Finite Fields: Minimal Polynomials
Definition: Minimal polynomials

For every $\beta \in \text{GF}(p^m)$, the **minimal polynomial** of $\beta$ over $\text{GF}(p)$ is the lowest degree monic polynomial $M(x)$ over $\text{GF}(p)$, such that

$$M(\beta) = 0$$

Lemma: Uniqueness of the minimal polynomial

For every $\beta \in \text{GF}(p^m)$, the minimal polynomial of $\beta$ is well-defined. That is, the polynomial $M(x)$ is unique.

**Proof.** Suppose $M_1(x)$ and $M_2(x)$ are both monic of degree $r$, and

$$M_1(\beta) = M_2(\beta) = 0$$

Then $M^*(x) = M_1(x) - M_2(x)$ has degree at most $r - 1$, and $M^*(\beta) = 0$. This implies that $r$ is not minimal. □
Property 1: Irreducibility of minimal polynomials

$M(x)$ is irreducible over $\text{GF}(p)$.

**Proof.** Assume to the contrary that $M(X)$ has nontrivial factors. That is, $M(x) = M_1(x)M_2(x)$ with $\deg M_1(x) > 0$ and $\deg M_2(x) > 0$. Then

$$M(\beta) = M_1(\beta)M_2(\beta) = 0 \implies M_1(\beta) = 0 \text{ or } M_2(\beta) = 0$$

$$\implies M(x) \text{ is not minimal}$$

□
Properties of minimal polynomials

Property 2: Divisibility by the minimal polynomial

If \( f(x) \) is a polynomial over \( \text{GF}(p) \) and \( f(\beta) = 0 \), then \( M(x) \mid f(x) \).

**Proof.** Write \( f(x) = q(x)M(x) + r(x) \), with \( \deg r(x) < \deg M(x) \). Then

\[
0 = f(\beta) = q(\beta)M(\beta) + r(\beta) \quad \Rightarrow \quad r(\beta) = 0
\]

\[
\Rightarrow \quad M(x) \text{ is not minimal unless } r(x) = 0
\]

Property 3: Divisor of \( x^{p^m} - x \)

\[
M(x) \mid x^{p^m} - x
\]

**Proof.** Every \( \beta \in \text{GF}(p^m) \) is a root of \( x^{p^m} - x \). Then use Property 2.
Property 4: Upper bound on the degree

\[ \deg M(x) \leq m \]

**Proof.** Recall that \( \text{GF}(p^m) \) is a vector space of dimension \( m \) over \( \text{GF}(p) \). Hence the \( m + 1 \) elements \( 1, \beta, \beta^2, \ldots, \beta^m \) are linearly dependent:

\[
\Rightarrow \exists a_i \in \text{GF}(p) : \quad a_0 + a_1 \beta + \cdots + a_m \beta^m = 0
\]

\[
\Rightarrow f(x) = a_0 + a_1 x + \cdots + a_m x^m \text{ is such that } f(\beta) = 0
\]

\[
\Rightarrow \deg M(x) \leq \deg f(x) \leq m
\]

\[\Box\]
Properties of minimal polynomials

Property 5: Lower bound on the degree

If $\alpha \in \text{GF}(p^m)$ is primitive, then $\deg M_\alpha(x) = m$.

Proof. Let $\deg M_\alpha(x) = d$. Since $M_\alpha(x)$ is irreducible, we can use it to construct the field $F = \text{GF}(p)[x]/M_\alpha(x)$ of order $p^d$. But

$$\alpha \in F \quad \Rightarrow \quad \text{GF}(p^m) \in F \quad \Rightarrow \quad p^d \geq p^m \quad \Rightarrow \quad d \geq m$$

$\alpha$ is primitive
Property 6: Conjugates have the same minimal polynomial

For all $\beta \in \text{GF}(p^m)$, $\beta$ and $\beta^p$ have the same minimal polynomial.

Proof. Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in \text{GF}(p)[x]$. Then

$$f(\beta^p) = a_0 + a_1\beta^p + \cdots + a_m\beta^{pm}$$
$$= a_0^p + a_1^p\beta^p + \cdots + a_m^p\beta^{pm}$$  \quad (a_i \in \text{GF}(p) \iff a_i^p = a_i)
$$= \left(a_0 + a_1\beta + \cdots + a_m\beta^m\right)^p$$
$$= f(\beta)^p$$

Hence $f(\beta) = 0 \iff f(\beta^p) = 0$. Since this is true for any polynomial over $\text{GF}(p)$, it follows that $\beta$ and $\beta^p$ have the same minimal polynomial.  \qed
Conjugates and cyclotomic cosets

**Definition: Conjugate field elements**

The elements $\beta, \beta^p, \beta^{p^2}, \ldots \in \text{GF}(p^m)$ are called the **conjugates** of $\beta$.

All these elements have the same minimal polynomial. Moreover, for any $f(x) \in \text{GF}(p)[x]$, we have

$$f(\beta) = 0 \iff f(\beta^p) = 0 \iff f(\beta^{p^2}) = 0 \iff f(\beta^{p^3}) = 0 \iff \cdots$$

If $\alpha$ is a primitive element of $\text{GF}(p^m)$, then $\beta = \alpha^s$ for some $s$, and

$$\{\beta, \beta^p, \beta^{p^2}, \ldots\} = \{\alpha^s, \alpha^{ps}, \alpha^{p^2s}, \ldots\}$$

**Definition: Cyclotomic cosets**

The **cyclotomic coset** of $s$ modulo $p^m - 1$ is

$$C_s = \{s, ps, p^2s, \ldots, p^{\ell-1}s\} \pmod{p^m - 1}$$

where $\ell$ is the smallest integer with $p^\ell s \equiv s \pmod{p^m - 1}$.
Properties of cyclotomic cosets

Note that $C_s$ and $C_t$ are either same or disjoint. Indeed, suppose that $C_s$ and $C_t$ are not disjoint, and let $a \in C_s \cap C_t$. Then

$$a = p^i s = p^j t \mod p^m - 1$$

$$\Rightarrow s = p^{j-i} t \mod p^m - 1 \Rightarrow C_s = C_t$$

It follows that all the integers $\{0, 1, \cdots, p^m-2\}$ may be partitioned into cyclotomic cosets.

**Example:** $p = 2$, $m = 4 \rightarrow$ cyclotomic cosets $\mod (2^4 - 1) = 15$

$C_0 = \{0\}$
$C_1 = \{1, 2, 4, 8\}$
$C_3 = \{3, 6, 12, 9\}$
$C_5 = \{5, 10\}$
$C_7 = \{7, 14, 13, 11\}$
Theorem: Computing the minimal polynomial

If $\beta = \alpha^i$ with $i \in C_s$, then

$$M_\beta(x) = \prod_{j \in C_s} (x - \alpha^j)$$

Note that the product $\prod_{j \in C_s} (x - \alpha^j)$ is computed over $\text{GF}(p^m)$ but gives coefficients over $\text{GF}(p)$. The proof of this is a homework problem.

Corollary: Factorization of the $x^{p^m} - x$ polynomial

$$x^{p^m} - x = \prod_{\beta \in \text{GF}(p^m)} (x - \beta) = x \cdot \prod_s M_\alpha^s(x)$$

Note that $s$ in the product $\prod_s M_\alpha^s(x)$ runs through all the cyclotomic cosets in the partition of $\{0, 1, \cdots, p^m-2\}$. 
**Example:** Let $\text{GF}(2^4) = \text{GF}(2)[x] / \langle x^4 + x + 1 \rangle$, so that $\alpha^4 = \alpha + 1$.

Then the minimal polynomial of $\alpha, \alpha^2, \alpha^4, \alpha^8$ is given by:

$$M_\alpha(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)$$

$$= x^4 + (\alpha + \alpha^2 + \alpha^4 + \alpha^8) x^3$$

$$= 0$$

$$+ (\alpha^3 + \alpha^5 + \alpha^6 + \alpha^9 + \alpha^{10} + \alpha^{12}) x^2$$

$$= 0$$

$$+ (\alpha^7 + \alpha^{11} + \alpha^{13} + \alpha^{14}) x + \alpha^{15}$$

$$= 1$$

$$= x^4 + x + 1$$
### Minimal polynomials: An example

**Example:** Let $\text{GF}(2^4) = \text{GF}(2)[x]/\langle x^4 + x + 1 \rangle$, so that $\alpha^4 = \alpha + 1$.

<table>
<thead>
<tr>
<th>elements</th>
<th>minimal polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0$</td>
<td>$x$</td>
</tr>
<tr>
<td>$1$</td>
<td>$x + 1$</td>
</tr>
<tr>
<td>$\alpha, \alpha^2, \alpha^4, \alpha^8$</td>
<td>$M_\alpha(x) = x^4 + x + 1$</td>
</tr>
<tr>
<td>$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$</td>
<td>$M_{\alpha^3}(x) = x^4 + x^3 + x^2 + x + 1$</td>
</tr>
<tr>
<td>$\alpha^5, \alpha^{10}$</td>
<td>$M_{\alpha^5}(x) = x^2 + x + 1$</td>
</tr>
<tr>
<td>$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$</td>
<td>$M_{\alpha^7}(x) = x^4 + x^3 + 1$</td>
</tr>
</tbody>
</table>

$$x^{16} - x = x(x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x^3 + 1)$$