consider factorization of the polynomials $X^n - 1$ over F_p as a product of irreducible polynomials over F_p.

Definition 4.6

Let K be a field, F a subfield of K and $\alpha \in K$. By $F(\alpha)$ we denote the smallest subfield of K which contains both F and α. We also call $F(\alpha)$ a **simple extension** of F.

Recall that if α is algebraic over F and the degree of the minimal polynomial of α over F is n then an arbitrary element of $F(\alpha)$ is of the form

$$a_0 + a_1\alpha + \cdots + a_m\alpha^m$$

where $a_i \in F, 0 \leq i \leq m$ and $m \leq n - 1$. If, on the other hand, α is transcendental over F, then an arbitrary element of $F(\alpha)$ is of the form $f(\alpha)/g(\alpha)$, where $f(X)$, $g(X) \in F[X]$ and $g(\alpha) \neq 0$.

Again, if $\alpha_1, \alpha_2, \ldots, \alpha_m$ are elements of the extension K of F, we write $F(\alpha_1, \alpha_2, \ldots, \alpha_m)$ for $F(\alpha_1)(\alpha_2)\ldots(\alpha_m)$.

Definition 4.7

Let F be a field and $f(X) \in F[X]$. An extension field K of F is called a **splitting field** of $f(X)$ if

(i) $f(X)$ factors as a product of linear factors over K; and
(ii) if $\alpha_1, \alpha_2, \ldots, \alpha_m$ are the roots of $f(X)$ then $K = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$.

The procedure adopted in Examples 4.1–3 for the construction of finite fields also yields the following result which besides being of independent interest is needed for the construction of a splitting field of a given polynomial.

Proposition 4.6

Let $f(X)$ be an irreducible polynomial over a field F. Then there exists an extension K of F in which $f(X)$ has a root.

Proof

The polynomial $f(X)$ being irreducible, $K = F[X]/\langle f(X) \rangle$ is a field (Theorem 4.2). The element $\alpha = X + \langle f(X) \rangle$ of K is then a root of $f(X)$. The map

$$a \to a + \langle f(X) \rangle \quad a \in F$$

is a homomorphism: $F \to K$ which is clearly a monomorphism. Identifying the element a of F with the corresponding element $a + \langle f(X) \rangle$ of K we can regard K as an extension of F.

Corollary

Given any non-constant polynomial $f(X)$ over a field F, there exists an extension K of F in which $f(X)$ has a root.

Proof

Let $g(X) \in F[X]$ be an irreducible factor of $f(X)$. Then there exists an extension K of F in which $g(X)$ has a root α (say). But then α is also a root of $f(X)$.

Observe that the field K constructed in Proposition 4.6 is the smallest extension of F in which $f(X)$ has a root.

Examples 4.4

Case (i)

Consider the polynomial $X^2 + 1$ over the field Q of rational numbers. This is an irreducible polynomial over Q and so

$$K = Q[X]/\langle X^2 + 1 \rangle$$

is a field. Let α denote the element $X + \langle X^2 + 1 \rangle$ of K. Then $\alpha^2 = -1$ and an arbitrary element of K is of the form $a + b\alpha$, $a, b \in Q$. In the usual terminology of complex numbers, α is the complex number i $(= \sqrt{-1})$ and so

$$K = \{a + b\mathrm{i}/a, b \in Q\} = Q(\mathrm{i})$$

is a subfield of the field $\mathbb{C}$ of complex numbers.

Case (ii)

As another example, consider the polynomial $X^2 - X + 1$ over Q. This is irreducible over Q and so $\langle X^2 - X + 1 \rangle$ is a maximal ideal in $Q[X]$. Hence

$$K = Q[X]/\langle X^2 - X + 1 \rangle$$

is a field. Let

$$\alpha = X + \langle X^2 - X + 1 \rangle$$

Since any element of K is of the form

$$aX + b + \langle X^2 - X + 1 \rangle$$

where $a, b \in Q$, and uniquely so, arbitrary element of K can be written as $a\alpha + b$, $a, b \in Q$. Also clearly α is a root of the polynomial $X^2 - X + 1$. The map

$$a \to a + \langle X^2 - X + 1 \rangle \quad a \in Q$$

is a ring monomorphism from Q into K and, therefore, its image in K is a subfield of K isomorphic to Q. We may identify $a \in Q$ with the corresponding element

$$a + \langle X^2 - X + 1 \rangle$$

of K and so Q may be regarded as a subfield of K.

In the usual terminology of complex numbers we may take α to be

$$\frac{1 + \sqrt{3}\mathrm{i}}{2} \quad \text{or} \quad \frac{1 - \sqrt{3}\mathrm{i}}{2}$$

If we take

$$\alpha = \frac{1+\sqrt{3}\mathrm{i}}{2}$$

then

$$\frac{1-\sqrt{3}\mathrm{i}}{2} = 1 - \alpha \in Q(\alpha)$$

and $K = Q(\alpha)$.

Given an irreducible polynomial $f(X) \in F[X]$, there can exist distinct but isomorphic field extensions of F in which $f(X)$ has a root.

Example 4.5

Consider the polynomial $X^4 - 2 \in Q[X]$. The Eisenstein's irreducibility criterion shows that $X^4 - 2$ is irreducible over Q. The roots of this polynomial are α, $-\alpha$, $\alpha\mathrm{i}$, $-\alpha\mathrm{i}$, where α is the real positive fourth root of 2 and $\mathrm{i} = \sqrt{-1}$. The polynomial $X^4 - 2$ is the minimal polynomial of both α and $\alpha\mathrm{i}$. Therefore, every element of $Q(\alpha)$ can be uniquely written as

$$a + b\alpha + c\alpha^2 + d\alpha^3$$

where $a, b, c, d \in Q$ and every element of $Q(\alpha\mathrm{i})$ can be uniquely written as

$$a + b\alpha\mathrm{i} - c\alpha^2 - d\alpha^3\mathrm{i}$$

where $a, b, c, d \in Q$. The map

$$\theta : Q(\alpha) \to Q(\alpha\mathrm{i})$$

defined by

$$\theta(a + b\alpha + c\alpha^2 + d\alpha^3) = a + b\alpha\mathrm{i} - c\alpha^2 - d\alpha^3\mathrm{i} \quad a, b, c, d \in Q$$

is an isomorphism of the two vector spaces. Also

$$\begin{aligned}
&\theta((a + b\alpha + c\alpha^2 + d\alpha^3)(a' + b'\alpha + c'\alpha^2 + d'\alpha^3)) \\
&\quad = \theta(aa' + (ab' + a'b)\alpha + (ac' + bb' + ca')\alpha^2 + (ad' + bc' + cb' + da')\alpha^3 \\
&\qquad + (bd' + cc' + db')2 + (cd' + dc')2\alpha + dd'2\alpha^2) \\
&\quad = \theta(aa' + 2(bd' + cc' + db') + (ab' + a'b + 2(cd' + dc'))\alpha \\
&\qquad + (ac' + bb' + ca' + 2dd')\alpha^2 + (ad' + bc' + cb' + da')\alpha^3) \\
&\quad = aa' + 2(bd' + cc' + db') + (ab' + a'b + 2(cd' + dc'))\alpha\mathrm{i} \\
&\qquad - (ac' + bb' + ca' + 2dd')\alpha^2 - (ad' + bc' + cb' + da')\alpha^3\mathrm{i} \\
&\quad = (a + b\alpha\mathrm{i} - c\alpha^2 - d\alpha^3\mathrm{i})(a' + b'\alpha\mathrm{i} - c'\alpha^2 - d'\alpha^3\mathrm{i}) \\
&\quad = \theta(a + b\alpha + c\alpha^2 + d\alpha^3)\theta(a' + b'\alpha + c'\alpha^2 + d'\alpha^3)
\end{aligned}$$

for $a, a', b, b', c, c', d, d' \in Q$.

Thus θ is an isomorphism of fields. Also $Q(\alpha)$ contains the root α of X^4-2 and $Q(\alpha i)$ contains the root αi of X^4-2. Clearly $Q(\alpha)$ is a subfield of $\mathbb{R}$, the field of real numbers while $Q(\alpha i)$ is not contained in $\mathbb{R}$.

Theorem 4.4
Let F be a field and $f(X)\in F[X]$. Then there exists a splitting field of $f(X)$ over F.

Proof
We prove the theorem by induction on the degree of $f(X)$. If $\deg f(X)=1$, then it is clear that F itself is a splitting field of $f(X)$. Suppose that $\deg f(X)=n\geq 2$. By Proposition 4.6 there exists an extension of F in which $f(X)$ has a root α_1 (say). Let

$$F_1=F(\alpha_1)$$

Then

$$f(X)=(X-\alpha_1)g(X)$$

where $g(X)\in F_1[X]$ and $\deg g(X)=n-1$. By induction hypothesis $g(X)$ has a splitting field K over F_1, i.e. $g(X)$ factors as a product of linear factors over K and

$$K=F_1(\alpha_2,\ldots,\alpha_n)$$

where $\alpha_2,\ldots,\alpha_n$ are the roots of $g(X)$. But then $\alpha_1,\alpha_2,\ldots,\alpha_n$ are the roots of $f(X)$, $K=F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ and $f(X)$ factors as a product of linear factors over K. Hence K is a splitting field of $f(X)$.

4.2 SOME EXAMPLES OF PRIMITIVE POLYNOMIALS

Examples 4.6
Let $F=F_3$ – the field of 3 elements. Then

$$aX^2+bX+1 \quad a,b\in F$$

are the only possible irreducible polynomials of degree 2 over F. But then we must also have

$$a+b+1\neq 0 \quad \text{and} \quad a-b+1\neq 0$$

Therefore the possible values of a and b are: $a=1$, $b=0$ or $a=-1$, $b=1$ or $a=-1=b$. Thus all the irreducible polynomials over F of degree 2 are:

$$X^2+1 \quad X^2-X-1 \quad X^2+X-1$$

The polynomial X^2+1 divides X^4-1 over F and so is not primitive. Again

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

and neither of $X^2 - X - 1$ and $X^2 + X - 1$ is a divisor of $X^3 + 1$. It is also clear that neither of these two polynomials is a divisor of

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

Also

$$X^6 - 1 = (X^3 - 1)(X^3 + 1) = (X - 1)^3(X + 1)^3$$

and so neither of the two polynomials is a divisor of $X^6 - 1$. Suppose that

$$X^2 + X - 1 | X^5 - 1$$

Then $X^2 + X - 1$ must divide $X^4 + X^3 + X^2 + X + 1$. Then

$$X^4 + X^3 + X^2 + X + 1 = (X^2 + X - 1)(X^2 + aX - 1)$$

and $1 = a + 1$ and $-a - 1 = 1$. This gives a contradiction. Similarly

$$X^4 + X^3 + X^2 + X + 1 = (X^2 - X - 1)(X^2 + aX - 1)$$

gives $-1 + a = 1$ and $-a - 1 = 1$ which again lead to a contradiction. Thus, neither of the two polynomials under consideration divides $X^5 - 1$ over F. If

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

then comparing coefficients of powers of X gives $1 + a = 1$, $a + b - 1 = 1$, $-a + b + c = 1$, $-b + c - 1 = 1$, $-c - 1 = 1$ in F which lead to a contradiction. Also

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

gives $-1 + a = 1$, $-1 - a + b = 1$, $-a - b + c = 1$, $-b - c - 1 = 1$, $-c + 1 = 1$ which again lead to a contradiction.

Thus, both the polynomials $X^2 + X - 1$ and $X^2 - X - 1$ are primitive over F. We have thus proved that $X^2 + X - 1$ and $X^2 - X - 1$ are the only primitive polynomials of degree 2 over $F_3 = F$.

Examples 4.7

Here we consider some primitive polynomials over $\mathbb{B}$.

Case (i)

The polynomial $X + 1$ over $\mathbb{B}$ is trivially the only primitive polynomial of degree 1.

Case (ii)

Neither 0 nor 1 is a root of the polynomial $X^2 + X + 1$ over $\mathbb{B}$ and so it is an irreducible polynomial. It is trivially a primitive polynomial.

Case (iii)

We have already proved in Example 4.3 Case (i) that $X^3 + X + 1$ is a primitive polynomial of degree 3 because the element $X + \langle X^3 + X + 1 \rangle$ of the field $\mathbb{B}[X]/\langle X^3 + X + 1 \rangle$ is primitive.

Observe that if $f(X)$ is any irreducible polynomial over $\mathbb{B}$ of degree 3, then the field

$$K = \mathbb{B}[X]/\langle f(X)\rangle$$

is of order 8 and the multiplicative group K^* of K being of prime order, every non-zero, non-identity element of K is a primitive element. In particular so is the element $X + \langle f(X)\rangle$. This proves that $f(X)$ is a primitive polynomial.

Clearly $X^3 + X^2 + 1$ and $X^3 + X + 1$ are the only cubic polynomials over $\mathbb{B}$ which are irreducible. Thus $X^3 + X + 1$ and $X^3 + X^2 + 1$ are the only cubic primitive polynomials over $\mathbb{B}$.

Case (iv)

The argument in Case (iii) above can also be used to prove that every irreducible polynomial of degree 5 over $\mathbb{B}$ is primitive. Observe that

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

and

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

Also neither 0 nor 1 is a root of the polynomial $X^5 + X^2 + 1$ or $X^5 + X^3 + 1$. Hence $X^5 + X^2 + 1$ and $X^5 + X^3 + 1$ are two primitive polynomials.

Similarly $X^5 + X^4 + X^3 + X^2 + 1$, $X^5 + X^4 + X^3 + X + 1$, $X^5 + X^4 + X^2 + X + 1$ and $X^5 + X^3 + X^2 + X + 1$ are all the other irreducible polynomials of degree 5 over $\mathbb{B}$. Hence all the primitive polynomials of degree 5 over $\mathbb{B}$ are

$$X^5 + X^2 + 1 \quad X^5 + X^3 + 1 \quad X^5 + X^4 + X^3 + X^2 + 1$$

$$X^5 + X^4 + X^3 + X + 1 \quad X^5 + X^4 + X^2 + X + 1 \quad X^5 + X^3 + X^2 + X + 1$$

Case (v)

Since the multiplicative group of a field K of order 2^7 is of order 127 (a prime), every non-zero, non-identity element of K is primitive and, therefore, every irreducible polynomial of degree 7 over $\mathbb{B}$ is primitive. By direct computation we find that

$$(X^2 + X + 1)(X^5 + X^2 + 1) = X^7 + X^6 + X^5 + X^4 + X^3 + X + 1$$

$$(X^2 + X + 1)(X^5 + X^3 + 1) = X^7 + X^6 + X^4 + X^3 + X^2 + X + 1$$

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

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

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

$$(X^2 + X + 1)(X^5 + X^3 + X^2 + X + 1) = X^7 + X^6 + X^3 + X^2 + 1$$

$$(X^3 + X + 1)(X^4 + X^3 + 1) = X^7 + X^6 + X^5 + X + 1$$

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

$$(X^3+X+1)(X^4+X^3+X^2+X+1)=X^7+X^6+X^5+X^4+X^3+1$$
$$(X^3+X^2+1)(X^4+X^3+1)=X^7+X^5+X^4+X^2+1$$
$$(X^3+X^2+1)(X^4+X+1)=X^7+X^6+X^2+X+1$$
$$(X^3+X^2+1)(X^4+X^3+X^2+X+1)=X^7+X^4+X^3+X+1$$

From these computations, we can read of all irreducible and hence primitive polynomials of degree 7 over $\mathbb{B}$. These are

X^7+X^6+1	$X^7+X^6+X^3+X+1$
X^7+X^4+1	$X^7+X^5+X^4+X^3+1$
X^7+X^3+1	$X^7+X^5+X^3+X+1$
X^7+X+1	$X^7+X^4+X^3+X^2+1$
$X^7+X^6+X^5+X^2+1$	$X^7+X^4+X^2+X+1$
$X^7+X^6+X^5+X^3+1$	$X^7+X^3+X^2+X+1$
$X^7+X^6+X^5+X^4+1$	$X^7+X^5+X^2+X+1$
$X^7+X^6+X^4+X+1$	$X^7+X^6+X^5+X^4+X^3+X^2+1$
$X^7+X^6+X^4+X^2+1$	$X^7+X^6+X^5+X^4+X^2+X+1$
$X^7+X^6+X^4+X^3+1$	$X^7+X^6+X^5+X^3+X^2+X+1$

4.3 BOSE–CHAUDHURI–HOCQUENGHEM CODES

Hocquenghem (1959) and Bose and Ray-Chaudhuri (1960) independently proved a remarkable theorem which enables us to systematically construct one of the most powerful multiple error-correcting codes for random independent errors. These are polynomial codes and are now called Bose–Chaudhuri–Hocquenghem codes (BCH codes for short!). Recall that a polynomial code is determined as soon as the generator polynomial is determined. Procedure for constructing a BCH code is as follows.

Suppose that a BCH code with code word length n, minimum distance d and with symbols in $F=\mathrm{GF}(q)$, a field of order q ($=$a power of a prime p) is required. We choose the least positive integer r which satisfies $q^r \geq n+1$. Let K be an extension of F of degree r and let α be a primitive element of K. Let $m_i(X)$ be the minimal polynomial of α^i, $1 \leq i \leq d-1$ and set

$$g(X)=\mathrm{LCM}(m_1(X),\ldots,m_{d-1}(X))$$

Theorem 4.5

The polynomial code with symbols in F and encoding polynomial $g(X)$ has minimum distance at least d.

Proof

Let $h(X)$ be any polynomial over F which has $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ among its roots. Then

$$m_i(X) \mid h(X) \forall i,\ 1 \leq i \leq d-1$$