Chapter 8

Burst-Correcting Codes

8.1 Introduction

Most of the error-correcting codes that were described in the previous chapter are designed to detect and correct errors that occur independently of each other. In many cases, however, disturbances last long enough to cause several errors in succession, so that this condition of independence is not met. In this chapter we will look at codes that are designed to deal with these cases, that is, codes that are designed to detect and correct *bursts* of errors. We begin by describing some more concepts relating to rings and fields. A more rigorous exposition of these concepts can be found in [1].

8.2 Finite Fields

In the previous chapter, it was stated that the ring $\mathbb{Z}_p$ is a field whenever p is a prime number. If p is a prime number and n is any positive integer, there is a unique (up to isomorphism) field with p^n elements.

DEFINITION 8.1 Galois Field *For any prime number p and positive integer n, the unique field with p^n elements is called the* Galois Field of order *p^n and is denoted by $GF(p^n)$.*

EXAMPLE 8.1

In Chapter 6, we presented the addition and multiplication tables for $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_5$, which are the Galois fields $GF(2)$, $GF(3)$ and $GF(5)$, respectively. The next Galois field is $GF(7)$ or $\mathbb{Z}_7$, whose addition and multiplication tables are shown below.

+	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

×	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

□

EXAMPLE 8.2

Taking $p = 2$ and $n = 2$, we see that there is a Galois field with four elements. Its addition and multiplication tables are:

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$GF(4)$ is not isomorphic to $\mathbb{Z}_4$. □

EXAMPLE 8.3

The next Galois field after $GF(7)$ is $GF(2^3)$, or $GF(8)$. It has eight elements and its addition and multiplication tables are shown below.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	6	4	3	7	2	5
2	2	6	0	7	5	4	1	3
3	3	4	7	0	1	6	5	2
4	4	3	5	1	0	2	7	6
5	5	7	4	6	2	0	3	1
6	6	2	1	5	7	3	0	4
7	7	5	3	2	6	1	4	0

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	3	4	5	6	7	1
3	0	3	4	5	6	7	1	2
4	0	4	5	6	7	1	2	3
5	0	5	6	7	1	2	3	4
6	0	6	7	1	2	3	4	5
7	0	7	1	2	3	4	5	6

□

EXAMPLE 8.4

The next Galois field is $GF(3^2)$, or $GF(9)$. It has nine elements and its addition and multiplication tables are shown below.

$+$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	5	8	4	6	0	3	2	7
2	2	8	6	1	5	7	0	4	3
3	3	4	1	7	2	6	8	0	5
4	4	6	5	2	8	3	7	1	0
5	5	0	7	6	3	1	4	8	2
6	6	3	0	8	7	4	2	5	1
7	7	2	4	0	1	8	5	3	6
8	8	7	3	5	0	2	1	6	4

$\times$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	3	4	5	6	7	8	1
3	0	3	4	5	6	7	8	1	2
4	0	4	5	6	7	8	1	2	3
5	0	5	6	7	8	1	2	3	4
6	0	6	7	8	1	2	3	4	5
7	0	7	8	1	2	3	4	5	6
8	0	8	1	2	3	4	5	6	7

□

In the examples above, we have simply presented addition and multiplication tables and claimed that the structures they define are fields. We will now consider how these tables may be constructed.

In Chapter 7, we constructed rings of polynomials where the multiplication operation was polynomial multiplication modulo the polynomials $(X^n + 1)$. The Galois fields can also be constructed as rings of polynomials where the multiplication operation is multiplication modulo some polynomial. To see which polynomials we can use for this purpose, we need to look at factorization of polynomials.

8.3 Irreducible Polynomials

Polynomials that cannot be factored have different properties from those which can be factored. Whether factorization is possible depends on the ring to which the coefficients of the polynomial belong. For example, the polynomial $(X^2 - 2)$ has no factors if the coefficients belong to the integers, but it can be factored if the coefficients are real numbers, since $(X^2 - 2) = (X + \sqrt{2})(X - \sqrt{2})$.

In the rest of this chapter, $\mathbb{F}$ will stand for a field.

DEFINITION 8.2 Irreducible over $\mathbb{F}$ *A polynomial* $p(X) \in \mathbb{F}[X]$ *of degree* $d \geq 1$ *is* irreducible over $\mathbb{F}$ *or is an* irreducible polynomial in $\mathbb{F}[X]$, *if* $p(X)$ *cannot be expressed as the product* $q(X)r(X)$ *of two polynomials* $q(X)$ *and* $r(X)$ *in* $\mathbb{F}[X]$, *where the degree of both* $q(X)$ *and* $r(X)$ *is greater than or equal to* 1 *but less than* d.

EXAMPLE 8.5

Any first-degree polynomial in $\mathbb{F}[X]$ is irreducible over $\mathbb{F}$. □

EXAMPLE 8.6

$(X^n + 1)$ is never irreducible over $\mathbb{B}[X]$ for any $n \geq 1$.

As we saw in Chapter 7, $(X + 1)$ is always a factor of $(X^n + 1)$ in $\mathbb{B}[X]$, since

$$X^n + 1 = (X + 1)(X^{n-1} + X^{n-2} + \ldots + X^2 + X + 1).$$

□

EXAMPLE 8.7

The only polynomials of degree 1 in $\mathbb{B}[X]$ are X and $(X + 1)$. It is easy to determine whether these polynomials are factors of other polynomials in $\mathbb{B}[X]$. If $p(X) \in \mathbb{B}[X]$ has no constant term, then X is a factor of $p(X)$. If substituting 1 for X in $p(X)$ gives 0, then $(X + 1)$ divides $p(X)$.

Using these tests, we can determine which polynomials of degree 2 and 3 in $\mathbb{B}[X]$ are irreducible over $\mathbb{B}$.

X^2: This has no constant term, so X is a factor; $X^2 = X \times X$.

$(X^2 + 1)$: Substituting 1 for X gives $1 + 1 = 0$, so $(X + 1)$ is a factor; $(X^2 + 1) = (X + 1)(X + 1)$.

$(X^2 + X)$: This has no constant term, and substituting 1 for X gives 0, so both X and $(X + 1)$ are factors; $(X^2 + X) = X(X + 1)$.

$(X^2 + X + 1)$: This has a constant term, and substituting 1 for X gives $1 + 1 + 1 = 1$, so neither of X and $(X + 1)$ is a factor; it is irreducible over $\mathbb{B}$.

X^3: This has no constant term, so X is a factor; $X^3 = X \times X^2$.

$(X^3 + 1)$: Substituting 1 for X gives $1 + 1 = 0$, so $(X + 1)$ is a factor; $(X^3 + 1) = (X + 1)(X^2 + X + 1)$.

$(X^3 + X)$: This has no constant term, $(X^3 + X) = X(X^2 + 1)$.

$(X^3 + X + 1)$: This has a constant term, and substituting 1 for X gives $1 + 1 + 1 = 1$, so neither of X and $(X + 1)$ is a factor. If it had a factor of degree 2, it would also have to have a factor of degree 1, which is impossible. It is irreducible over $\mathbb{B}$.

$(X^3 + X^2)$: This has no constant term, $(X^3 + X^2) = X^2(X + 1)$.

$(X^3 + X^2 + 1)$: This has a constant term, and substituting 1 for X gives $1 + 1 + 1 = 1$, so neither of X and $(X + 1)$ is a factor. It is irreducible over $\mathbb{B}$.

$(X^3 + X^2 + X)$: This has no constant term, $(X^3 + X^2 + X) = X(X^2 + X + 1)$.

(X^3+X^2+X+1): $(X+1)$ is a factor; $(X^3+X^2+X+1) = (X+1)(X^2+1)$.

□

EXAMPLE 8.8

$(X^4+X^2+1) \in \mathbb{B}[X]$ has a constant term and substituting 1 for X gives $1+1+1 = 1$, so neither X or $(X+1)$ is a factor. It is not irreducible over $\mathbb{B}$, however, as

$$(X^4+X^2+1) = (X^2+X+1)(X^2+X+1).$$

□

EXAMPLE 8.9

$(X^4+X+1) \in \mathbb{B}[X]$ has a constant term and substituting 1 for X gives $1+1+1 = 1$, so neither X or $(X+1)$ is a factor. This means that it cannot have a factor that is a third degree polynomial, so the only possible factorizations are of the form

$$(X^4+X+1) = (X^2+aX+1)(X^2+bX+1)$$

for some $a, b \in \mathbb{B}$.

Since

$$(X^2+aX+1)(X^2+bX+1) = (X^4+(a+b)X^3+(1+ab+1)X^+(a+b)X+1),$$

equating coefficients of terms of equal degree gives us the equations

$$\begin{aligned} a+b &= 0 \\ ab &= 0 \\ a+b &= 1. \end{aligned}$$

The first and third of these equations contradict each other; so they have no solution. This shows that (X^4+X+1) is irreducible over $\mathbb{B}$. □

EXAMPLE 8.10

Consider $(X^7+X+1) \in \mathbb{B}[X]$. It has no linear factors, which means that it cannot have factors of degree six. There are two possible factorizations of this polynomial: either

$$(X^7+X+1) = (X^5+a_4X^4+a_3X_3+a_2X^2+a_1X+1)(X^2+b_1X+1)$$

or

$$(X^7+X+1) = (X^4+a_3X^3+a_2X^2+a_1X+1)(X^3+b_2X^2+b_1X+1).$$

Expanding the first factorization and rearranging terms gives

$$a_4 + b_1 = 0, \quad a_3 + a_4 b_1 = 1, \quad a_2 + a_3 b_1 + a_4 = 0,$$

$$a_1 + a_2 b_1 + a_3 = 0, \quad a_1 b_1 + a_2 = 1, \quad a_1 + b_1 = 1.$$

To find a solution of these equations, we can try all possible combinations of values for the coefficients. It is convenient to do this in a table.

a_1	a_2	a_3	a_4	b_1	$a_4 + b_1$	$a_3 + a_4 b_1$	$a_2 + a_3 b_1$	$a_1 + a_2 b_1$	$a_1 b_2 + a_2$	$a_1 + b_1$
							$+a_4$	$+a_3$		
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	1	0	0	0	0	1
0	0	0	1	0	1	0	1	0	0	0
0	0	0	1	1	0	1	1	0	0	1
0	0	1	0	0	0	1	0	1	0	0
0	0	1	0	1	1	1	1	1	0	1
0	0	1	1	0	1	1	1	1	0	0
0	0	1	1	1	0	0	0	1	0	1
0	1	0	0	0	0	0	1	0	1	0
0	1	0	0	1	1	0	1	1	1	1
0	1	0	1	0	1	0	0	0	1	0
0	1	0	1	1	0	1	0	1	1	1
0	1	1	0	0	0	1	1	1	1	0
0	1	1	0	1	1	1	0	0	1	1
0	1	1	1	0	1	1	0	1	1	0
0	1	1	1	1	0	0	1	0	1	1
1	0	0	0	0	0	0	0	1	0	1
1	0	0	0	1	1	0	0	1	1	0
1	0	0	1	0	1	0	1	1	0	1
1	0	0	1	1	0	1	1	1	1	0
1	0	1	0	0	0	1	0	0	0	1
1	0	1	0	1	1	1	1	0	1	0
1	0	1	1	0	1	1	1	0	0	1
1	0	1	1	1	0	0	0	0	1	0
1	1	0	0	0	0	0	1	1	1	1
1	1	0	0	1	1	0	1	0	0	0
1	1	0	1	0	1	0	0	1	1	1
1	1	0	1	1	0	1	0	0	0	0
1	1	1	0	0	0	1	1	0	1	1
1	1	1	0	1	1	1	0	1	0	0
1	1	1	1	0	1	1	0	0	1	1
1	1	1	1	1	0	0	1	1	0	0

The table shows that there is no solution to the equations, and hence there is no factorization of $(X^7 + X + 1)$ into the product of a fifth degree polynomial and a quadratic polynomial.

Expanding the second factorization and rearranging terms gives

$$a_3 + b_2 = 0, \quad a_2 + a_3b_2 + b_1 = 0, \quad a_1 + a_2b_2 + a_3b_1 = 1,$$

$$a_1b_2 + a_2b_1 + a_3 = 1, \quad a_1b_1 + a_2 + b_2 = 0, \quad a_1 + b_1 = 1.$$

a_1	a_2	a_3	b_1	b_2	$a_3 + b_2$	$a_2 + a_3b_2$	$a_1 + a_2b_2$	$a_1b_2 + a_2b_1$	$a_1b_1 + a_2$	$a_1 + b_1$
						$+b_1$	$+a_3b_1$	$+a_3$	$+b_2$	
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	1	0	0	0	0	0
0	0	0	1	0	0	1	0	0	0	1
0	0	0	1	1	1	1	0	0	0	1
0	0	1	0	0	1	0	0	1	0	0
0	0	1	0	1	0	1	0	1	0	0
0	0	1	1	0	1	1	1	1	0	1
0	0	1	1	1	0	1	1	1	0	1
0	1	0	0	0	0	1	0	0	0	0
0	1	0	0	1	1	1	1	0	1	0
0	1	0	1	0	0	0	0	1	0	1
0	1	0	1	1	1	0	1	1	1	1
0	1	1	0	0	1	1	0	1	0	0
0	1	1	0	1	0	0	1	1	1	0
0	1	1	1	0	1	0	1	0	0	1
0	1	1	1	1	0	0	0	0	1	1
1	0	0	0	0	0	0	1	0	0	1
1	0	0	0	1	1	0	1	1	0	1
1	0	0	1	0	0	1	1	0	1	0
1	0	0	1	1	1	1	1	1	1	0
1	0	1	0	0	1	0	1	1	0	1
1	0	1	0	1	0	1	1	0	0	1
1	0	1	1	0	1	1	0	1	1	0
1	0	1	1	1	0	1	0	0	1	0
1	1	0	0	0	0	1	1	0	0	1
1	1	0	0	1	1	1	0	1	1	1
1	1	0	1	0	0	0	1	1	1	0
1	1	0	1	1	1	0	0	0	0	0
1	1	1	0	0	1	1	1	1	0	1
1	1	1	0	1	0	0	0	0	1	1
1	1	1	1	0	1	0	0	0	1	0
1	1	1	1	1	0	0	1	1	0	0

The table above lists all possible values of the coefficients for the second set of equations. Again, there is no solution to the equations, and hence there is no factorization of $(X^7 + X + 1)$ into the product of a fourth degree polynomial and a third degree polynomial.

This exhausts all the possible factorizations, so $(X^7 + X + 1)$ is irreducible over $\mathbb{B}$. We will use this result in examples later. $\square$

EXAMPLE 8.11

The polynomials of degree 1 in $GF(3)[X] = \mathbb{Z}_3[X]$ are X, $(X + 1)$, $(X + 2)$, $2X$, $(2X + 1)$ and $(2X + 2)$. X is a factor of any polynomial without a constant term. If substituting 1 for X in $p(X) \in GF(3)[X]$ gives 0, $(X + 2)$ is a factor of $p(X)$, and if substituting 2 for X in $p(X)$ gives 0, $(X + 1)$ is a factor of $p(X)$. (These conditions arise from the fact that $2 = -1$ in $GF(3)$.)

We can use these conditions to find the irreducible polynomials of degree 2 over $GF(3)$:

X^2: This has no constant term; $X^2 = X \times X$.

$(X^2 + 1)$: This has a constant term so X is not a factor. Substituting 1 for X gives $1 + 1 = 2$, so $X + 2$ is not a factor; substituting 2 for X gives $2^2 + 1 = 1 + 1 = 2$, so $X + 1$ is not a factor. $(X^2 + 1)$ is irreducible over $GF(3)$.

$(X^2 + 2)$: This has a constant term so X is not a factor. Substituting 1 for X gives $1 + 2 = 0$, so $X + 2$ is a factor; substituting 2 for X gives $2^2 + 2 = 1 + 2 = 0$, so $X + 1$ is a factor. $(X^2 + 1) = (X + 1)(X + 2)$.

$(X^2 + X)$: This has no constant term; $(X^2 + X) = X(X + 1)$.

$(X^2 + X + 1)$: This is not irreducible; it is the square of $(X + 2)$.

$(X^2 + X + 2)$: This is irreducible over $GF(3)$.

$(X^2 + 2X)$: This has no constant term; $(X^2 + 2X) = X(X + 2)$.

$(X^2 + 2X + 1)$: This is not irreducible; it is the square of $(X + 1)$.

$(X^2 + 2X + 2)$: This is irreducible over $GF(3)$.

$2X^2$: This has no constant term; $X^2 = 2X \times X$.

$(2X^2 + 1)$: Substituting 1 for X gives $2 + 1 = 0$, so $(X + 2)$ is a factor; $(2X^2 + 1) = (2X + 2)(X + 2)$.

$(2X^2 + 2)$: This is $2(X^2 + 1)$, so it is irreducible over $GF(3)$.

$(2X^2 + X)$: This has no constant term; $(2X^2 + X) = X(2X + 1)$.

$(2X^2 + X + 1)$: This is irreducible over $GF(3)$.

$(2X^2 + X + 2)$: This is not irreducible; it is $2(X + 1)^2$.

$(2X^2 + 2X)$: This has no constant term; $(2X^2 + 2X) = 2X(X + 1)$.

$(2X^2 + 2X + 1)$: This is irreducible over $GF(3)$.

$(2X^2 + 2X + 2)$: This is not irreducible; it is $2(X + 2)^2$.

□

8.4 Construction of Finite Fields

In Chapter 7, we constructed the rings $\mathbb{B}[X]/(X^n + 1)$ and used them to study the cyclic codes. If $\mathbb{F}$ is any field and $p(X)$ is any polynomial in $\mathbb{F}[X]$, we can construct the quotient ring $\mathbb{F}[X]/p(X)$. This ring is a field if and only if $p(X)$ is irreducible over $\mathbb{F}$.

In the case where $\mathbb{F} = \mathbb{Z}_p$ for a prime number p, and the irreducible polynomial is of degree $k > 1$, the resulting field has p^k elements and is isomorphic to the Galois field $GF(p^k)$.

There is always at least one element ρ of $GF(p^k)$ with the property that $\rho^{p^k-1} = 1$ and $\rho^m \neq 1$ for $m < p^k - 1$. These elements have a special name.

DEFINITION 8.3 Primitive Element *ρ is a* primitive element *of the field $\mathbb{F}$ with n elements if $\rho^{n-1} = 1$ and $\rho^m \neq 1$ for all $m < n - 1$.*

The following examples illustrate the construction of Galois fields.

EXAMPLE 8.12

The polynomial $(X^2 + X + 1)$ in $\mathbb{B}[X]$ is irreducible over $\mathbb{B}$. $\mathbb{B}[X]/(X^2 + X + 1)$ is a finite field with $2^2 = 4$ elements, isomorphic to $GF(4)$.

To construct the addition and multiplication tables of the field, we use α to denote the coset of X. Since taking the quotient modulo $(X^2 + X + 1)$ means that the coset of $(X^2 + X + 1)$ is the coset of 0, it follows that $\alpha^2 + \alpha + 1 = 0$ or $\alpha^2 = \alpha + 1$. The other two elements of the field are 0 and 1. This gives us the addition table.

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

Since $\alpha^2 = \alpha + 1$, multiplying by α gives $\alpha^3 = \alpha^2 + \alpha$. Substituting for α^2 gives $\alpha^3 = 1$, which enables us to construct the multiplication table.

$\times$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

To see that this is isomorphic to $GF(4)$ as given in the example above, we use the mapping $0 \leftrightarrow 0$, $1 \leftrightarrow 1$, $\alpha \leftrightarrow 2$, $\alpha^2 \leftrightarrow 3$.

We can use the result $\alpha^2 = \alpha + 1$ to write out the addition and multiplication tables in terms of the elements 0, 1, α, $\alpha + 1$:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

□

EXAMPLE 8.13

$(X^3 + X^2 + 1) \in \mathbb{B}[X]$ is irreducible over $\mathbb{B}$. The quotient $\mathbb{B}[X]/(X^3 + X^2 + 1)$ is a finite field with $2^3 = 8$ elements, isomorphic to $GF(8)$.

As before, we will use α to stand for the coset of X. Then

α^2	is the coset of X^2
α^3	is the coset of $X^2 + 1$
α^4	is the coset of $X^2 + X + 1$
α^5	is the coset of $X + 1$
α^6	is the coset of $X^2 + X$,

where we have used that fact that the coset of $X^3 + X^2 + 1$ is the coset of 0.

These relationships allow us to construct the addition table.

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

Substituting for powers of α, we see that

$$\alpha^7 = \alpha^2\alpha^5 = \alpha^2(\alpha + 1) = \alpha^3 + \alpha^2 = \alpha^2 + 1 + \alpha^2 = 1.$$

This gives us the multiplication table.

$\times$	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

To show that this field is isomorphic to $GF(8)$ in the example above, we use the mapping $0 \leftrightarrow 0$, $1 \leftrightarrow 1$, $\alpha \leftrightarrow 2$, $\alpha^2 \leftrightarrow 3$, $\alpha^3 \leftrightarrow 4$, $\alpha^4 \leftrightarrow 5$, $\alpha^5 \leftrightarrow 6$, $\alpha^6 \leftrightarrow 7$.

It is possible to write out the addition and multiplication tables for this field in terms of the elements $0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1$; see Exercise 6. □

EXAMPLE 8.14

$(X^2 + 1) \in \mathbb{Z}_3[X]$ is irreducible over $\mathbb{Z}_3$. The quotient $\mathbb{Z}_3[X]/(X^2 + 1)$ is a finite field with $3^2 = 9$ elements, isomorphic to $GF(9)$.

To construct the addition and multiplication tables, we will use α to denote the coset of $(X + 1)$. Then:

α^2 is the coset of $2X$
α^3 is the coset of $2X + 1$
α^4 is the coset of 2
α^5 is the coset of $2X + 2$
α^6 is the coset of X
α^7 is the coset of $X + 2$,

where we have used the fact that the coset of (X^2+1) is the coset of 0.

This gives us the addition table.

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
0	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	1	α^4	α^7	α^3	α^5	0	α^2	α	α^6
α	α	α^7	α^5	1	α^4	α^6	0	α^3	α^2
α^2	α^2	α^3	1	α^6	α	α^5	α^7	0	α^4
α^3	α^3	α^5	α^4	α	α^7	α^2	α^6	1	0
α^4	α^4	0	α^6	α^5	α^2	1	α^3	α^7	α
α^5	α^5	α^2	0	α^7	α^6	α^3	α	α^4	1
α^6	α^6	α	α^3	0	1	α^7	α^4	α^2	α^5
α^7	α^6	α^6	α^2	α^4	0	α	1	α^5	α^3

We also have

$$\alpha^8 = \alpha^4 \times \alpha^4 = 2 \times 2 = 1.$$

This gives us the multiplication table.

$\times$	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
0	0	0	0	0	0	0	0	0	α^7
1	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
α	0	α	α^2	α^3	α^4	α^5	α^6	α^7	1
α^2	0	α^2	α^3	α^4	α^5	α^6	α^7	1	α
α^3	0	α^3	α^4	α^5	α^6	α^7	1	α	α^2
α^4	0	α^4	α^5	α^6	α^7	1	α	α^2	α^3
α^5	0	α^5	α^6	α^7	1	α	α^2	α^3	α^4
α^6	0	α^6	α^7	1	α	α^2	α^3	α^4	α^5
α^7	0	α^7	1	α	α^2	α^3	α^4	α^5	α^6

The isomorphism between this field and GF(9) in the example above is given by $0 \leftrightarrow 0$, $1 \leftrightarrow 1$, $\alpha^k \leftrightarrow k+1$, for $k = 1, 2, \ldots, 7$.

It is also possible to write out the addition and multiplication tables of this field in terms of the elements 0, 1, 2, α, $\alpha+1$, $\alpha+2$, 2α, $2\alpha+1$, $2\alpha+2$; see Exercise 8.

□

EXAMPLE 8.15

We have shown that (X^7+X+1) is irreducible over $\mathbb{B}$. We will now use this result to construct the field $GF(2^7) = GF(128)$ with 128 elements.

$GF(128)$ is the quotient $\mathbb{B}[X]/(X^7+X+1)$. If we denote the coset of X by α, the powers of α must satisfy the equation

$$\alpha^7 = \alpha + 1.$$

It follows that

$$\begin{aligned}
\alpha^8 &= \alpha^2 + \alpha, \\
\alpha^9 &= \alpha^3 + \alpha^2, \\
\alpha^{10} &= \alpha^4 + \alpha^3, \\
\alpha^{11} &= \alpha^5 + \alpha^4, \\
\alpha^{12} &= \alpha^6 + \alpha^5, \\
\alpha^{13} &= \alpha^6 + \alpha + 1, \\
\alpha^{14} &= \alpha^2 + 1, \\
\alpha^{15} &= \alpha^3 + \alpha,
\end{aligned}$$

and so on. These equations can be used to construct the addition and multiplication tables of $GF(128)$. As these tables have over one hundred rows and columns, we will not show the entire tables here. We will show only the top left corners of the tables.

We can express the elements of $GF(128)$ as sums of the powers α, α^2, α^3, α^4, α^5 and α^6. If we do this, the corners of the addition and multiplication tables are:

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6	$\ldots$
0	0	1	α	α^2	α^3	α^4	α^5	α^6	$\ldots$
1	1	0	$\alpha+1$	α^2+1	α^3+1	α^4+1	α^5+1	α^6+1	$\ldots$
α	α	$\alpha+1$	0	$\alpha^2+\alpha$	$\alpha^3+\alpha$	$\alpha^4+\alpha$	$\alpha^5+\alpha$	$\alpha^6+\alpha$	$\ldots$
α^2	α^2	α^2+1	$\alpha^2+\alpha$	0	$\alpha^3+\alpha^2$	$\alpha^4+\alpha^2$	$\alpha^5+\alpha^2$	$\alpha^6+\alpha^2$	$\ldots$
α^3	α^3	α^3+1	$\alpha^3+\alpha$	$\alpha^3+\alpha^2$	0	$\alpha^4+\alpha^3$	$\alpha^5+\alpha^3$	$\alpha^6+\alpha^3$	$\ldots$
α^4	α^4	α^4+1	$\alpha^4+\alpha$	$\alpha^4+\alpha^2$	$\alpha^4+\alpha^3$	0	$\alpha^5+\alpha^4$	$\alpha^6+\alpha^4$	$\ldots$
α^5	α^5	α^5+1	$\alpha^5+\alpha$	$\alpha^5+\alpha^2$	$\alpha^5+\alpha^3$	$\alpha^5+\alpha^4$	0	$\alpha^6+\alpha^5$	$\ldots$
α^6	α^6	α^6+1	$\alpha^6+\alpha$	$\alpha^6+\alpha^2$	$\alpha^6+\alpha^3$	$\alpha^6+\alpha^4$	$\alpha^6+\alpha^5$	0	$\ldots$
$\vdots$					$\vdots$				$\ddots$

and

$\times$	0	1	α	α^2	α^3	α^4	α^5	α^6	$\ldots$
0	0	0	0	0	0	0	0	0	$\ldots$
1	0	1	α	α^2	α^3	α^4	α^5	α^6	$\ldots$
α	0	α	α^2	α^3	α^4	α^5	α^6	$\alpha+1$	$\ldots$
α^2	0	α^2	α^3	α^4	α^5	α^6	$\alpha+1$	$\alpha^2+\alpha$	$\ldots$
α^3	0	α^3	α^4	α^5	α^6	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\ldots$
α^4	0	α^4	α^5	α^6	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^4+\alpha^3$	$\ldots$
α^5	0	α^5	α^6	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^4+\alpha^3$	$\alpha^4+\alpha^5$	$\ldots$
α^6	0	α^6	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^4+\alpha^3$	$\alpha^4+\alpha^5$	$\alpha^6+\alpha^5$	$\ldots$
$\vdots$					$\vdots$				$\ddots$

Starting from $\alpha^{15} = \alpha^3 + \alpha$, we can compute $\alpha^{30} = \alpha^6 + \alpha^2$, $\alpha^{60} = \alpha^6 + \alpha^5 + \alpha^4$, $\alpha^{120} = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$, and finally $\alpha^{127} = 1$, showing that α is a primitive element of $GF(128)$. This means we can label the elements of $GF(128)$ by powers of α, so that

$$GF(128) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{126}\}.$$

If we do this the corner of the addition table becomes

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6	$\ldots$
0	0	1	α	α^2	α^3	α^4	α^5	α^6	$\ldots$
1	1	0	α^7	α^{14}	α^{63}	α^{28}	α^{54}	α^{126}	$\ldots$
α	α	α^7	0	α^8	α^{15}	α^{64}	α^{29}	α^{55}	$\ldots$
α^2	α^2	α^{14}	α^8	0	α^9	α^{16}	α^{65}	α^{30}	$\ldots$
α^3	α^3	α^{63}	α^{15}	α^9	0	α^{10}	α^{17}	α^{66}	$\ldots$
α^4	α^4	α^{28}	α^{64}	α^{16}	α^{10}	0	α^{11}	α^{18}	$\ldots$
α^5	α^5	α^{54}	α^{29}	α^{65}	α^{17}	α^{11}	0	α^{12}	$\ldots$
α^6	α^6	α^{126}	α^{55}	α^{30}	α^{66}	α^{18}	α^{12}	0	$\ldots$
$\vdots$					$\vdots$				$\ddots$

and the corner of the multiplication table is

$\times$	0	1	α	α^2	α^3	α^4	α^5	α^6	$\ldots$
0	0	0	0	0	0	0	0	0	$\ldots$
1	0	1	α	α^2	α^3	α^4	α^5	α^6	$\ldots$
α	0	α	α^2	α^3	α^4	α^5	α^6	α^7	$\ldots$
α^2	0	α^2	α^3	α^4	α^5	α^6	α^7	α^8	$\ldots$
α^3	0	α^3	α^4	α^5	α^6	α^7	α^8	α^9	$\ldots$
α^4	0	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	$\ldots$
α^5	0	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	$\ldots$
α^6	0	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	$\ldots$
$\vdots$					$\vdots$				$\ddots$

Finally, we can label the elements of $GF(128)$ with the integers from 0 to 127, using k to represent the $(k-1)$th power of α. When we do this, the corner of the addition table becomes

+	0	1	2	3	4	5	6	7	8	9	...
0	0	1	2	3	4	5	6	7	8	9	...
1	1	0	8	15	64	29	55	127	2	57	...
2	2	8	0	9	16	65	30	56	1	3	...
3	3	15	9	0	10	17	66	31	57	2	...
4	4	64	16	10	0	11	18	67	32	58	...
5	5	29	65	17	11	0	12	19	68	33	...
6	6	55	30	66	18	12	0	13	20	69	...
7	7	127	56	31	67	19	13	0	14	21	...
8	8	2	1	57	32	68	20	14	0	15	...
9	9	57	3	2	58	33	69	21	15	0	...
⋮					⋮					⋱	

and the corner of the multiplication table becomes

×	0	1	2	3	4	5	6	7	8	9	...
0	0	0	0	0	0	0	0	0	0	0	...
1	0	1	2	3	4	5	6	7	8	9	...
2	0	2	3	4	5	6	7	8	9	10	...
3	0	3	4	5	6	7	8	9	10	11	...
4	0	4	5	6	7	8	9	10	11	12	...
5	0	5	6	7	8	9	10	11	12	13	...
6	0	6	7	8	9	10	11	12	13	14	...
7	0	7	8	9	10	11	12	13	14	15	...
8	0	8	9	10	11	12	13	14	15	16	...
9	0	9	10	11	12	13	14	15	16	17	...
⋮					⋮					⋱	

The following table shows the relationships between the three labellings of the elements of $GF(128)$.

0	0	0	1	1	1
2	α^1	α	3	α^2	α^2
4	α^3	α^3	5	α^4	α^4
6	α^5	α^5	7	α^6	α^6
8	α^7	$\alpha + 1$	9	α^8	$\alpha^2 + \alpha$
10	α^9	$\alpha^3 + \alpha^2$	11	α^{10}	$\alpha^4 + \alpha^3$
12	α^{11}	$\alpha^5 + \alpha^4$	13	α^{12}	$\alpha^6 + \alpha^5$
14	α^{13}	$\alpha^6 + \alpha + 1$	15	α^{14}	$\alpha^2 + 1$
16	α^{15}	$\alpha^3 + \alpha$	17	α^{16}	$\alpha^4 + \alpha^2$
18	α^{17}	$\alpha^5 + \alpha^3$	19	α^{18}	$\alpha^6 + \alpha^4$
20	α^{19}	$\alpha^5 + \alpha + 1$	21	α^{20}	$\alpha^6 + \alpha^2 + \alpha$
22	α^{21}	$\alpha^3 + \alpha^2 + \alpha + 1$	23	α^{22}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$
24	α^{23}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	25	α^{24}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3$
26	α^{25}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1$	27	α^{26}	$\alpha^6 + \alpha^5 + \alpha^2 + 1$
28	α^{27}	$\alpha^6 + \alpha^3 + 1$	29	α^{28}	$\alpha^4 + 1$
30	α^{29}	$\alpha^5 + \alpha$	31	α^{30}	$\alpha^6 + \alpha^2$
32	α^{31}	$\alpha^3 + \alpha + 1$	33	α^{32}	$\alpha^4 + \alpha^2 + \alpha$
34	α^{33}	$\alpha^5 + \alpha^3 + \alpha^2$	35	α^{34}	$\alpha^6 + \alpha^4 + \alpha^3$
36	α^{35}	$\alpha^5 + \alpha^4 + \alpha + 1$	37	α^{36}	$\alpha^6 + \alpha^5 + \alpha^2 + \alpha$
38	α^{37}	$\alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1$	39	α^{38}	$\alpha^4 + \alpha^3 + \alpha^2 + 1$
40	α^{39}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha$	41	α^{40}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$
42	α^{41}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1$	43	α^{42}	$\alpha^6 + \alpha^4 + \alpha^2 + 1$
44	α^{43}	$\alpha^5 + \alpha^3 + 1$	45	α^{44}	$\alpha^6 + \alpha^4 + \alpha$
46	α^{45}	$\alpha^5 + \alpha^2 + \alpha + 1$	47	α^{46}	$\alpha^6 + \alpha^3 + \alpha^2 + \alpha$
48	α^{47}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	49	α^{48}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$
50	α^{49}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$	51	α^{50}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$
52	α^{51}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1$	53	α^{52}	$\alpha^6 + \alpha^5 + \alpha^3 + 1$
54	α^{53}	$\alpha^6 + \alpha^4 + 1$	55	α^{54}	$\alpha^5 + 1$
56	α^{55}	$\alpha^6 + \alpha$	57	α^{56}	$\alpha^2 + \alpha + 1$
58	α^{57}	$\alpha^3 + \alpha^2 + \alpha$	59	α^{58}	$\alpha^4 + \alpha^3 + \alpha^2$
60	α^{59}	$\alpha^5 + \alpha^4 + \alpha^3$	61	α^{60}	$\alpha^6 + \alpha^5 + \alpha^4$
62	α^{61}	$\alpha^6 + \alpha^5 + \alpha + 1$	63	α^{62}	$\alpha^6 + \alpha^2 + 1$
64	α^{63}	$\alpha^3 + 1$	65	α^{64}	$\alpha^4 + \alpha$
66	α^{65}	$\alpha^5 + \alpha^2$	67	α^{66}	$\alpha^6 + \alpha^3$
68	α^{67}	$\alpha^4 + \alpha + 1$	69	α^{68}	$\alpha^5 + \alpha^2 + \alpha$
70	α^{69}	$\alpha^6 + \alpha^3 + \alpha^2$	71	α^{70}	$\alpha^4 + \alpha^3 + \alpha + 1$
72	α^{71}	$\alpha^5 + \alpha^4 + \alpha^2 + \alpha$	73	α^{72}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2$
74	α^{73}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1$	75	α^{74}	$\alpha^5 + \alpha^4 + \alpha^2 + 1$
76	α^{75}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha$	77	α^{76}	$\alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1$
78	α^{77}	$\alpha^5 + \alpha^3 + \alpha^2 + 1$	79	α^{78}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha$
80	α^{79}	$\alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$	81	α^{80}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha$
82	α^{81}	$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	83	α^{82}	$\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$
84	α^{83}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$	85	α^{84}	$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1$
86	α^{85}	$\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1$	87	α^{86}	$\alpha^6 + \alpha^4 + \alpha^3 + 1$
88	α^{87}	$\alpha^5 + \alpha^4 + 1$	89	α^{88}	$\alpha^6 + \alpha^5 + \alpha$
90	α^{89}	$\alpha^6 + \alpha^2 + \alpha + 1$	91	α^{90}	$\alpha^3 + \alpha^2 + 1$

92	α^{91}	$\alpha^4+\alpha^3+\alpha$	93	α^{92}	$\alpha^5+\alpha^4+\alpha^2$
94	α^{93}	$\alpha^6+\alpha^5+\alpha^3$	95	α^{94}	$\alpha^6+\alpha^4+\alpha+1$
96	α^{95}	$\alpha^5+\alpha^2+1$	97	α^{96}	$\alpha^6+\alpha^3+\alpha$
98	α^{97}	$\alpha^4+\alpha^2+\alpha+1$	99	α^{98}	$\alpha^5+\alpha^3+\alpha^2+\alpha$
100	α^{99}	$\alpha^6+\alpha^4+\alpha^3+\alpha^2$	101	α^{100}	$\alpha^5+\alpha^4+\alpha^3+\alpha+1$
102	α^{101}	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha$	103	α^{102}	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha+1$
104	α^{103}	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+1$	105	α^{104}	$\alpha^5+\alpha^4+\alpha^3+1$
106	α^{105}	$\alpha^6+\alpha^5+\alpha^4+\alpha$	107	α^{106}	$\alpha^6+\alpha^5+\alpha^2+\alpha+1$
108	α^{107}	$\alpha^6+\alpha^3+\alpha^2+1$	109	α^{108}	$\alpha^4+\alpha^3+1$
110	α^{109}	$\alpha^5+\alpha^4+\alpha$	111	α^{110}	$\alpha^6+\alpha^5+\alpha^2$
112	α^{111}	$\alpha^6+\alpha^3+\alpha+1$	113	α^{112}	$\alpha^4+\alpha^2+1$
114	α^{113}	$\alpha^5+\alpha^3+\alpha$	115	α^{114}	$\alpha^6+\alpha^4+\alpha^2$
116	α^{115}	$\alpha^5+\alpha^3+\alpha+1$	117	α^{116}	$\alpha^6+\alpha^4+\alpha^2+\alpha$
118	α^{117}	$\alpha^5+\alpha^3+\alpha^2+\alpha+1$	119	α^{118}	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha$
120	α^{119}	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	121	α^{120}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha$
122	α^{121}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1$	123	α^{122}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$
124	α^{123}	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+1$	125	α^{124}	$\alpha^6+\alpha^5+\alpha^4+1$
126	α^{125}	$\alpha^6+\alpha^5+1$	127	α^{126}	α^6+1

The labelling that uses sums of powers of α is convenient to use when computations involving addition are involved. The labelling that uses all the powers of α is more convenient for computations involving multiplications.

□

A Galois field that is constructed by taking the quotient $\mathbb{F}[X]/p(X)$ for some irreducible polynomial p also has the structure of a linear space over $\mathbb{F}$. In the examples above, the powers of α are the elements of a basis for the linear space. We will not use these facts, but they are important results in the theory of finite fields.

In the quotient ring $\mathbb{F}[X]/p(X)$, the coset of $p(X)$ is 0. If $p(X)$ is irreducible over $\mathbb{F}$, then $p(a) \neq 0$ for all $a \in \mathbb{F}$. If α denotes the coset of X, then $p(\alpha) = p(X) = 0$. So α is a root of $p(X)$ in $\mathbb{F}[X]/p(X)$, and $p(X)$ is not irreducible over $\mathbb{F}[X]/p(X)$.

DEFINITION 8.4 Order of the Root of a Polynomial *If $p(X) \in \mathbb{F}[X]$ is an irreducible polynomial over $\mathbb{F}$, and α is a root of $p(X)$ in the quotient field $\mathbb{F}[X]/p(X)$, the* order *of α is the least positive integer p for which $\alpha^p = 1$.*

All the roots of $p(X)$ have the same order.

EXAMPLE 8.16

In the construction of $\mathbb{B}[X]/(X^2 + X + 1)$, we used α to denote the coset of X, which became a root of $(X^2 + X + 1)$. Since $\alpha^3 = 1$, α is a root of order 3.

If we consider

$$(\alpha^2)^2 + \alpha^2 + 1 = \alpha^4 + \alpha^2 + 1 = \alpha + \alpha^2 + 1 = 0,$$

we see that α^2 is also a root of $(X^2 + X + 1)$. Since $(\alpha^2)^3 = \alpha^6 = 1$, it is also a root of order 3.

□

EXAMPLE 8.17

In the construction of $\mathbb{B}[X]/(X^3 + X^2 + 1)$, we used α to denote the coset of X, which became a root of $(X^3 + X^2 + 1)$. Since $\alpha^7 = 1$, α is a root of order 7.

α^2 is also a root of $(X^3 + X^2 + 1)$, since

$$\begin{aligned}(\alpha^2)^3 + (\alpha^2)^2 + 1 &= \alpha^6 + \alpha^4 + 1 \\ &= \alpha^2\alpha + \alpha^2\alpha + 1 + 1 \\ &= 0.\end{aligned}$$

Since $(\alpha^2)^7 = (\alpha^7)^2 = 1$, it is also a root of order 7.

The third root of $(X^3 + X^2 + 1)$ is α^4, since

$$\begin{aligned}(\alpha^4)^3 + (\alpha^4)^2 + 1 &= \alpha^{12} + \alpha^8 + 1 \\ &= \alpha^5 + \alpha + 1 \\ &= \alpha + 1 + \alpha + 1 \\ &= 0.\end{aligned}$$

It is also a root of order 7.

□

EXAMPLE 8.18

In the construction of $\mathbb{Z}_3[X]/(X^2 + 1)$, α was used to denote the coset of $(X + 1)$. In this case, α is not a root of $(X^2 + 1)$. Instead, α^2 and α^6 are roots of $(X^2 + 1)$, since

$$(\alpha^2)^2 + 1 = \alpha^4 + 1 = 2 + 1 = 0,$$

and

$$(\alpha^6)^2 + 1 = (\alpha^4)^3 + 1 = 2 + 1 = 0.$$

They are both roots of order 4.

□

8.5 Bursts of Errors

Before we apply the concepts developed above to the design of codes, we will define bursts of errors and state some simple results about them.

DEFINITION 8.5 Burst *A* burst of length d *is a vector whose only non-zero components belong to a set of* d *successive components, of which the first and last are not zero.*

A burst of length d will change a code word into another word whose Hamming distance from the original code word will be between 1 and d. This means that a code that can detect a burst of length d must have a minimum distance greater than d. Roughly speaking, adding a parity check symbol to a code increases the minimum distance of the code by 1. It follows that a linear code of length n can detect all bursts of errors of length d or less if and only if it has d parity-check symbols. Similar arguments show that, in order to correct all bursts of errors of length b or less, the code must have at least $2b$ parity-check symbols, and to correct all bursts of errors of length b or less and simultaneously detect all bursts of length $d \geq b$ or less, it must have at least $b + d$ parity-check symbols.

More detailed analyses of the burst detection and correction capabilities of linear and cyclic codes can be found in [2], Chapters 8 and 9; [3], Section 8.4 and [4], Chapter 10.

The following sections describe types of codes that are designed to correct bursts of errors.

8.6 Fire Codes

Fire codes correct single-burst errors in code vectors.

DEFINITION 8.6 Fire Code *A* Fire code *is a cyclic code with a generator polynomial of the form*

$$g(X) = p(X)(X^c + 1), \tag{8.1}$$

where $p(X)$ is an irreducible polynomial over $\mathbb{B}$ of degree m, whose roots have order r and c is not divisible by r.

The length n of the code words in a Fire Code is the least common multiple of c and r, the number of parity check bits is $c + m$ and the number of information bits is $n - c - m$. The code is capable of correcting a single burst of length b and simultaneously detecting a burst of length $d \geq b$ or less if $b \leq m$ and $b + d \leq c + 1$.

EXAMPLE 8.19

We have seen that $(X^2 + X + 1)$ is irreducible over $\mathbb{B}$ and that the order of its roots is 3. We can use this polynomial to construct a generator polynomial for a Fire code by multiplying it by $(X^4 + 1)$ to give

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

In this case, we have $c = 4$, $m = 2$ and $r = 3$. The code has code words that are twelve bits long, with six information bits and six parity check bits. It can correct bursts up to two bits long.

Its generator matrix is

$$G = \begin{bmatrix} 1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0 \\ 0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1 \end{bmatrix}.$$

□

EXAMPLE 8.20

It is easy to construct Fire codes with long code words. Consider

$$g(X) = (X^7 + X^3 + 1)(X^8 + 1).$$

$(X^7 + X^3 + 1)$ is irreducible over $\mathbb{B}$, and the order of its roots is 127. We therefore have $m = 7, r = 127$ and $c = 8$. The least common multiple of c and r is $8 \times 127 = 1016$. The code has code words that are 1016 bits long, with 15 parity check bits and 1001 information bits. It can correct bursts up to seven bits long. □

8.7 Minimum Polynomials

Let $\mathbb{F}$ be any field. For any $a \in \mathbb{F}$, the polynomial $(X - a)$ has a as a zero. It is irreducible over $\mathbb{F}$.

If $p(X) \in \mathbb{F}[X]$ is irreducible over $\mathbb{F}$, and the degree of $p(X)$ is greater than 1, then $\mathbb{F}[X]/p(X)$ is a field in which the coset of X is a zero of $p(X)$.

There may be many polynomials that have a given zero, some of which are irreducible and some of which are not. Of these, there is one special polynomial that has the smallest degree. To specify it, we need the following definitions.

DEFINITION 8.7 Extension Field *Let $\mathbb{F}$ and $\mathbb{G}$ be two fields. $\mathbb{G}$ is an* extension field *of $\mathbb{F}$ if there exists a ring isomorphism from $\mathbb{F}$ onto a subset of $\mathbb{G}$.*

DEFINITION 8.8 Monic Polynomial *A polynomial of degree $n \geq 1$ in which the coefficient of X^n is 1 is a* monic polynomial

DEFINITION 8.9 Minimum Polynomial *Let $\mathbb{F}$ be a field, and let a belong either to $\mathbb{F}$ or an extension field of $\mathbb{F}$. If $p(X) \in \mathbb{F}[X]$ is an irreducible monic polynomial of which a is a zero, and there is no polynomial of lesser degree of which a is a zero, then $p(X)$ is the* minimum polynomial of a over $\mathbb{F}$.

Note that if $p(X)$ is the minimum polynomial of α over $\mathbb{F}$, then $p(X)$ will be a factor of any other polynomial of which α is a zero.

EXAMPLE 8.21

$GF(4)$ is an extension field of $\mathbb{B}$. If we let $GF(4) = \mathbb{B}[X]/(X^2 + X + 1)$, and let α denote the coset of X, then α is a zero of $(X^2 + X + 1)$, $(X^3 + 1)$, and $(X^5 + X^3 + X^2 + 1)$, and other polynomials. All these polynomials are monic, but only $(X^2 + X + 1)$ is irreducible over $\mathbb{B}$. It is the minimum polynomial of α, and is a factor of $(X^3 + 1)$ and $(X^5 + X^3 + X^2 + 1)$. □

EXAMPLE 8.22

We can construct $GF(25)$ as the quotient $\mathbb{Z}_5[X]/(X^2 + 1)$. If α denotes the coset of X in $GF(25)$, it is a zero of $(X^2 + 1)$. It is also a zero of $(2X^2 + 2)$, $(3X^2 + 3)$, $(4X^2 + 4)$, $(X^3 + X^2 + X + 1)$, $(X^4 + 2X^2 + 1)$, and other polynomials. $(2X^2 + 2)$, $(3X^2 + 3)$ and $(4X^2 + 4)$ are not monic polynomials and $(X^3 + X^2 + X + 1)$ and $(X^4 + 2X^2 + 1)$ are not irreducible over $\mathbb{Z}_5$. $(X^2 + 1)$ is the minimum polynomial of α over $\mathbb{Z}_5$. □

8.8 Bose-Chaudhuri-Hocquenghem Codes

Bose-Chaudhuri-Hocquenghem (BCH) codes are cyclic codes whose generator polynomial has been chosen to make the distance between code words large, and for which effective decoding procedures have been devised. The construction of BCH codes uses roots of unity.

DEFINITION 8.10 nth Root of Unity *Let $\mathbb{F}$ be a field. An* nth root of unity *is a zero of the polynomial $(X^n - 1) \in \mathbb{F}[X]$.*

1 is obviously always an nth root of unity, but in most cases, the roots of unity will not belong to $\mathbb{F}$, but to some extension field of $\mathbb{F}$. For a Galois field $GF(p)$ there will be some m such that the nth roots of unity belong to $GF(p^m)$. In this case, n must divide $p^m - 1$. (This means that n and p cannot have any common factors.)

DEFINITION 8.11 Primitive Root of Unity *Let $GF(p^m)$ be the Galois field that contains the nth roots of unity of $GF(p)$. Let α be one of these roots of unity. If α, α^2, $\alpha^3, \ldots, \alpha^n$ are all distinct roots of unity, then α is called a* primitive root of unity.

EXAMPLE 8.23

The 3rd roots of unity of $\mathbb{B}$ have $n = 3$, $p = 2$. Since $2^2 - 1 = 3$, we have $m = 2$. The roots of unity are the three non-zero elements of $GF(4)$. Since

$$(X^3 + 1) = (X + 1)(X^2 + X + 1),$$

the minimum polynomial of 1 is $(X + 1)$ and the minimum polynomial of the other roots of unity is $(X^2 + X + 1)$. The zeros of $(X^2 + X + 1)$ in $GF(4)$ are primitive roots of unity in $\mathbb{B}$. □

EXAMPLE 8.24

The fifth roots of unity in $GF(3)$ have $n = 5$, $p = 3$. Since $3^4 - 1 = 80$, $m = 4$. The roots belong to $GF(3^4)$. In $GF(3)[X]$, $(X^5 - 1) = (X^5 + 2)$, and

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

so 1 is a fifth root of unity with minimum polynomial $(X + 2)$, and the other four fifth roots of unity have minimum polynomial $(X^4 + X^3 + X^2 + X + 1)$, which is irreducible over $GF(3)$ (see Exercise 5). □

DEFINITION 8.12 Least Common Multiple *The* least common multiple *of a set of polynomials is the polynomial of minimum degree that is divisible by all the polynomials in the set.*

EXAMPLE 8.25

In $\mathbb{B}[X]$, the least common multiple of X and $(X + 1)$ is $(X^2 + X)$.

The least common multiple of $(X + 1)$ and $(X^2 + 1)$ is $(X^2 + 1)$, since $(X + 1)$ divides $(X^2 + 1)$.

The least common multiple of $(X^2 + 1)$ and $(X^3 + 1)$ can be found by finding the factors of these polynomials and multiplying together those that appear in at least one of the polynomials. Since

$$(X^2 + 1) = (X + 1)(X + 1)$$

and

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

their least common multiple is given by

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

□

DEFINITION 8.13 Bose-Chaudhuri-Hocquenghem (BCH) Code *A* Bose-Chaudhuri-Hocquenghem (BCH) code *is a cyclic code of length n whose generator polynomial is the least common multiple of the minimal polynomials of successive powers of a primitive nth root of unity in $\mathbb{B}$.*

From the above, there is some m such that $GF(2^m)$ contains a primitive nth root of unity in $\mathbb{B}$. If b and δ are positive integers, then α^b, $\alpha^{b+1} \ldots \alpha^{b+\delta-2}$ are successive powers of α. Each of these powers will have a minimal polynomial in $\mathbb{B}[X]$. The least common multiple of these minimal polynomials will be the generator polynomial of a cyclic code whose minimum distance will be no less than δ. δ is the *designed distance* of the code.

The most important BCH codes are obtained by taking $b = 1$. It can be shown that for any positive integers m and t, there is a BCH binary code of length $n = 2^m - 1$ which corrects all combinations of t or fewer errors and has no more than mt parity-check bits. In particular, the code will correct bursts of length t or less.

EXAMPLE 8.26

$p(X) = X^3 + X^2 + 1$ is irreducible over $\mathbb{B}$. If we let α be the coset of X in $\mathbb{B}[X]/p(X)$, and take $m = 3$, $b = 1$ and $\delta = 3$, we get a BCH code whose code words are 7 bits long. The generator polynomial of this code is the polynomial in $\mathbb{B}[X]$ of minimal degree whose roots include α and α^2. The polynomial X^3+X^2+1 has this property, since

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

The generator matrix of the code is

$$G = \begin{bmatrix} 1\,0\,1\,1\,0\,0\,0 \\ 0\,1\,0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1 \end{bmatrix}.$$

The code has three information bits and four parity check bits.

□

There are error-correction procedures for BCH codes which identify the locations of errors, in a way similar to the procedure for Hamming codes.

8.9 Other Fields

The error-correcting codes that we have discussed so far have all been binary codes. The code words of these codes are strings consisting of the characters 0 and 1, and no others. The theory that underlies the construction and use of these codes is based on the fact that $\mathbb{Z}_2$, or $\mathbb{B}$, is a finite field. From this fact it follows that $\mathbb{B}^n$ is a linear space over $\mathbb{B}$ and that if $p(X)$ is a polynomial with coefficients in $\mathbb{B}$, $\mathbb{B}[X]/p(X)$ is a ring in general, and a field if $p(X)$ is irreducible over $\mathbb{B}$.

It is possible to develop the theory in exactly the same way for other finite fields, such as $\mathbb{Z}_p$ for prime numbers p or $GF(q)$, and devise error-correcting codes with alphabets other than $\{0, 1\}$. If $\mathbb{F}$ stands for $\mathbb{Z}_p$ or $GF(q)$, then just as in the case of $\mathbb{B}$, $\mathbb{F}^n$ is a linear space over $\mathbb{F}$, and if $p(X)$ is a polynomial with coefficients in $\mathbb{F}$, then $\mathbb{F}[X]/p(X)$ is ring in general and a field if $p(X)$ is irreducible over $\mathbb{F}$.

There are three important differences between the binary case and all the other cases, however. First, when reducing the generator matrix to canonical form, the row operations are performed by replacing a row with the result of multiplying the row by some element of the field, or by multiplying a row by some element of the field and then adding the result to another row. Second, when constructing the parity check matrix from the canonical form of the generator matrix, we use $-A^T$, not A^T. Third, for cyclic codes, we considered the rings $\mathbb{B}[X]/(X^n + 1)$, but in all other cases, the cyclic codes are derived from operations in the ring $\mathbb{F}[X]/(X^n - 1)$.

The following examples construct linear and cyclic codes based on various fields.

EXAMPLE 8.27

Consider $\mathbb{Z}_3$, the finite field with elements 0, 1 and 2. Let us construct a linear code with code words that are four ternary digits long, that is, code words that are members of $\mathbb{Z}_3^4$. For a linear code of dimension 2, we choose two basis elements, say 1001 and 0202. The code consists of 3^2 code words, obtained by multiplying the basis elements by 0, 1 and 2 and adding the results. This gives the subspace $\{0000, 1001, 2002, 0101, 0202, 1102, 2100, 1200, 2201\}$. The generator matrix is

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 2 \end{bmatrix}.$$

To reduce it to canonical form, we multiply the second row by 2 to get

$$G_c = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix},$$

and the canonical form of the parity check matrix is

$$H_c = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{bmatrix}.$$

As we did not permute the columns of G to find G_c, H_c is also the parity check matrix of G.

□

EXAMPLE 8.28

$GF(4)$ is the finite field with the elements $0, 1, 2$ and 3, in which $1+1=0, 2+2=0$ and $3+3=0$. We will construct a linear code of length 4 and dimension 3. The basis elements are 1001, 0102 and 0013 and there are $4^3 = 64$ code words in the code. The generator matrix is

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{bmatrix}.$$

This is in canonical form, so the parity check matrix is

$$H = \begin{bmatrix} 1 & 2 & 3 & 1 \end{bmatrix},$$

where we have used the fact that $-a = a$ in GF(4).

Using the parity check matrix, we see that 1110 belongs to the code, since $1110H^T = 0$, while 1213 does not belong to the code, as $1213H^T = 2$. □

EXAMPLE 8.29

To construct a cyclic code of length 3 using the finite field $\mathbb{Z}_5$, we have to use polynomials in the ring $\mathbb{Z}_5[X]/(X^3 - 1)$.

The generator polynomial will be $(X - 1)$. This must divide $(X^3 - 1)$, and in fact,

$$(X^3 - 1) = (X - 1)(X^2 + X + 1).$$

The generator matrix is

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

or,

$$G = \begin{bmatrix} 4 & 1 & 0 \\ 0 & 4 & 1 \end{bmatrix},$$

since $-1 = 4$ in $\mathbb{Z}_5$.

The canonical form of G is

$$G_c = \begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 4 \end{bmatrix},$$

after permuting the columns of G.

The canonical form of the parity check matrix is

$$H_c = \begin{bmatrix} -4 & -4 & 1 \end{bmatrix},$$

or

$$H_c = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}.$$

H_c is also the parity check matrix of G.

□

EXAMPLE 8.30

The *ternary Golay code* is the only known perfect code on a field other than $\mathbb{B}$. It has code words in $\mathbb{Z}_3[X]/(X^{11} - 1)$, which are 11 ternary digits long with 6 information digits and 5 check digits.

The code can be generated by either of the polynomials

$$g_1(X) = X^5 + X^4 - X^3 + X^2 - 1 = X^5 + X^4 + 2X^3 + X^2 + 2,$$

whose generator matrix is

$$G_1 = \begin{bmatrix} 2&0&1&2&1&1&0&0&0&0&0 \\ 0&2&0&1&2&1&1&0&0&0&0 \\ 0&0&2&0&1&2&1&1&0&0&0 \\ 0&0&0&2&0&1&2&1&1&0&0 \\ 0&0&0&0&2&0&1&2&1&1&0 \\ 0&0&0&0&0&2&0&1&2&1&1 \end{bmatrix},$$

or

$$g_2(X) = X^5 - X^3 + X^2 - X - 1 = X^5 + 2X^3 + X^2 + 2X + 2,$$

whose generator matrix is

$$G_2 = \begin{bmatrix} 2&2&1&2&0&1&0&0&0&0&0 \\ 0&2&2&1&2&0&1&0&0&0&0 \\ 0&0&2&2&1&2&0&1&0&0&0 \\ 0&0&0&2&2&1&2&0&1&0&0 \\ 0&0&0&0&2&2&1&2&0&1&0 \\ 0&0&0&0&0&2&2&1&2&0&1 \end{bmatrix}.$$

$\Box$

These codes can be decoded using syndromes.

8.10 Reed-Solomon Codes

DEFINITION 8.14 Reed-Solomon Code *A* Reed-Solomon code *is a BCH code with parameters $m = 1$ and $b = 1$.*

Reed-Solomon codes are an important subclass of BCH codes. They are constructed in the following manner. Let $\mathbb{F}$ be a finite field, and let n be the order of $\alpha \in \mathbb{F}$, that is, $\alpha^n = 1$. The polynomial

$$g(X) = (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{d-1}) \tag{8.2}$$

is the generator polynomial of a code whose words have n digits, $(d-1)$ parity check digits and minimum distance d.

EXAMPLE 8.31

In $\mathbb{Z}_7$ the powers of 3 are 3, 2, 6, 4, 5, 1, so $n = 6$. If we take $d = 4$, we get

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

This gives us a code whose generator matrix is

$$G = \begin{bmatrix} 6 & 1 & 3 & 1 & 0 & 0 \\ 0 & 6 & 1 & 3 & 1 & 0 \\ 0 & 0 & 6 & 1 & 3 & 1 \end{bmatrix}.$$

□

If the number of elements in $\mathbb{F}$ is a power of two, we can construct a binary code from the Reed-Solomon code by renaming the elements, as shown in the following example.

EXAMPLE 8.32

In $\mathbb{B}[X]/(X^3 + X^2 + 1)$, if α denotes the coset of X, $\alpha^7 = 1$. If we take $d = 4$, our generator polynomial is

$$g(X) = (X + \alpha)(X + \alpha^2)(X + \alpha^3) = X^3 + \alpha^5 X^2 + X + \alpha^6.$$

If we rename the elements of $\mathbb{B}[X]/(X^3 + X^2 + 1)$ with the digits 0, 1, 2, 3, 4, 5, 6, 7, the generator polynomial is

$$g(X) = X^3 + 6X^2 + X + 7,$$

and we have a generator matrix

$$G = \begin{bmatrix} 7 & 1 & 6 & 1 & 0 & 0 & 0 \\ 0 & 7 & 1 & 6 & 1 & 0 & 0 \\ 0 & 0 & 7 & 1 & 6 & 1 & 0 \\ 0 & 0 & 0 & 7 & 1 & 6 & 1 \end{bmatrix}$$

for a code on $\{0, 1, \ldots, 7\}$.

If we express the digits in the generator matrix in binary notation, we get the generator matrix for a binary code with code words that are 21 bits long:

$$G = \begin{bmatrix} 111 & 001 & 110 & 001 & 000 & 000 & 000 \\ 000 & 111 & 001 & 110 & 001 & 000 & 000 \\ 000 & 000 & 111 & 001 & 110 & 001 & 000 \\ 000 & 000 & 000 & 111 & 001 & 110 & 001 \end{bmatrix}.$$

Note that if G is used to generate code words, the operations of $\mathbb{B}[X]/(X^3 + X^2 + 1)$, with the elements suitably renamed, must be used in the computations. □

This procedure can be used generally to produce binary Reed-Solomon codes with code words that are $m(2^m - 1)$ bits long with $m(2^m - 1 - 2t)$ information bits. They are capable of correcting errors occurring in up to t $m-$bit blocks.

EXAMPLE 8.33

In previous examples, we have shown that $(X^7+X+1) \in \mathbb{B}[X]$ is irreducible over $\mathbb{B}$ and used this to study the structure of $GF(128) = GF(2^7) = \mathbb{B}[X]/(X^7+X+1)$. If α denotes the coset of X in $GF(128)$, then $\alpha^{127} = 1$, and we can use the polynomial

$$g(X) = (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)$$

as the generator polynomial of a Reed-Solomon code.

If we expand $g(X)$ and simplify the result, we get

$$\begin{aligned} g(X) = X^4 + (\alpha^4+\alpha^3+\alpha^2+\alpha)X^3 + (\alpha^6+\alpha^4+\alpha^3+\alpha+1)X^2 \\ +(\alpha^6+\alpha^3+1)X + (\alpha^4+\alpha^3). \end{aligned}$$

Labelling the elements of $GF(128)$ with the integers $0, 1, \ldots, 127$, we can write this as

$$g(X) = X^4 + 23X^3 + 74X^2 + 28X + 11.$$

The generator matrix for the code has 123 rows and 127 columns:

$$G = \begin{bmatrix} 11 & 28 & 74 & 23 & 1 & 0 & 0 \ldots 0 \\ 0 & 11 & 28 & 74 & 23 & 1 & 0 \ldots 0 \\ \vdots & & & & \vdots & & \ddots \ \vdots \\ 0 & 0 \ldots & 0 & 11 & 28 & 74 & 23 \ 1 \end{bmatrix}.$$

We can construct binary code words that are 889 bits long by replacing the integer labels with their decimal equivalents. If we do this, the code word corresponding to the generator polynomial is

$$0001011\ 0011100\ 1001010\ 0010111\ 0000001\ 0000000 \ldots 0000000,$$

where the spaces have been introduced for clarity. The code words have 861 information bits and are capable of correcting burst errors in up to two seven-bit blocks.

□

8.11 Exercises

1. The first five Galois fields are $GF(2)$, $GF(3)$, $GF(4)$, $GF(5)$ and $GF(7)$. What are the next ten Galois fields?
2. Find the factors of $(X^5 + X + 1)$ in $\mathbb{B}[X]$.

3. Show that $(X^5 + X^2 + 1)$ is irreducible over $\mathbb{B}$.

4. Is $(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$ irreducible over $\mathbb{B}$?

5. Show that $(X^4 + X^3 + X^2 + X + 1)$ is irreducible over $GF(3)$.

6. Write out the addition and multiplication tables of the field

$$GF(8) = \mathbb{B}[X]/(X^3 + X^2 + 1)$$

in terms of the elements $0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1$.

7. Write out the addition and multiplication tables of the field

$$\mathbb{B}[X]/(X^3 + X + 1)$$

and show that it is isomorphic to $GF(8)$.

8. Write out the addition and multiplication tables of the field

$$GF(9) = \mathbb{Z}_3[X]/(X^2 + 1)$$

in terms of the elements $0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2$.

9. Show that $(X^2 + X + 1)$ is irreducible over $\mathbb{Z}_5$. Construct the Galois Field $GF(25) = \mathbb{Z}_5[X]/(X^2 + X + 1)$. Let α denote the coset of $X + 2$ in $GF(25)$. Draw up the addition and multiplication tables in terms of:

   (a) the elements $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{23}\}$;

   (b) terms of the form $(i\alpha + j)$, for $i, j \in \mathbb{Z}_5$;

   (c) the integers $\{0, 1, \ldots, 24\}$, where k represents the $(k - 1)$th power of α.

10. Show that the polynomial $(X^2 + 1)$ is irreducible over $\mathbb{R}$. Find its roots in $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$. What is their order?

11. Find the roots of $(X^2 + X + 1)$ in $\mathbb{Z}_5[X]/(X^2 + X + 1)$. What is their order?

12. $(X^3 + X^2 + 1)$ is irreducible over $\mathbb{B}$ and the order of its roots is 7. Use this fact to construct a Fire code whose code words have length 14. Write down the generator polynomial and generator matrix for this code. How many information bits and how many parity check bits does the code have?

13. The real numbers, $\mathbb{R}$, form an extension field of the rational numbers, $\mathbb{Q}$. What is the minimum polynomial in $\mathbb{Q}[X]$ of $5 \in \mathbb{Q}$? What is the minimum polynomial in $\mathbb{Q}[X]$ of $\sqrt[7]{5} \in \mathbb{R}$? What is the minimum polynomial in $\mathbb{Q}[X]$ of $(1 + \sqrt{5}) \in \mathbb{R}$?

*14. Show that $GF(9)$ is an extension field of $\mathbb{Z}_3$ by finding a mapping from $\mathbb{Z}_3$ into a subset of $GF(9)$ that is a ring isomorphism. Find the minimum polynomial in $\mathbb{Z}_3[X]$ of $2 \in \mathbb{Z}_3$ and the minimum polynomial in $\mathbb{Z}_3[X]$ of $5 \in GF(9)$. (Use the addition and multiplication tables for $GF(9)$ given in Example 8.4.)

15. Find the least common multiple of the following sets of polynomials:

    (a) $(X+1)$ and (X^2+1) in $\mathbb{B}[X]$;

    (b) (X^2+1) and (X^3+1) in $\mathbb{B}[X]$;

    (c) (X^2+2) and (X^2+X) in $\mathbb{Z}_3[X]$;

    (d) (X^2+X+2) and (X^2+3X+2) in $\mathbb{Z}_4[X]$;

    (e) (X^2+X+3) and (X^2+4X+3) in $\mathbb{Z}_5[X]$.

16. Construct a linear code whose code words are five ternary digits long and whose dimension is 2. List all its code words and find its parity check matrix.

17. Construct a linear code whose code words belong to $\mathbb{Z}_5^4$ and whose dimension is 2. List all its code words and find its parity check matrix.

18. Construct a cyclic code whose code words are six ternary digits long and whose dimension is 3. List all its code words and find its parity check matrix.

19. Find the powers of 3 in $\mathbb{Z}_5$. Use them to construct a Reed-Solomon code with $n = 4$ and $d = 3$.

20. Find the powers of 2 in $\mathbb{Z}_{11}$. Use them to construct a Reed-Solomon code with $n = 10$ and $d = 5$.

8.12 References

[1] J. B. Fraleigh, *A First Course in Abstract Algebra,* 5th ed., Addison-Wesley, Reading, MA, 1994.

[2] S. Lin, *An Introduction of Error-Correcting Codes,* Prentice-Hall, Englewood Cliffs, NJ, 1970.

[3] R. J. McEliece, *The Theory of Information and Coding,* 2nd ed., Cambridge University Press, Cambridge, 2002.

[4] W. W. Peterson, *Error-correcting Codes,* MIT Press, Cambridge, MA, 1961.