

**Exercise 6.6**

1. Determine all non-cyclic binary Abelian codes of length 9. (Hint: Compute all the ideals in the group algebra  $FA$ , where  $A$  is direct sum of two cyclic groups of order 3 each.)
2. Determine all non-cyclic ternary Abelian codes of length 4. (As in 1 above, here we need all ideals of the group algebra  $FA$  when  $F$  is the field of 3 elements and  $A$  is direct sum of two cyclic groups each of order 2.)

**6.8 SELF DUAL BINARY CYCLIC CODES**

Let  $\mathcal{C}$  be a binary cyclic code of length  $n$  with generator polynomial  $g(X)$ . Let  $h(X)$  be its check polynomial. Then the dual  $\mathcal{C}^\perp$  is generated by

$$k(X) = X^{n-r}h(X^{-1})$$

The relation  $X^n + 1 = g(X)h(X)$  shows that

$$\begin{aligned} X^n + 1 &= X^n g(X^{-1})h(X^{-1}) \\ &= X^r g(X^{-1}) \times X^{n-r} h(X^{-1}) \\ &= X^r g(X^{-1}) k(X) \end{aligned}$$

Thus

$$k(X) = -\frac{X^n + 1}{X^r g(X^{-1})}$$

It then follows that  $\mathcal{C}$  is self dual iff

$$g(X) = -\frac{X^n + 1}{X^r g(X^{-1})}$$

or iff

$$X^r g(X) g(X^{-1}) = X^n + 1$$

We then have the following theorem.

**Theorem 6.11**

A binary cyclic code of length  $n$  generated by  $g(X)$  of degree  $r$  is self dual iff

$$X^n + 1 = X^r g(X) g(X^{-1})$$

In a similar fashion we can prove that a cyclic code of length  $n$  generated by  $g(X)$  of degree  $r$  over  $\text{GF}(q)$  is self dual iff

$$X^r g(X) g(X^{-1}) = -(X^n - 1)$$

**Examples 6.5**

The binary polynomial  $X^{14} + 1$  factors as

$$X^{14} + 1 = (X^7 + 1)^2 = (X + 1)^2(X^3 + X^2 + 1)^2(X^3 + X + 1)^2$$

The polynomial

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

is such that

$$X^7 g(X) g(X^{-1}) = (X + 1)(X^3 + X + 1)^2(X + 1)(X^3 + X^2 + 1)^2 = X^{14} + 1$$

Hence the binary cyclic code of length 14 generated by  $g(X)$  is self dual.

The binary polynomial  $X^{30} + 1$  factors as

$$X^{30} + 1 = (X^{15} + 1)^2 = (X^5 + 1)^2(X^{10} + X^5 + 1)^2$$

and the factor

$$g(X) = (X^5 + 1)(X^{10} + X^5 + 1)$$

is such that

$$X^{15} g(X) g(X^{-1}) = X^{30} + 1$$

Hence  $g(X)$  generates a binary self dual code of length 30.

The binary polynomial  $X^{42} + 1$  factors over  $\mathbb{B}$  as

$$\begin{aligned} X^{42} + 1 &= (X^6 + 1)(X^{18} + X^6 + 1)(X^{18} + X^{12} + 1) \\ &= (X + 1)^2(X^2 + X + 1)^2(X^{18} + X^6 + 1)(X^{18} + X^{12} + 1) \end{aligned}$$

Consider the binary code of length 42 generated by

$$g(X) = (X + 1)(X^2 + X + 1)(X^{18} + X^6 + 1)$$

Clearly

$$X^{21} g(X) g(X^{-1}) = X^{42} + 1$$

Therefore the code is self dual.

**Exercise 6.7**

- Find the minimum distance of the binary self dual code of length (i) 14; (ii) 30; (iii) 42, constructed above.
- Construct some cyclic self dual codes over  $\text{GF}(4)$ .
- Construct some cyclic self dual codes over  $\text{GF}(8)$ .

We now show that no cyclic self dual codes over an odd order field exist.

Let  $F = \text{GF}(q)$  where  $q = p^r$  and  $p$  is an odd prime. If possible, let  $\mathcal{C}$  be a cyclic self dual code of length  $n$  over  $F$  generated by  $g(X)$  (say). Let  $h(X)$  be its check polynomial. Then

$$g(X) = aX^{n-m}h(X^{-1})$$

where  $0 \neq a \in F$ , and  $m = \deg g(X) (= n/2)$ . The relation  $X^n - 1 = g(X)h(X)$  then implies that

$$X^n - 1 = -aX^m g(X)g(X^{-1}) \quad (6.4)$$

If  $n$  and  $p$  are coprime,  $X^n - 1$  has no repeated roots in any extension field of  $F$ . But (6.4) shows that 1 is a root of  $X^n - 1$  repeated at least twice – a contradiction.

If  $n, p$  are not coprime, let  $n = p^t u$ , where  $u$  and  $p$  are coprime. Then

$$X^n - 1 = (X^u - 1)^{p^t}$$

and  $X^u - 1$  has no repeated roots. Therefore, every root of  $X^n - 1$  and, in particular, 1 is repeated exactly  $p^t$  times. However, (6.4) shows that 1 is a root repeated an even number of times – again a contradiction. Hence, a cyclic self dual code over an odd order field does not exist.

# 7

# Factorization of polynomials

---

## 7.1 FACTORS OF $X^n - 1$

In the construction of finite fields, we were required to find certain irreducible factors of  $X^n - 1$  where  $n = p^m - 1$ ,  $p$  a prime. Again, while studying cyclic codes we encountered the same problem. Here we study the problem of factorization of  $X^n - 1$  as a product of irreducible polynomials. However, first we consider a couple of results about finite fields.

### Theorem 7.1

- (i)  $\text{GF}(p^r)$ ,  $p$  a prime contains a subfield of order  $p^s$  iff  $s|r$ .
- (ii) If  $\text{GF}(p^s)$  is a subfield of  $\text{GF}(p^r)$  and  $\beta \in \text{GF}(p^r)$ , then

$$\beta \in \text{GF}(p^s) \quad \text{iff} \quad \beta^{p^s} = \beta$$

### *Proof*

#### *Part (i)*

Suppose that  $s|r$  and let  $k$  be a positive integer such that  $r = ks$ . Let  $\alpha$  be a primitive element of  $\text{GF}(p^r)$ . Then

$$\text{GF}(p^r) = \{0, 1, \alpha, \dots, \alpha^{p^r-1}\}$$

Let

$$F = \{\beta \in \text{GF}(p^r) \mid \beta^{p^s} = \beta\}$$

Since  $\text{GF}(p^r)$  is of characteristic  $p$ , if the elements  $\beta, \gamma \in F$  then so do the elements  $\beta \pm \gamma$  and  $\beta\gamma^{-1}$ ,  $\gamma \neq 0$ . Thus  $F$  is a subfield of  $\text{GF}(p^r)$ . As the polynomial

$$X^{p^s} - X$$