6)=3+1=4]. For division, we use the multiplication table. Suppose that we divide 3 by 2. We first find the multiplicative inverse of 2, which is 4, and then we multiply 3 by 4 to obtain the result ,[i.e., $3 \div 2 = 3.(2^{-1}) = 3.4 = 5$].

3. Computations with Polynomials

Next we consider computations with polynomials whose coefficients are from the binary field GF(2). A polynomial f(X) with one *variable X* and with coefficients from GF(2) is of the following form:

$$f(X) = f_0 + f_1 X + f_2 X^2 + \cdots + f_n X^n,$$

$$\text{where } f_i = 0 \text{ or } 1 \text{ for } 0 \leq i \leq n.$$

The *degree* of a polynomial is the largest power of X with a nonzero coefficient. For the polynomial above, if $f_n = l$,$f(X)$ is a polynomial of degree n; if $f_n = 0$, ,$f(X)$ is a polynomial of degree less than n. The degree of $f(X) = f_0$ is zero. In the following we use the phrase "a polynomial over GF(2)" to mean "a polynomial with coefficients from GF(2)."

EXAMPLE 4: There are two polynomials over GF(2) with degree 1: X and $1+X$.

EXAMPLE 5*:* There are four polynomials over GF(2) with degree 2: X^2, $1 + X^2$, $X + X^2$, and $1 + X + X^2$.

In general, there are 2^n polynomials over GF(2) with degree n. Polynomials over GF(2) can be added (or subtracted), multiplied, and divided in the usual way. Let

$$g(X) = g_0 + g_1X + g_2X^2 + \cdots + g_mX^m$$

be another polynomial over GF(2). To add $f(X)$ and $g(X)$, we simply add the coefficients of the same power of X in $f(X)$ and g(X) as follows (assuming that $m \leq n$):

$$f(X) + g(X) = (f_0 + g_0) + (f_1 + g_1)X + \cdots$$
$$+ (f_m + g_m)X^m + f_{m+1}X^{m+1} + \cdots + f_nX^n,$$

EXAMPLE 6: Add $a(X)=1+X+X^3 + X^5$ with $b(X)=1+ X^2+ X^3+ X^4+ X^7$?

Sol:

$$a(X) + b(X) = (1 + 1) + X + X^2 + (1 + 1)X^3 + X^4 + X^5 + X^7$$

$$= X + X^2 + X^4 + X^5 + X^7.$$

Suppose that the degree of *g{X)* is not zero. When *f(X)* is divided *by g(X),* we obtain a unique pair of polynomials over GF(2)—*q(X),* called the quotient, and *r(X),* called the remainder—such that

$$f(X) = q(X)g(X) + r(X)$$

EXAMPLE 7: Divide f*(X)* = 1 + *X* + X^x + X^s + X^6 by g(X)= 1 + X + X^3?

Sol:

$$\begin{array}{r l}
 & X^3 + X^2 \quad \text{(quotient)} \\
\cline{2-2}
X^3 + X + 1 \big) & X^6 + X^5 + X^4 \qquad\qquad + X + 1 \\
 & X^6 \qquad + X^4 + X^3 \\
\cline{2-2}
 & \qquad X^5 \qquad + X^3 \qquad + X + 1 \\
 & \qquad X^5 \qquad + X^3 + X^2 \\
\cline{2-2}
 & \qquad\qquad\qquad X^2 + X + 1 \quad \text{(remainder).}
\end{array}$$

We can easily verify that

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

When *f* (X) is divided by *g(X),* if the remainder *r*(X) is identical to zero *[r(X)* = 0], we say that *f(X)* is divisible by *g(X)* and *g(X)* is a factor of *f(X).*
For real numbers, if a is a *root* of a polynomial *f(X)* [i.e., *f* (a) = 0], *f(X)* is divisible by x — *a.*

EXAMPLE 8: For example, let *f(X)* = 1 + X^2 + X^3 + *X*\
Substituting *X* = 1, we obtain

$$f(1) = 1 + 1^2 + 1^3 + 1^4 = 1 + 1 + 1 + 1 = 0.$$

Thus, *f(X)* has 1 as a root and it should be divisible by *X* + 1.

$$
\begin{array}{r l}
 & X^3 + X + 1 \\
X + 1 & \overline{)\,X^4 + X^3 + X^2 \qquad\quad + 1} \\
 & \underline{X^4 + X^3 \qquad\qquad\qquad\qquad} \\
 & \qquad\qquad\quad X^2 \qquad\quad + 1 \\
 & \qquad\qquad\quad \underline{X^2 + X \qquad\quad} \\
 & \qquad\qquad\qquad\qquad X + 1 \\
 & \qquad\qquad\qquad\qquad \underline{X + 1} \\
 & \qquad\qquad\qquad\qquad\qquad 0
\end{array}
$$

For a polynomial *f*(X) over GF(2), if it has an even number of terms, it is divisible by X+ 1.
A polynomial p*(X)* over GF(2) of degree *m* is said to be *irreducible* over GF(2) if *p(X}* is not devisable by any polynomial over GF(2) of degree less than *m* but greater than zero.

EXAMPLE 9: Among the four polynomials of degree 2 ; X^2, $X^2 + 1$ and $X^2 + X$ are not irreducible since they are either divisible by X or $X + 1$. However, $X^2 + X + 1$ does not have either "0" or "1" as a root and so is not divisible by any polynomial of degree 1.Therefore, $X^2 + X + 1$ is an irreducible polynomial of degree 2.

H.W. Check that if $X^3 + X + 1$ is an irreducible polynomial over GF(2)?

For any $m \geq 1$, there exists an irreducible polynomial of degree m which divides $X^{2^m-1} + 1$

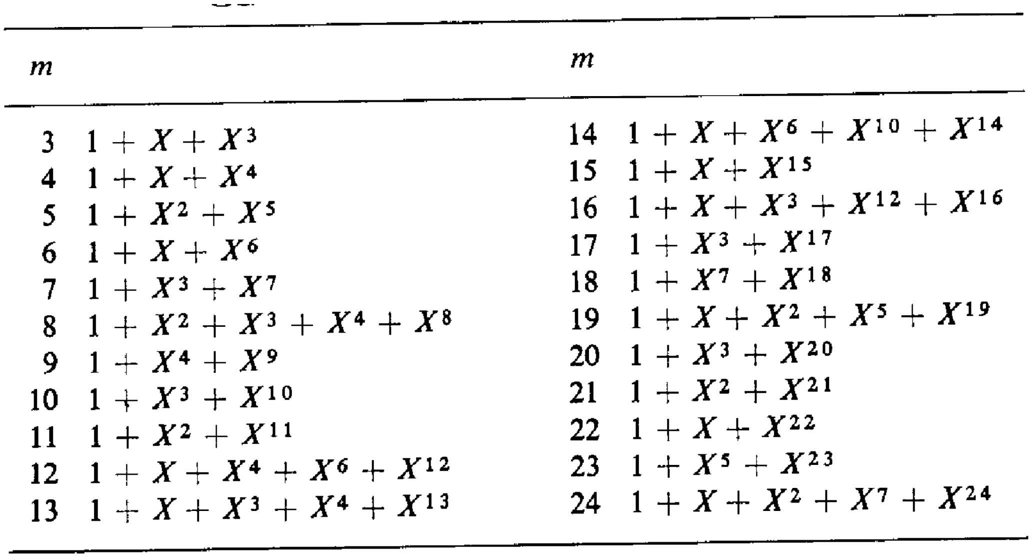
EXAMPLE 10: We can check that $X^3 + X + 1$ divide $X^{2^m-1} + 1 = X^7 + 1$

$$\begin{array}{rl}
 & X^4 + X^2 + X + 1 \\ \cline{2-2}
X^3 + X + 1\big) & X^7 \qquad\qquad\qquad\qquad\qquad\qquad + 1 \\
 & X^7 \qquad + X^5 + X^4 \\ \cline{2-2}
 & \qquad\qquad X^5 + X^4 \qquad\qquad\qquad + 1 \\
 & \qquad\qquad X^5 \qquad + X^3 + X^2 \\ \cline{2-2}
 & \qquad\qquad\qquad X^4 + X^3 + X^2 \qquad + 1 \\
 & \qquad\qquad\qquad X^4 \qquad + X^2 + X \\ \cline{2-2}
 & \qquad\qquad\qquad\qquad X^3 \qquad + X + 1 \\
 & \qquad\qquad\qquad\qquad X^3 \qquad + X + 1 \\ \cline{2-2}
 & \qquad\qquad\qquad\qquad\qquad\qquad\qquad 0.
\end{array}$$

An irreducible polynomial p(X) of degree m is said to be *primitive* if the smallest positive integer n for which $p(X)$ divides $X^n + 1$ is $n = 2^m - 1$.

We may check that $p(X) = X^4 + X + 1$ divides $X^{15} + 1$ but does not divide any $X^n + 1$ for $1 \leq n < 15$. Hence, $X^4 + X + 1$ is a primitive polynomial. The polynomial $X^4 + X^3 + X^2 + X + 1$ is irreducible but it is not primitive, since it divides $X^5 + 1$.

It is not easy to recognize a primitive polynomial. However, there are tables of irreducible polynomials in which primitive polynomials are indicated. For a given *m*, there may be more than one primitive polynomial of degree *m*. A list of primitive polynomials is given in Table below:-



m		*m*	
3	$1 + X + X^3$	14	$1 + X + X^6 + X^{10} + X^{14}$
4	$1 + X + X^4$	15	$1 + X + X^{15}$
5	$1 + X^2 + X^5$	16	$1 + X + X^3 + X^{12} + X^{16}$
6	$1 + X + X^6$	17	$1 + X^3 + X^{17}$
7	$1 + X^3 + X^7$	18	$1 + X^7 + X^{18}$
8	$1 + X^2 + X^3 + X^4 + X^8$	19	$1 + X + X^2 + X^5 + X^{19}$
9	$1 + X^4 + X^9$	20	$1 + X^3 + X^{20}$
10	$1 + X^3 + X^{10}$	21	$1 + X^2 + X^{21}$
11	$1 + X^2 + X^{11}$	22	$1 + X + X^{22}$
12	$1 + X + X^4 + X^6 + X^{12}$	23	$1 + X^5 + X^{23}$
13	$1 + X + X^3 + X^4 + X^{13}$	24	$1 + X + X^2 + X^7 + X^{24}$

4. CONSTRUCTION OF GALOIS FIELD GF(2^m)

In this section we present a method for constructing the Galois field of 2^m elements $(m > 1)$ from the binary field GF(2). We begin with the two elements 0 and I, from GF(2) and a new symbol α. Then we define a multiplication " •" to introduce a sequence of powers of α as follows:

$$
\begin{aligned}
&0 \cdot 0 = 0, \\
&0 \cdot 1 = 1 \cdot 0 = 0, \\
&1 \cdot 1 = 1, \\
&0 \cdot \alpha = \alpha \cdot 0 = 0, \\
&1 \cdot \alpha = \alpha \cdot 1 = \alpha,
\end{aligned}
$$

$$
\begin{aligned}
&\alpha^2 = \alpha \cdot \alpha, \\
&\alpha^3 = \alpha \cdot \alpha \cdot \alpha, \\
&\quad \cdot \\
&\quad \cdot \\
&\quad \cdot \\
&\alpha^j = \alpha \cdot \alpha \cdot \cdots \cdot \alpha \quad (j \text{ times}), \\
&\quad \cdot \\
&\quad \cdot \\
&\quad \cdot
\end{aligned}
$$

It follows from the definition of multiplication above that

$$0 \cdot \alpha^j = \alpha^j \cdot 0 = 0,$$

$$1 \cdot \alpha^j = \alpha^j \cdot 1 = \alpha^j,$$

$$\alpha^i \cdot \alpha^j = \alpha^j \cdot \alpha^i = \alpha^{i+j}.$$

Now, we have the following set of elements on which a multiplication operation "•" is defined:

$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^j, \ldots\}.$$

Let *p(X)* be a primitive polynomial of degree *m* over GF(2). We assume that *p* (α) = 0. Since *p(X)* divides X^{2^m-1} $+1$,we have:-

$$X^{2^m-1} + 1 = q(X)p(X).$$

If we replace *X* by α in above equation, we obtain

$$\alpha^{2^m-1} + 1 = q(\alpha)p(\alpha).$$

Since *p*(α) = 0, we have

$$\alpha^{2^m-1} + 1 = q(\alpha) \cdot 0.$$

If we regard *q*(α) as a polynomial of α over GF(2), it follows that *q*(α)*.0* = 0. As a result, we obtain the following equality:

$$\alpha^{2^m-1}+1=0.$$

Adding 1 to both sides of above equation (use modulo-2 addition) results in the following equality:

$$\alpha^{2^m-1}=1.$$

Therefore, under the condition that $p(\alpha)=0$, the set F becomes finite and contains the following elements:

$$F^*=\{0,1,\alpha,\alpha^2,\ldots,\alpha^{2^m-2}\}.$$

Therefore, the set F^* *(see above equation)* is a Galois field of 2^m elements, GF(2^m). Also GF(2) is a subfield of GF(2^m).

EXAMPLE 11: Let $m = 4$. The polynomial $p(X) = 1 + X + X^*$ is a primitive polynomial over GF(2). Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$. Then $\alpha^4 = 1 + \alpha$. Using this, we can construct GF(2^4). The elements of GF(2^4) are given in Table 5 shown below. The identity $\alpha^4 = 1 + \alpha$ is used repeatedly to form the polynomial representations for the elements of GF(2^4). For example,

$$\alpha^5=\alpha\cdot\alpha^4=\alpha(1+\alpha)=\alpha+\alpha^2,$$

$$\alpha^6=\alpha\cdot\alpha^5=\alpha(\alpha+\alpha^2)=\alpha^2+\alpha^3,$$

$$\alpha^7=\alpha\cdot\alpha^6=\alpha(\alpha^2+\alpha^3)=\alpha^3+\alpha^4=\alpha^3+1+\alpha=1+\alpha+\alpha^3.$$

TABLE 5 THREE REPRESENTATIONS FOR THE ELEMENTS OF GF(2^4) GENERATED BY $p(X) = 1 + X + X^4$

Power representation	Polynomial representation	4-Tuple representation
0	0	(0 0 0 0)
1	1	(1 0 0 0)
α	α	(0 1 0 0)
α^2	α^2	(0 0 1 0)
α^3	α^3	(0 0 0 1)
α^4	$1 + \alpha$	(1 1 0 0)
α^5	$\alpha + \alpha^2$	(0 1 1 0)
α^6	$\alpha^2 + \alpha^3$	(0 0 1 1)
α^7	$1 + \alpha + \alpha^3$	(1 1 0 1)
α^8	$1 + \alpha^2$	(1 0 1 0)
α^9	$\alpha + \alpha^3$	(0 1 0 1)
α^{10}	$1 + \alpha + \alpha^2$	(1 1 1 0)
α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0 1 1 1)
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1 1 1 1)
α^{13}	$1 + \alpha^2 + \alpha^3$	(1 0 1 1)
α^{14}	$1 + \alpha^3$	(1 0 0 1)

To multiply two elements α^i and α^j, we simply add their exponents and use the fact that $\alpha^{15} = 1$. For example, $\alpha^5 \cdot \alpha^7 = \alpha^{12}$ and $\alpha^{12} \cdot \alpha^7 = \alpha^{19} = \alpha^4$. Dividing α^j by α^i, we simply multiply α^j by the multiplicative inverse α^{15-i} of α^i. For example, $\alpha^4/\alpha^{12} = \alpha^4 \cdot \alpha^3 = \alpha^7$ and $\alpha^{12}/\alpha^5 = \alpha^{12} \cdot \alpha^{10} = \alpha^{22} = \alpha^7$. To add α^i and α^j, we use their polynomial representations in Table . Thus,

$$\alpha^5 + \alpha^7 = (\alpha + \alpha^2) + (1 + \alpha + \alpha^3) = 1 + \alpha^2 + \alpha^3 = \alpha^{13}$$

$$1 + \alpha^5 + \alpha^{10} = 1 + (\alpha + \alpha^2) + (1 + \alpha + \alpha^2) = 0.$$

5. BASIC PROPERTIES OF GALOIS FIELD GF(2^m)

In ordinary algebra we often see that a polynomial with real coefficients has roots not from the field of real numbers but from the field of complex numbers that contains the field of real numbers as a subfield.

For example, the polynomial $X^2 + 6X + 25$ does not have roots from the field of real numbers but has two complex conjugate roots, —3 + 4j and —3 — $4j$, where j = $\sqrt{-1}$ •

This is also true for polynomials with coefficients from GF(2). In this case, a polynomial with coefficients from GF(2) may not have roots from GF(2) but has roots from an extension field of GF(2).

EXAMPLE 12:- For example, $X^4 + X^3 + 1$ is irreducible over GF(2) and therefore it does not have roots from GF(2). However, it has four roots from the field GF(2^4). If we substitute the elements of GF(2^4) given by Table 5 into $X^4 + X^3 + 1$, we find that α^7, α^{11}, α^{13}, and α^{14} are the roots of $X^4 + X^3 + 1$. We may verify this as follows:

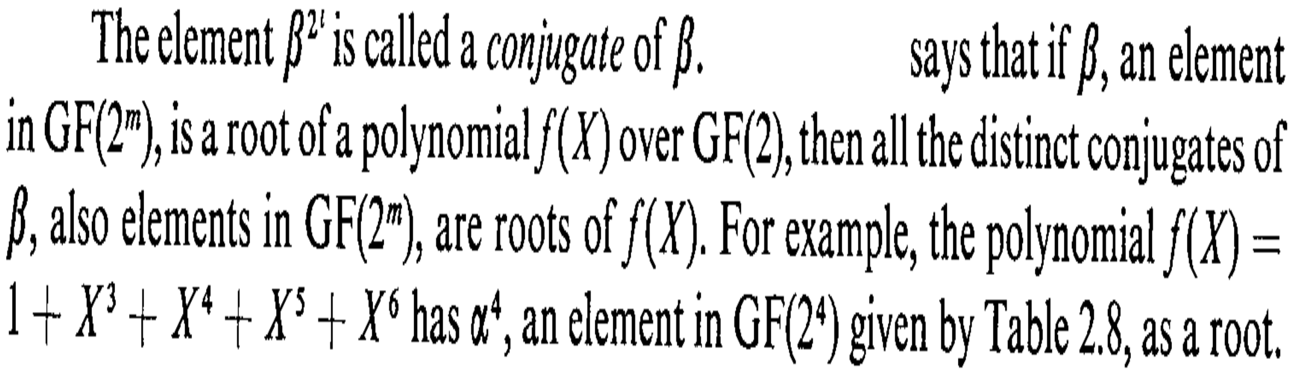
$$(\alpha^7)^4 + (\alpha^7)^3 + 1 = \alpha^{28} + \alpha^{21} + 1 = (1 + \alpha^2 + \alpha^3) + (\alpha^2 + \alpha^3) + 1 = 0.$$

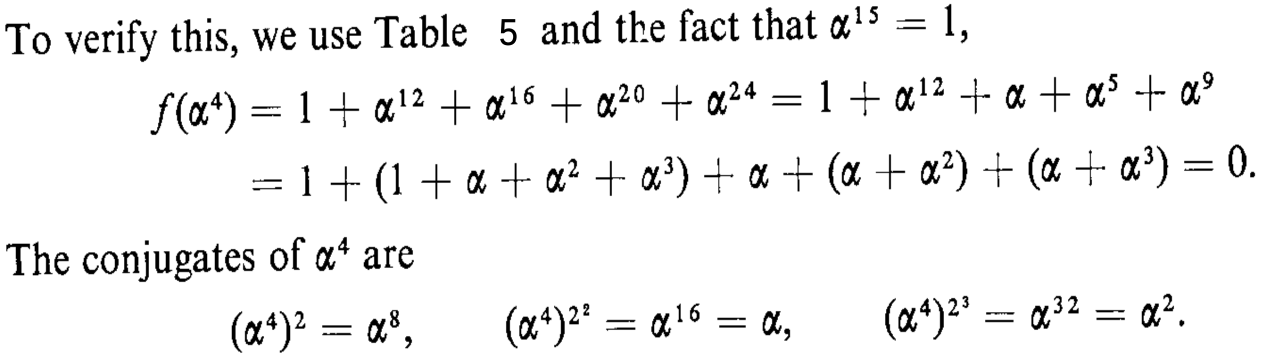
Indeed, α^7 is a root for $X^4 + X^3 + 1$. Similarly, we may verify that α^{11}, α^{13}, and α^{14} are the other three roots. Since $\alpha^7, \alpha^{11}, \alpha^{13}$, and α^{14} are all roots of $X^4 + X^3 + 1$, then $(X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14})$ must be equal to $X^4 + X^3 + 1$. To see this, we multiply out the product above using Table 5

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

Let $f(X)$ be a polynomial with coefficients from GF(2). If β, an element in GF(2^m), is a root of $f(X)$, the polynomial $f(X)$ may have other roots from GF(2^m). Then, what are these roots? This is answered by the following

Let $f(X)$ be a polynomial with coefficients from GF(2). Let β be an element in an extension field of GF(2). If β is a root of $f(X)$, then for any $l \geq 0$, β^{2^l} is also a root of $f(X)$.


The element β^{2^l} is called a *conjugate* of β. says that if β, an element in GF(2^m), is a root of a polynomial $f(X)$ over GF(2), then all the distinct conjugates of β, also elements in GF(2^m), are roots of $f(X)$. For example, the polynomial $f(X) = 1 + X^3 + X^4 + X^5 + X^6$ has α^4, an element in GF(2^4) given by Table 2.8, as a root.


To verify this, we use Table 5 and the fact that $\alpha^{15} = 1$,

$$f(\alpha^4) = 1 + \alpha^{12} + \alpha^{16} + \alpha^{20} + \alpha^{24} = 1 + \alpha^{12} + \alpha + \alpha^5 + \alpha^9$$
$$= 1 + (1 + \alpha + \alpha^2 + \alpha^3) + \alpha + (\alpha + \alpha^2) + (\alpha + \alpha^3) = 0.$$

The conjugates of α^4 are

$$(\alpha^4)^2 = \alpha^8, \qquad (\alpha^4)^{2^2} = \alpha^{16} = \alpha, \qquad (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2.$$

[Note that $(\alpha^4)^{2^4} = \alpha^{64} = \alpha^4$.] It follows l that α^8, α, and α^2 must be also roots of $f(X) = 1 + X^3 + X^4 + X^5 + X^6$. We can check that α^5 and its conjugate α^{10} are roots of $f(X) = 1 + X^3 + X^4 + X^5 + X^6$.

Let β be a nonzero element in the field GF(2^m). It follows from T

that

$$\beta^{2^m-1} = 1.$$

Adding 1 to both sides of $\beta^{2^m-1} = 1$, we obtain

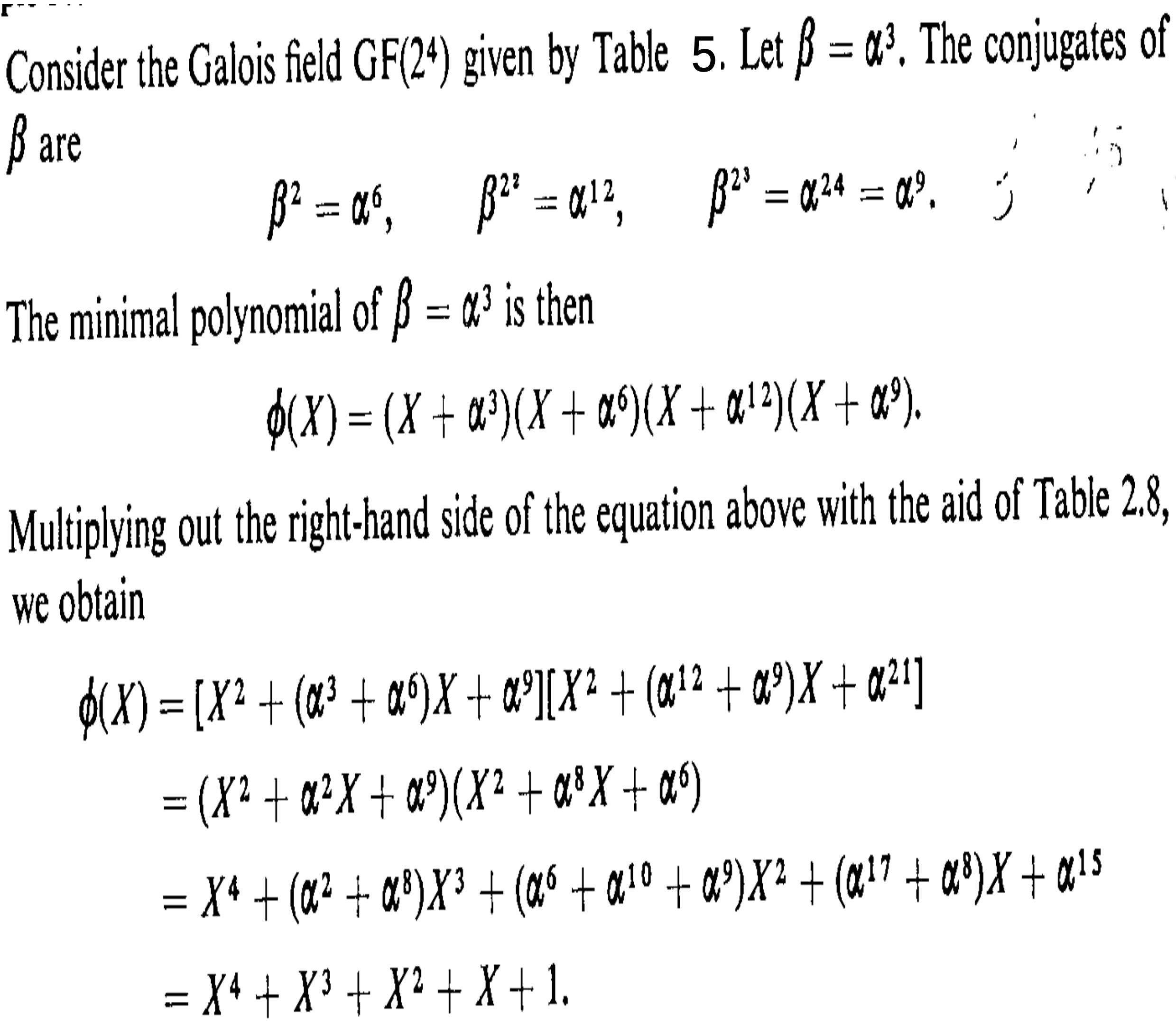
$$\beta^{2^m-1} + 1 = 0.$$

This says that β is a root of the polynomial $X^{2^m-1} + 1$. Hence, every nonzero element of GF(2^m) is a root of $X^{2^m-1} + 1$. Since the degree of $X^{2^m-1} + 1$ is $2^m - 1$, the $2^m - 1$ nonzero elements of GF(2^m) form all the roots of $X^{2^m-1} + 1$.

The minimal polynomial *($\Phi(X)$* of a field element β is irreducible.

Let $f(X)$ be a polynomial over GF(2). Let $\phi(X)$ be the minimal polynomial of a field element β. If β is a root of $f(X)$, then $f(X)$ is divisible by $\phi(X)$.

EXAMPLE 13



Consider the Galois field GF(2^4) given by Table 5. Let $\beta = \alpha^3$. The conjugates of β are

$$\beta^2 = \alpha^6, \qquad \beta^{2^2} = \alpha^{12}, \qquad \beta^{2^3} = \alpha^{24} = \alpha^9.$$

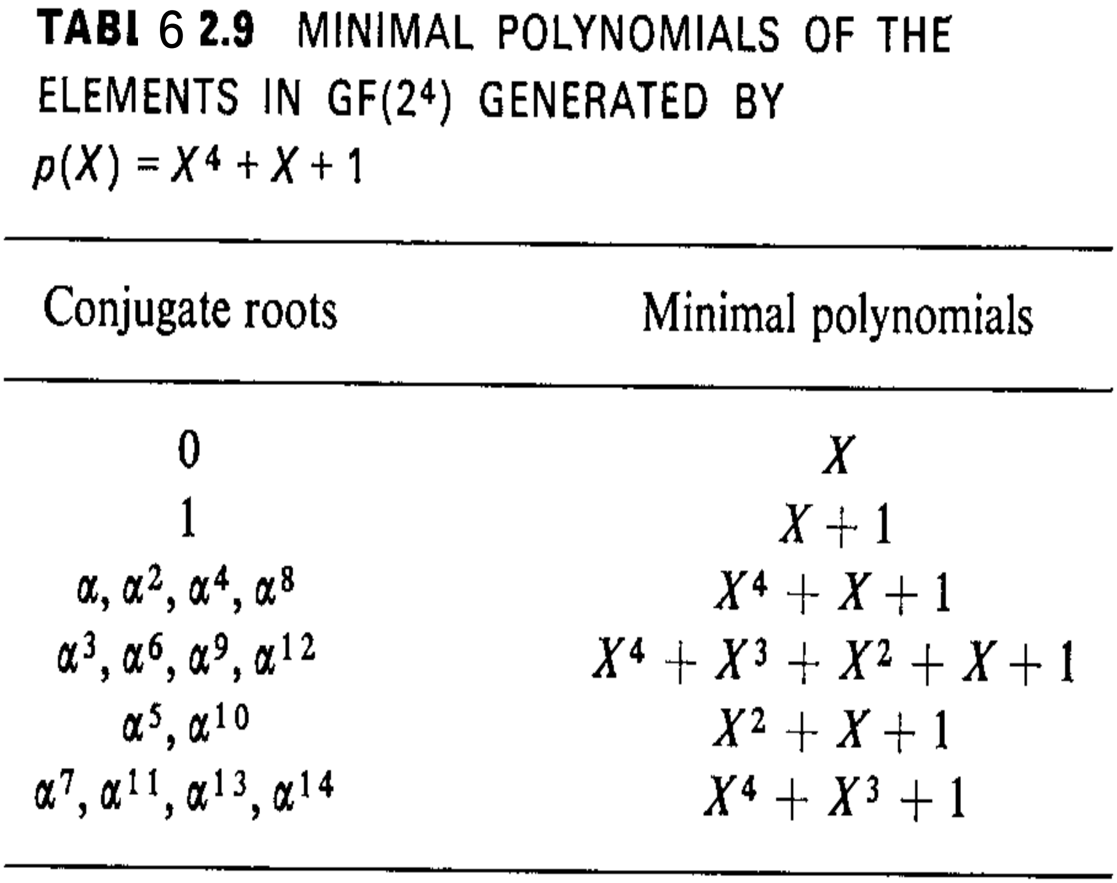
The minimal polynomial of $\beta = \alpha^3$ is then

$$\phi(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9).$$

Multiplying out the right-hand side of the equation above with the aid of Table 2.8, we obtain

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

All the minimal polynomials of the elements in GF(2^4) are given by Table 6.



TABL 6 2.9 MINIMAL POLYNOMIALS OF THE ELEMENTS IN GF(2^4) GENERATED BY $p(X) = X^4 + X + 1$

Conjugate roots	Minimal polynomials
0	X
1	$X + 1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$X^4 + X + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4 + X^3 + X^2 + X + 1$
α^5, α^{10}	$X^2 + X + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$X^4 + X^3 + 1$