Minimal Polynomials

Definition

Let α be an element in $GF(p^e)$. We call the monic polynomial of smallest degree which has coefficients in GF(p) and α as a root, the ***minimal polyonomial*** of α.

Example: We will find the minimal polynomials of all the elements of GF(8).

First of all, the elements 0 and 1 will have minimal polynomials x and x + 1 respectively. We construct GF(8) using the primitive polynomial $x^3 + x + 1$ which has the primitive element λ as a root. There are 4 monic 2^{nd} degree polynomials over GF(2), x^2, $x^2 + 1$, x^2+x, and $x^2+ x +1$. The first three factor and so have roots in GF(2), but these elements have already been taken care of. The last quadratic has no roots in GF(8) – which we can determine by substituting the elements into this polynomial.

Example

Consequently, any other minimal polynomials will have to have degree at least 3. The minimal polynomial of λ is therefore the primitive polynomial $x^3 + x + 1$. This polynomial also has two other roots, λ^2 and λ^4 (which we can determine by substitution of the field elements). The three elements λ^3, λ^6 and λ^5 all satisfy the cubic $x^3 + x^2 + 1$, so it must be the minimal polynomial for these elements.

Element	*Minimal Polynomial*
0	x
1	$x + 1$
λ, λ^2, λ^4	$x^3 + x + 1$
λ^3, λ^6, λ^5	$x^3 + x^2 + 1$

Properties

Theorem 38: Let m(x) be the minimal polynomial of an element α in GF(p^e). Then:

(i) m(x) is irreducible.

(ii) if α is a root of a polynomial f(x) with coefficients in GF(p), then m(x) divides f(x).

(iii) m(x) divides $x^{p^e} - x$.

(iv) if m(x) is primitive, then its degree is e. In any case, the degree of m(x) is $\leq$ e.

Pf: (i) If m(x) is reducible, then m(x) = a(x)b(x), and since m(α) = 0, either a(α) or b(α) is 0 contradicting the fact that m(x) is the polynomial of *smallest* degree having α as a root.

Properties

Theorem 38: Let m(x) be the minimal polynomial of an element α in GF(p^e). Then:

(i) m(x) is irreducible.

(ii) if α is a root of a polynomial f(x) with coefficients in GF(p), then m(x) divides f(x).

(iii) m(x) divides $x^{p^e} - x$.

(iv) if m(x) is primitive, then its degree is e. In any case, the degree of m(x) is $\leq$ e.

Pf: (ii) By division, f(x) = a(x)m(x) + r(x) where the degree of r(x) is less than that of m(x). Since $f(\alpha) = 0$ and $m(\alpha) = 0$ we must have $r(\alpha) = 0$, and since the degree of r(x) is less than that of m(x), we must have that r(x) is identically zero.

(iii) This follows directly from (ii) since every element of GF(p^e) is a root of the polynomial $x^{p^e} - x$.

(iv) Since GF(p^e) is an e-dimensional vector space over GF(p), the elements $1, \alpha, \alpha^2, \ldots \alpha^e$ are linearly dependent and so α satisfies an equation of degree less than or equal to e. If m(x) is primitive then α is a generator and $1, \alpha, \alpha^2, \ldots \alpha^{e-1}$ are linearly independent, so α satisfies no polynomial of degree less than e. ❑

Reciprocal Polynomials

Division of one polynomial by another does not usually result in a polynomial, in particular, polynomials do not have multiplicative inverses that are polynomials. Given a polynomial f(x) of degree n there is a polynomial which has some "inverse like" properties.

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, then the polynomial defined by $x^n f(x^{-1}) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$ is called the ***reciprocal polynomial of f(x)***. [Note that the coefficients come in reverse order].

Example: If $f(x) = 2x^4 + 3x^2 + 5x + 6$, then the reciprocal of f(x) would be $6x^4 + 5x^3 + 3x^2 + 2$.

Example: The reciprocal of $x^3 + x + 1$ is $x^3 + x^2 + 1$.

Reciprocal Polynomials

Theorem 39: If $\alpha \neq 0$ is a root of f(x), α^{-1} is a root of the reciprocal polynomial of f(x). Also, f(x) is irreducible iff its reciprocal polynomial is irreducible, and f(x) is primitive iff its reciprocal polynomial is primitive.

Pf: Suppose that f(x) has degree n, and let $g(x) = x^n f(x^{-1})$ be its reciprocal polynomial. Then, since $f(\alpha) = 0$, $g(\alpha^{-1}) = \alpha^{-n} f(\alpha) = 0$. Suppose that f(x) = a(x)b(x) where the degree of a(x) = i and degree of b(x) = n – i. Then $g(x) = x^n a(x^{-1})b(x^{-1}) = x^i a(x^{-1}) x^{n-i} b(x^{-1})$ which is the product of two polynomials, so g(x) is reducible. On the other hand, if g(x) = a(x)b(x) with degree a(x) + degree b(x) = n, then $g(x) = x^i a(x^{-1})\, x^j b(x^{-1}) = x^n a(x^{-1})b(x^{-1})$, so $f(x^{-1}) = a(x^{-1})b(x^{-1})$ and so f(x) is reducible. Since the order of an element and its inverse are equal, f(x) is primitive iff g(x) is primitive. ❑

Example

In our GF(8) example, we noticed that $x^3 + x + 1$ was the minimal polynomial for λ, λ^2, and λ^4. By the previous theorem, we see that $\lambda^{-1} = \lambda^6$, $\lambda^{-2} = \lambda^5$ and $\lambda^{-4} = \lambda^3$ are all roots of the irreducible (and primitive) polynomial $x^3 + x^2 + 1$, since it is the reciprocal of the original polynomial. Thus, we could have determined that this was the minimal polynomial for them without calculation.

As another observation from this example, recall that the minimal polynomials are irreducible over GF(2) and are divisors of $x^8 - x$. So we have $x^8 - x = x(x+1)(x^3+x+1)(x^3 + x^2 +1)$ as the complete factorization over GF(2). [The degree sum on the right tells us that there are no more factors.]

Automorphisms and Subfields

Consider the field $GF(p^e)$. We know that this field contains as subfields the fields $GF(p^r)$ iff $r|e$. We also know that for any field $GF(p^s)$, the elements of the field are the roots of the equation

$$x^{p^s} - x = 0.$$

Combining these facts we can make the observation that:

An element x of $GF(p^e)$ is in a subfield $GF(p^r)$, where $r|e$, iff

$$x^{p^r} = x,$$

i.e., x is a fixed point of the automorphism $t \rightarrow t^{p^r}$.

Polynomials

Theorem 42: If $f(x)$ is a polynomial with coefficients in $GF(p^r)$, then $f(x^{p^r}) = (f(x))^{p^r}$.

Pf: Let $f(x) = a_0 + a_1 x + \ldots + a_m x^m$. Then

$$f(x^{p^r}) = a_0 + a_1 x^{p^r} + \ldots + a_m (x^m)^{p^r}$$

$$= a_0^{p^r} + a_1^{p^r} x^{p^r} + \ldots + a_m^{p^r} (x^m)^{p^r} \qquad \text{(since } a_i \in GF(p^r)\text{)}$$

$$= (a_0 + a_1 x + \ldots + a_m x^m)^{p^r}$$

(since $t \rightarrow t^{p^r}$ is an automorphism)

Polynomials

As a partial converse of Theorem 42 we have:

Theorem 42*: Let f(x) be a polynomial over $GF(p^e)$ of degree less than p^{e-r}. Then if $f(x^{p^r}) = (f(x))^{p^r}$ the coefficients of f(x) are all in $GF(p^r)$.

Pf: Let $f(x) = a_0 + a_1x + \ldots + a_m x^m$. If $g(x) = f(x^{p^r}) - (f(x))^{p^r}$ is the zero polynomial, then its coefficients $a_i - a_i^{p^r} = 0\ \forall i$, so $a_i \in GF(p^r)\ \forall i$. But, g(x) could have positive degree and still be zero for each value in the field. This can occur only if $x^{p^e}-x$ is a factor of g(x) which implies that the degree of g(x) is at least p^e. However, the assumption on the degree of f implies that the degree of g is less than p^e. ❑

Polynomials

Theorem 43: Let f(x) be a polynomial over GF(p), and let α be a root of f(x) of order n in the multiplicative group of some field F of characteristic p. Let r be the smallest integer so that $p^{r+1} \equiv 1 \bmod n$. Then $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^r}$ are all distinct roots of f(x).

Pf: Since the coefficients of f(x) are in GF(p), each of $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^r}$ are roots of f(x). We need to show that they are distinct.

Suppose that $\alpha^{p^i} = \alpha^{p^j}$ for some i and j with, say $i > j$, then $\alpha^{p^i - p^j} = 1$. Thus $p^i - p^j$ is a multiple of n. Hence, $p^i \equiv p^j \bmod n$ iff $p^{i-j} \equiv 1 \bmod n$, since (p,n) = 1 as n is a divisor of p^e-1, iff i-j is a multiple of r+1 which can not occur if both i and j are less than r+1. ❑

Examples

Consider the field GF($16 = 2^4$). The polynomial $x^4 + x^3 + 1$ has coefficients in GF(2) and is irreducible over that field. Let α be a primitive element of GF(16) which is a root of this polynomial. Since α is primitive, it has order 15 in GF(16)*. Because $2^4 \equiv 1 \mod 15$, we have $r = 3$ and by the last theorem α, α^2, α^{2^2} and α^{2^3} are all roots of this polynomial [and since the degree is 4, these are the only roots].

We can verify this by either "plugging in" each of these values in the polynomial and seeing that the result is 0, or by multiplying out the expression $(x + \alpha)(x + \alpha^2)(x + \alpha^4)(x + \alpha^8)$ to see that we obtain the given polynomial. We will carry out the details of this second approach.

Examples

a
a^2
a^3
$a^4 = a^3 + 1$
$a^5 = a^3 + a + 1$
$a^6 = a^3 + a^2 + a + 1$
$a^7 = a^2 + a + 1$
$a^8 = a^3 + a^2 + a$
$a^9 = a^2 + 1$
$a^{10} = a^3 + a$
$a^{11} = a^3 + a^2 + 1$
$a^{12} = a + 1$
$a^{13} = a^2 + a$
$a^{14} = a^3 + a^2$

$$(x + \alpha)(x + \alpha^2)(x + \alpha^4)(x + \alpha^8) =$$
$$(x^2 + (\alpha + \alpha^2)x + \alpha^3)(x^2 + (\alpha^4 + \alpha^8)x + \alpha^{12}) =$$
$$(x^2 + \alpha^{13}x + \alpha^3)(x^2 + \alpha^7x + \alpha^{12}) =$$
$$x^4+(\alpha^{13}+\alpha^7)x^3+(\alpha^{12}+\alpha^3+\alpha^{20})x^2+(\alpha^{25}+\alpha^{10})x+\alpha^{15} =$$
$$x^4+(\alpha^{13}+\alpha^7)x^3+(\alpha^{12}+\alpha^3+\alpha^5)x^2+(\alpha^{10}+\alpha^{10})x+1 =$$
$$x^4 + x^3 + (\alpha^5+\alpha^5)x^2 + 1 =$$
$$x^4 + x^3 + 1$$

Example

As another example in the same field, notice that since

$$\alpha^{10} + \alpha^5 + 1 = 0,$$

α^5 is a root of the polynomial $x^2 + x + 1$, with coefficients in GF(2). In GF(16)*, α^5 has order 3. Since $2^2 \equiv 1 \bmod 3$, $r = 1$ and the theorem says that α^5 and $(\alpha^5)^2 = \alpha^{10}$ are distinct roots of this polynomial. This can be easily verified since $(\alpha^{10})^2 = \alpha^{20} = \alpha^5$.

Cyclotomic Cosets

The polynomials of the last two examples were minimal polynomials. Let's consider the minimal polynomials of all the non-zero elements of GF(16):

Minimal Polynomial	Powers of α
$x^4 + x^3 + 1$	{1,2,4,8}
$x^4 + x + 1$	{7,14,13,11}
$x^4 + x^3 + x^2 + x + 1$	{3,6,12,9}
$x^2 + x + 1$	{5, 10}
$x + 1$	{0}

The last theorem tells us that the sets of powers of the primitive element which are the roots of a minimal polynomial is closed under multiplication by 2 mod 15. They are called ***cyclotomic cosets***.

Cyclotomic Cosets

More formally, for any integer s, $0 \leq s < p^m - 1$, let r be the smallest integer with the property that $p^{r+1}s \equiv s \bmod (p^m - 1)$. The ***cyclotomic coset*** containing s consists of

$$\{s, ps, p^2s, p^3s, ..., p^rs\}$$

where each p^is is reduced mod (p^m-1).

The cyclotomic cosets partition the integers of $\{0,...,p^m-1\}$. If s is relatively prime to $p^m - 1$, then r = m-1, but if there is a common factor then the sizes of these cosets vary. {0} is always a cyclotomic coset and contains only the one element. If $p^m - 1$ is prime, then all the other cyclotomic cosets will have the same size (m).

Examples

The cyclotomic cosets mod 7 (p = 2) are:

{0}
{1, 2, 4}
{3, 6, 5}

The cyclotomic cosets mod 8 (p = 3) are:

{0}
{1, 3}
{2, 6}
{4}
{5, 7}

Minimal Polynomial Structure

Theorem 44: Let α be an element of $GF(p^e)$ and let $m(x)$ be its minimal polynomial. If β is a primitive element of $GF(p^e)$ and $\alpha = \beta^t$, then $m(x) = \Pi_i (x - \beta^i)$, where i ranges over the cyclotomic coset which contains t.

Proof: The cyclotomic coset which contains t is $\{t, pt, ..., p^r t\}$ where $p^{r+1}t \equiv t \bmod (p^e - 1)$. Thus, $p^{r+1} \equiv 1 \bmod (n)$ where $n = p^e\text{-}1/\gcd(p^e\text{-}1,t)$. But this n is the order of α in $GF(p^e)^*$. Thus, by Thm 43, each $\beta^i = \beta^{p^j t} = \alpha^{p^j}$ as i ranges over the cyclotomic coset containing t is a distinct root of $m(x)$. So, $f(x) = \Pi_i (x - \beta^i)$ divides the minimal polynomial $m(x)$. Now, $f(x^p) = f(x)^p$ since raising to the pth power just permutes the β^i. By Thm 42*, the coefficients of $f(x)$ are in $GF(p)$, so $f(x) = m(x)$. ❑

Remarks

As a consequence of this theorem we see that:

1) The degree of a minimal polynomial is always the size of a cyclotomic coset.

2) Elements α^i and α^j have the same minimal polynomial iff i and j are in the same cyclotomic coset.

Factoring $x^n - 1$

Factoring $x^n - 1$ is important in the construction of cyclic codes. When $n = p^e - 1$, we have some information about the factors since $GF(p^e)$ is the splitting field of $x^{p^e} - x = x(x^{p^e-1} - 1)$. In particular, we know that all the minimal polynomials of the elements of the field will be the factors (irreducible polynomials over GF(p) whose degrees divide e).

We now consider the situation when n does not have this form and we wish to factor $x^n - 1$ over GF(p). To simplify this discussion we will assume that the g.c.d. (n, p) = 1 (if this is not true there will be factors with multiplicity greater than 1). We can extend the definition of cyclotomic cosets to arbitrary integers n. With respect to the prime p, the cyclotomic cosets partition the elements of $\mathbb{Z}_n$.

Example

Thus, with respect to p = 3, the cyclotomic cosets of $\mathbb{Z}_{11}$ are:

{0}
{1, 3, 9, 5, 4}
{2, 6, 7, 10, 8}

while with respect to p = 2 they are:

{0}
{1, 2, 4, 8, 5, 10, 9, 7, 3, 6}.

Given n and p, there is a smallest m so that n divides p^m-1. For this m, we have x^n -1 divides x^{p^m-1} -1, showing that every root of $x^n - 1$ is in GF(p^m). This field will be the smallest field of characteristic p which contains all the roots of $x^n - 1$. These roots form a cyclic subgroup in GF(p^m)*, generated by a ***primitive n^{th} root of unity.***

Theorem 45

Let α be a root of $x^n - 1$ in the smallest finite field F of characteristic p that contains α, and let m(x) be its minimal polynomial. Let β be a primitive n^{th} root of unity in F and let $\alpha = \beta^s$. Then

$$m(x) = \Pi (x - \beta^i)$$

where i varies over the cyclotomic coset of $\mathbb{Z}_n$ with respect to p which contains s.

The proof is similar to that of Theorem 44, so we will not give it.

Example

Consider factoring $x^{11} - 1$ over GF(3). From the cyclotomic coset calculation we have seen, this polynomial will have 3 factors, one of degree 1, namely, (x-1), and 2 of degree 5. Since $11 \mid 3^5 - 1 = 242$, the degree 5 polynomials are minimal polynomials of a primitive 11^{th} root of unity contained in $GF(3^5)$.

If β is an primitive 11^{th} root of unity in $GF(3^5)$, then these polynomials are :

$$(x - \beta)\,(x - \beta^3)(x - \beta^9)\,(x - \beta^5)(x - \beta^4)$$

and

$$(x - \beta^2)(x - \beta^6)(x - \beta^7)(x - \beta^{10})(x - \beta^8).$$

Giving:

$$x^{11}-1 = (x-1)(x^5 + 2x^3 + x^2 + 2x + 2)(x^5 + x^4 + 2x^3 + x^2 + 2)$$