has $p^s$ roots in its splitting field, $O(F) \leq p^s$. Take

$$\lambda = \alpha^{1+p^s+\cdots+p^{(k-1)s}} = \alpha^{(p^{ks}-1)/(p^s-1)}$$

The elements

$$1, \lambda, \lambda^2, \ldots, \lambda^{p^s-2}$$

are all distinct and

$$\lambda^{ip^s} = \lambda^i \quad \text{for } 0 \leq i < p^s - 1$$

Thus $O(F) \geq p^s$ and, therefore, $F$ is a subfield of $GF(p^r)$ of order $p^s$.

*Part (ii)*
That

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

is clear and the converse follows from the construction of $F$ in the above proof.

**Lemma 7.1**
Let $n, r, s$ be positive integers with $n \geq 2$. Then $n^s - 1 | n^r - 1$ iff $s | r$.

***Proof***
Write $r = sa + b$ where $0 \leq b < s$. Then

$$\frac{n^r - 1}{n^s - 1} = \frac{n^{sa+b} - n^b + n^b - 1}{n^s - 1}$$

$$= n^b \frac{n^{sa} - 1}{n^s - 1} + \frac{n^b - 1}{n^s - 1}$$

Since $(n^s - 1) | (n^{sa} - 1)$, it follows that $(n^s - 1) | (n^r - 1)$ iff $b = 0$.

**Theorem 7.2**
If $p$ is a prime

$$X^{p^m} - X$$

is a product of all monic polynomials, irreducible over $GF(p)$, whose degree divides $m$.

***Proof***
Let $f(X)$ be an irreducible monic polynomial over $GF(p)$ of degree $d$, where $d | m$. The case $f(X) = X$ is trivial, so assume that $f(X) \neq X$. Use $f(X)$ to construct a field $F$ of order $p^d$. Then $f(X)$ is the minimal polynomial of one of the elements of $F$ and so

$$f(X) | X^{p^d - 1} - 1$$

Now

$$d|m \Rightarrow (p^d - 1)|(p^m - 1)$$
$$\Rightarrow X^{p^d-1} - 1 | X^{p^m-1} - 1$$

Hence

$$f(X)|X^{p^m} - X$$

Conversely, let

$$f(X) \text{ be a divisor of } X^{p^m} - X$$

irreducible and of degree $d$. We have to prove that $d|m$. We can again assume that $f(X) \neq X$ so that

$$f(X)|(X^{p^m-1} - 1)$$

Use $f(X)$ to construct a field $F$ of order $p^d$. Let $\alpha \in F$ be a root of $f(X)$ and let $\beta$ be a primitive element of $F$, say

$$\beta = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \quad a_i \in \mathrm{GF}(p)$$

Now

$$f(\alpha) = 0 \Rightarrow \alpha^{p^m} = \alpha$$

Also

$$a_i^p = a_i \forall i,\ 0 \leq i \leq d-1$$

It then follows that

$$\beta^{p^m} = \beta$$

and so

$$\beta^{p^m-1} = 1$$

But the multiplicative order of $\beta$ is $p^d - 1$. Therefore $(p^d - 1)|(p^m - 1)$ and so $d|m$.

Finally, the formal derivative of

$$X^{p^m} - X$$

being

$$p^m X^{p^m-1} - 1 = -1$$

the polynomial

$$X^{p^m} - X$$

does not have repeated roots and so no repeated irreducible factors. ■

As applications of this theorem, we have the following for polynomials over $\mathbb{B}$.

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

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

$$X^8 + X = X(X+1)(X^3+X+1)(X^3+X^2+1) \qquad \text{(Proposition 4.4)}$$

$$X^{16} + X = X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)$$
$$\times (X^4+X^3+X^2+X+1) \qquad \text{(Examples 4.3)}$$

Over the field of 3 elements, we have the following decomposition as product of irreducible polynomials

$$X^9 - X = X^{3^2} - X$$
$$= X(X+1)(X+2)(X^2+1)(X^2+X+2)(X^2+2X+2)$$

$$X^{27} - X = X^{3^3} - X$$
$$= X(X+1)(X+2)(X^3+2X+2)(X^3+2X+1)(X^3+X^2+2)$$
$$\times (X^3+2X^2+1)(X^3+X^2+X+2)(X^3+X^2+2X+1)$$
$$\times (X^3+2X^2+X+1)(X^3+2X^2+2X+2) \qquad \text{(Proposition 4.4)}$$

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

## 7.2 FACTORIZATION THROUGH CYCLOTOMIC COSETS

**Definition 7.1**

In this section, $p$ is a prime, $n$ is a positive integer not divisible by $p$ and $q$ is a power of $p$. To obtain factorization of $X^n - 1$ over GF($q$), we first define cyclotomic classes and partition the set $S = \{0, 1, 2, \ldots, n-1\}$ of integers into cyclotomic classes or cosets modulo $n$ over GF($q$). Since g.c.d.$(n, q) = 1$, there exists a smallest positive integer $m$ such that $q^m \equiv 1 \pmod{n}$ or $q^m - 1$ is divisible by $n$ (by Euler–Fermat theorem and also $m = \phi(n)$ – the Euler totient function). This $m$ is called the **multiplicative order** of $q$ modulo $n$. In $S$ define a relation '$\sim$' as follows:

For $a, b \in S$, say that $a \sim b$ if $a \equiv bq^i \pmod{n}$ for some $i$. This relation is an equivalence relation and partitions the set $S$ into equivalence classes. Each such equivalence class is called a **cyclotomic class** or **coset mod** $n$ over GF($q$). Observe that the cyclotomic class containing $s \in S$ is

$$C_s = \{s, qs, \ldots, q^{m_s - 1}s\}$$

where $m_s$ is the smallest positive integer with

$$sq^{m_s} \equiv s \pmod{n}$$

Then $m_1 = m$ – the multiplicative order of $q$ modulo $n$.

**Examples 7.1**

(i) For $n = 7$, $q = 2$,

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

(ii) For $n = 11$, $q = 2$,

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

(iii) For $n = 15$, $q = 2$,

$$C_0 = \{0\} \qquad C_1 = \{1, 2, 4, 8\} \qquad C_3 = \{3, 6, 12, 9\}$$
$$C_5 = \{5, 10\} \qquad C_7 = \{7, 14, 13, 11\}$$

**Lemma 7.2**

If $s$ is relatively prime to $n$, then $C_s$ has $m$ elements.

***Proof***

Since $q^m \equiv 1 \pmod{n}$, $sq^m \equiv s \pmod{n}$. Also

$$sq^{m_s} \equiv s \pmod{n}$$

Therefore

$$sq^{m_s}(q^{m-m_s} - 1) \equiv 0 \pmod{n}$$

But g.c.d.$(s, n) = 1$ and, so

$$q^{m-m_s} - 1 \equiv 0 \pmod{n}$$

But $m$ being the smallest positive integer with this property, $m = m_s$. ■

From now on we assume that $q = p$ itself. Let GF($p^m$) be an extension of GF($p$) and $\alpha$ be a primitive $n$th root of unity. Then $\alpha \in$ GF($p^m$).

**Theorem 7.3**

If $C_s$ is the cyclotomic coset mod $n$ over GF($p$) containing the integer $s$, then

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

is the minimal polynomial of $\alpha^s$ over GF($p$).

***Proof***

Let $M_s(X)$ denote the minimal polynomial of $\alpha^s$ over GF($p$). Since the elements $\beta$ and $\beta^p$ of GF($p^m$) have the same minimal polynomial over GF($p$) (Proposition 4.2)

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