is a factor of $M_s(X)$ over GF(p^m). In particular

$$\deg \prod_{i \in C_s} (X - \alpha^i) \leq \deg M_s(X) \tag{7.1}$$

Let

$$C_s(\alpha) = \{\alpha^s, \alpha^{ps}, \ldots, \alpha^{sp^{m_s-1}}\}$$

Since

$$sp^{m_s} \equiv s (\mathrm{mod}\, n)$$

then

$$\alpha^{sp^{m_s}} = \alpha^s$$

Therefore, with $A^p = \{a^p | a \in A\}$ for any subset A of GF(p^m), we find that

$$C_s(\alpha)^p = C_s(\alpha)$$

It follows that if

$$\sigma_1, \sigma_2, \ldots, \sigma_{m_s}$$

denote the symmetric polynomials in the elements of $C_s(\alpha)$, then

$$\sigma_i^p = \sigma_i \quad \forall 1 \leq i \leq m_s$$

and, hence, $\sigma_i \in$ GF(p) for $1 \leq i \leq m_s$ (by Theorem 7.1 Part (ii)). Therefore

$$\prod_{i \in C_s} (X - \alpha^i)$$

is a polynomial over GF(p) having α^s as a root. But then

$$M_s(X) \mid \prod_{i \in C_s} (X - \alpha^i)$$

over GF(p). Both the polynomials being monic, it follows from this and (7.1) that

$$M_s(X) = \prod_{i \in C_s} (X - \alpha^i)$$

Corollary

$$X^n - 1 = \prod_s M_s(X)$$

where s runs over a set of representatives of cyclotomic cosets modulo n over GF(p).

Examples 7.2

Case (i)

We use this theorem first to obtain factorization of $X^9 + 1$ over $\mathbb{B}$. Here the least m such that $9 | 2^m - 1$ is 6. So, we have to construct a field of order 64. The polynomial $X^6 + X + 1$ is irreducible over $\mathbb{B}$ and so

$$F = \mathbb{B}[X]/\langle X^6 + X + 1 \rangle$$

is a field of order 64. Let

$$\alpha = X + \langle X^6 + X + 1 \rangle$$

It is a primitive element of F and so $\beta = \alpha^7 = \alpha^2 + \alpha$ is a primitive 9th root of unity. The cyclotomic classes modulo 9 over $\mathbb{B}$ are:

$$C_0 = \{0\} \qquad C_1 = \{1, 2, 4, 8, 7, 5\} \qquad C_3 = \{3, 6\}$$

Then, $M_0(X) = X + 1$ and $M_3(X) = X^2 + X + 1$ – this being the only irreducible polynomial of degree 2 over $\mathbb{B}$. Also then, it follows that

$$\beta^6 + \beta^3 + 1 = 0$$

The polynomial $X^6 + X^3 + 1$ being irreducible, it follows that

$$M_1(X) = X^6 + X^3 + 1$$

Hence

$$X^9 + 1 = (X + 1)(X^2 + X + 1)(X^6 + X^3 + 1)$$

Case (ii)

Now we factorize $X^{13} - 1$ over GF(3). The order of 3 modulo 13 is 3. So, we have to construct a field of order 27. The polynomial $X^3 + 2X + 1$ is irreducible over F and so

$$F_1 = F[X]/\langle X^3 + 2X + 1 \rangle$$

is a field of order 27. The element

$$\alpha = X + \langle X^3 + 2X + 1 \rangle$$

of F_1 is primitive and so $\beta = \alpha^2$ is a primitive 13th root of unity. The cyclotomic classes modulo 13 over F are:

$$C_0 = \{0\} \qquad C_1 = \{1, 3, 9\} \qquad C_2 = \{2, 6, 5\}$$
$$C_4 = \{4, 12, 10\} \qquad C_7 = \{7, 8, 11\}$$

so we have to find the minimal polynomials of β, β^2, β^4 and β^7.

The minimal polynomial of α is $X^3 + 2X + 1$. Therefore,

$$\alpha^3 = \alpha + 2$$

Now

$$\begin{aligned}\beta^2 &= \alpha^4 = \alpha^2 + 2\alpha \\ \beta^3 &= \alpha^4 + 2\alpha^3 \\ &= \alpha^2 + 2\alpha + 2\alpha + 1 \\ &= \alpha^2 + \alpha + 1\end{aligned}$$

Clearly, $\beta^3 + \beta^2 + \beta = 1$ and as $X^3 + X^2 + X + 2$ is irreducible over F, it is the minimal polynomial of β. Now,

$$\begin{aligned}M_2(X) &= X^3 - X^2(\beta^2 + \beta^5 + \beta^6) + X(\beta^7 + \beta^8 + \beta^{11}) - 1 \\ M_7(X) &= X^3 - X^2(\beta^7 + \beta^8 + \beta^{11}) + X(\beta^2 + \beta^5 + \beta^6) - 1 \\ M_4(X) &= X^3 - X^2(\beta^4 + \beta^{10} + \beta^{12}) + X(\beta + \beta^3 + \beta^9) - 1\end{aligned}$$

Now

$$\beta^3 = -\beta^2 - \beta + 1$$

and so

$$\begin{aligned}\beta^6 &= \beta^4 + \beta^2 + 1 - \beta^3 + \beta^2 + \beta \\ &= \beta^4 - \beta^3 - \beta^2 + \beta + 1\end{aligned}$$

and

$$\begin{aligned}\beta^2 + \beta^5 + \beta^6 &= \beta^2 - \beta^4 - \beta^3 + \beta^2 + \beta^4 - \beta^3 - \beta^2 + \beta + 1 \\ &= \beta^3 + \beta^2 + \beta + 1 \\ &= 2 \\ \beta^7 &= \beta^5 - \beta^4 - \beta^3 + \beta^2 + \beta \\ \beta^9 &= -\beta^6 - \beta^3 + 1\end{aligned}$$

and so

$$\beta^{11} = -\beta^8 - \beta^5 + \beta^2$$

Therefore

$$\begin{aligned}\beta^7 + \beta^8 + \beta^{11} &= -\beta^4 - \beta^3 - \beta^2 + \beta \\ &= -\beta(\beta^3 + \beta^2 + \beta) + \beta = 0\end{aligned}$$

Again

$$\begin{aligned}\beta^4 &= -\beta^3 - \beta^2 + \beta \\ \beta^{12} &= -\beta^9 - \beta^6 + \beta^3 = -\beta^3 - 1 \\ \beta^{10} &= -\beta^7 - \beta^4 + \beta\end{aligned}$$

and so

$$\begin{aligned}\beta^4+\beta^{10}+\beta^{12} &= -\beta^7+\beta-\beta^3-1\\ &= -\beta^5+\beta^4-\beta^2-1\\ &= -\beta^4+\beta^3+\beta^2-1\\ &= -\beta^3-\beta^2-\beta-1=1\end{aligned}$$

Also

$$\begin{aligned}\beta^3+\beta^9 &= -\beta^6+1\\ &= -\beta^4+\beta^3+\beta^2-\beta\\ &= -\beta^3-\beta^2-2\beta\\ &= -1-\beta\end{aligned}$$

or

$$\beta+\beta^3+\beta^9=2$$

Thus

$$M_2(X)=X^3+X^2+2 \qquad M_7(X)=X^3+2X+2$$
$$M_4(X)=X^3+2X^2-X+2$$

and

$$\begin{aligned}X^{13}-1=(X-1)(X^3+X^2+X+2)(X^3+X^2+2)(X^3+2X+2)\\ \times(X^3+2X^2+2X+2)\end{aligned}$$

Exercise 7.1

1. Prove that over any field $X^s-1 \mid X^r-1$ iff $s \mid r$.
2. Show that g.c.d.$(X^s-1, X^r-1)=X^d-1$, where $d=$ g.c.d.(r,s).
3. Let q be a prime power, n a positive integer relatively coprime to q and m be the multiplicative order of q mod n. Prove that X^n-1 has all its roots in an extension field GF(q^m) of GF(q).
4. Let α be a primitive nth root of unity in an extension GF(2^m) of $\mathbb{B}$ and let

$$f(X)=\prod_{i\in K}(X+\alpha^i)$$

   where K is a subset of $\{0,1,2,\ldots,n-1\}$. Show that the coefficients of $f(X)$ are in $\mathbb{B}$ iff $k\in K$ implies $2k\in K$ modulo n.
5. Find the irreducible factors of X^n+1 over $\mathbb{B}$ for $n \leq 15$.
6. Find the irreducible factors of X^n-1 over GF(3) for $n \leq 8$.
7. Write down some symmetric polynomials in commuting variables
   (i) X, Y;
   (ii) X, Y, Z.