Introduction to Algebra

The basics of finite field algebra are presented in this lecture. We begin with some basic definitions followed by introduction to Galois fields. We conclude with polynomial over Galois fields.

Groups

Let G be a set of elements and * is a binary operation defined on G such that for all elements $a, b \in$ G then $c = a*b \in$ G. We say that the group is closed under operation *. For example, if G is the set of all real numbers, then G is closed under the real addition (+) operation.

Also, the operation is said to be associative if for a, b, c$\in$ G, then (a*b)*c = a*(b*c).

The set G on which the binary operation * is defined is referred to as a group if the following conditions are met:

1) * is associative
2) G contains an identity element. In other words, for $a, e \in$ G, e is an identity element if $a*e = a$ for all a.
3) For any element $a \in$ G, there exists an inverse element $a' \in$ G such that $a*a' = e$.

The group is a commutative group if for any $a, b \in$ G, $a*b = b*a$.

Examples

a) G is the set of all real numbers under multiplication.

1) Multiplication is associative
2) a×1 = a for all a$\in$ G and 1$\in$ G.
3) a×(1/a) = 1 and 1/a$\in$ G.

Furthermore, multiplication is commutative; therefore the set of real numbers is a commutative group under multiplication.

b) G is the set of all positive integers plus 0 under addition

1) Addition is associative
2) a + 0 = a, 0$\in$ G.
3) a + (-a), -a$\notin$ G.

G is not a group under addition.

Theorem 1

The identity element in any group is unique. To prove this, let us assume that there are two identity elements; $e, f \in$ G. Then $f*e = f$ and $e*f = e$. But since $f*e = e*f$, then $f = e$.

Theorem 2

The inverse of a group element is unique. Again, let us assume that for $a \in$ G, there exist two inverses, a' and a''. Then $a' = a' * e$. Also, $e = a * a''$. Therefore $a' = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$. Therefore, this implies that $a' = a''$.

Subgroups

Let G be a group under the binary operation *. Let H be a nonempty subset of G. H is a subgroup of G if the following conditions are met:

1) H is closed under *.
2) For any element $a \in$ H, the inverse of a, $a' \in$ H.

H is a group on its own. Because a'$\in$ H, then e$\in$ H also. Since H is made up of elements in G, the associative condition on * must hold on these elements as well. Since H is a group that consists entirely of elements from G, then H is a subgroup of G.

Example

G is the set of all integers under addition.

1) Addition is associative.
2) a + 0 = a, 0$\in$ G.
3) a + -a = 0, -a$\in$ G

Let H be the set of all even integers under addition

1) An even number added to an even number produces another even number, hence the set is closed
2) a + -a = 0. If a is even, then so is –a, hence -a$\in$ H.

Therefore H is a subgroup of G.

Example 2

Let F be the set of all odd integers. F is a subset of G. Is it a subgroup of G?

1) Addition of two odd numbers produces an even number. Even numbers are not in F, therefore F is not closed under addition. It cannot be a group.
2) We can show that all additive inverses are in F

Since the first condition is not met, F is not a subgroup of G.

Cosets

Let H be a subgroup of a group G under the binary operation *. Let a be any element in G. Then the set of elements a*H which is defined as $\{a*h : h \in \mathrm{H}\}$ is called a left coset of H and the set of elements H*a which is defined as $\{h*a : h \in H\}$ is called a right coset of H.

Example

G = {0, 1, 2, 3, 4, 5} under modulo-6 addition is a group.

Let H = {0, 2, 4}

We can show that H is a group under modulo-6 addition; therefore H is a subgroup of G.

Let $a = 1$

(a+H)mod6 = {1, 3, 5} is a left coset of H. (H + a)mod6 = {1, 3, 5} is a right coset of H. If, for the same a, the left and right cosets are equal, then G must be a commutative group. In this case, we don't refer to cosets as being left or right cosets. They are simply referred to as cosets of H.

(setting a = 2 or 4 produces H}
(setting a = 3 or 5 produces (1+H)mod6)

There are no other distinct cosets of H. Note that H and its coset contain all of the elements in G. In fact, a subgroup of G and its cosets are always disjoint and their union always forms G.

Theorem 3

Let H be a subgroup of G under *. No two elements in a coset of H are identical.

Since a coset of H is defined as a*H, then if h_1, $h_2 \in$ H are distinct elements, then $a*h_1$, $a*h_2 \in$ G. Let $a*h_1 = a*h_2$, then $a'*(a*h_1) = a'*(a*h_2)$. Since * is associative, this means that $(a'*a)*h_1 = (a'*a)*h_2$, or $e*h_1 = h_1 = e*h_2 = h_2$. This implies that for $a*h_1 = a*h_2$, h_1 must equal h_2. Since h_1 and h_2 are different, $a*h_1$ and $a*h_2$ must be different.

Theorem 4

No two elements in different cosets of a subgroup H of a group G are identical.

Let a*H and b*H be two distinct cosets of H, where a, $b \in$ G. Let $a*h_1 \in a$*H and $b*h_2 \in b$*H where h_1, $h_2 \in$ H. Let $a*h_1 = b*h_2$. Therefore $(a*h_1)*h_1' = (b*h_2)*h_1'$. Because of the associative property of G, $a*(h_1*h_1') = b*(h_2*h_1')$. This implies that $a = b*(h_2*h_1')$.

This also means that a*H = $b*(h_2*h1')$*H. Since h_1, $h_2 \in$ H, this means that $h_1' \in$ H. Thus $h_2*h_1' \in$ H. Thus we let $h_2*h_1' = h_3 \in$ H. Therefore a*H = $(b*h_3)$*H. Every element in a*H is determined by $(b*h_3)*h = b*(h_3*h)$. Since h_3, $h \in$ H, then $h_3*h \in$ H. Therefore $b*h_3$*H = b*H. This means that a*H = b*H. However, above we stated that a*H and b*H are distinct cosets. Therefore it is impossible to have distinct cosets with one or more identical elements.

Let G be a group of order n (contains n elements). Let H be a subgroup of G of order m. Then m divides n and G is made up of the union of n/m cosets of H. This fact is a consequence of theorems 3 and 4.

Fields

A field is a set of elements on which we can perform addition, subtraction, multiplication and division without leaving the set. More formally, a field is defined as follows.

Let F be a set of elements on which two binary operations called addition '+' and multiplication '×' are defined. The set is a field under these two operations if the following conditions are satisfied:

1) F is a commutative group under addition. The identity element with respect to addition is called the zero element of F and is denoted by 0.
2) The nonzero elements of F ({F}-0} form a commutative group under multiplication. The multiplicative identity is termed the unity element in F and is denoted by 1.
3) Multiplication is distributive over addition. In other words, for a, b, $c \in$ F, $a\times(b+c) = a\times b + a\times c$.

A finite field contains a finite number of elements. In order for the field to form a group over addition or multiplication, modulo arithmetic must be used.

Properties of fields

1) For every element $a\in$ F, $a\times 0 = 0\times a = 0$.
   $a=a\times 1 = a\times(1+0) = a+a\times 0$. Let $-a$ = additive inverse of a. Then $-a+a = 0 = -a+a+ a\times 0 = 0 + a\times 0 = 0$.
2) For every two non-zero elements a, $b\in$ F, $a\times b \neq 0$.
   This is a direct consequence of the non-zero elements of F being a closed set under multiplication.
3) $a\times b = 0$ for $a\neq 0$ implies $b = 0$. (From properties 1 and 2).
4) For any two elements in a field $-(a \times b) = (-a) \times b = a \times (-b)$.
   $0=0\times b = (a+-a) \times b = a \times b + (-a) \times b$. Therefore $(-a) \times b$ is the additive inverse of $a \times b$. ie $(-a) \times b = -(a \times b)$. Similarly, we can show the same for $-(a \times b) = a \times (-b)$.
5) For $a \neq 0$, $a \times b = a \times c$ implies that $b = c$.

$$a^{-1}\times(a\times b) = a^{-1}\times(a\times c)$$
$$(a^{-1}\times a) \times b = (a^{-1}\times a)\times c$$
$$b = c$$

The set of real numbers is a field under real-number addition and multiplication. This field has an infinite number of elements. Fields with a finite number of elements (finite fields) can be constructed. Addition and multiplication for these fields must be defined.

Galois Field 2 - GF(2): The Binary Field

A binary field can be constructed under modulo-2 addition and modulo-2 multiplication. Modulo-2 addition and multiplication are shown in the tables below:

+	0	1
0	0	1
1	1	0

Modulo-2 Addition

×	0	1
0	0	0
1	0	1

Modulo-2 Multiplication

We can easily check that this field forms a commutative group under addition (ie {0,1} are closed under addition, addition is associative, there is an identity and each element has an inverse. Furthermore, addition is commutative). We can also show that {1} forms a commutative group under multiplication. Also, multiplication distributes over addition.

Galois Field p – GF(p)

Using the same idea as GF(2), we can generate any Galois field with a prime number, p, of elements over modulo-p addition and multiplication. For example, GF(3) would have the following addition and multiplication tables:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Modulo-3 Addition

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Modulo-3 Multiplication

It is not possible to construct finite fields with a nonprime number of elements in this manner. In other words, GF(4) is not a four element field over modulo-4 arithmetic. However, GF(4) can be constructed. We can construct GF(p^m), where m is an integer provided it is an extension field of GF(p).

Characteristic of a field

Consider a finite field of q elements, GF(q). Let $t_k = \sum_{i=1}^{k} 1$. Let λ be the smallest value of k for which t_k = 0. Then λ is called the characteristic of the field GF(q). For example, in GF(2), $\lambda = 2$ (since 1+1 = 0). In GF(3), 1+1+1 = 0, thus $\lambda = 3$.

Theorem 5

The characteristic of a field is always a prime number.

Proof

Suppose that λ is not prime and is equal to the product of two smaller integers k and m. In other words,

$$\sum_{i=1}^{km} 1 = 0 = \sum_{i=1}^{k} 1\left(\sum_{j=1}^{m} 1\right) = \left(\sum_{i=1}^{k} 1\right)\left(\sum_{j=1}^{m} 1\right) = 0$$

which implies that either $\sum_{i=1}^{k} 1$ or $\sum_{j=1}^{m} 1$ is zero. Thus $\lambda = km$ cannot be the characteristic of the field since it is not the smallest number of successive additions of 1 which produces 0. Therefore, λ must be prime.

Order of an element in GF(q)

Suppose α is a nonzero element in GF(q). Since the non-zero elements in a field form a closed set under multiplication, then α^2, α^3, α^4 … are also elements in GF(q). The order of element α in GF(q) is the smallest integer, ord(α), for which $\alpha^{\text{ord}(\alpha)} = 1$.

Example GF(3)

$1^1 = 1$. Therefore ord(1) = 1.
$2^1 = 2$, $2^2 = 1$. Therefore ord(2) = 2.

Theorem 6

Let α be a non-zero element in GF(q). Then $\alpha^{q-1} = 1$.

Proof

Let $a_1, a_2, \ldots a_{q-1}$ be the q-1 non-zero elements in GF(q). Also $\alpha \times a_i$ and $\alpha \times a_j$ are distinct elements in GF(q) for $i \neq j$. Therefore $\alpha \times a_1, \alpha \times a_2, \ldots, \alpha \times a_{q-1}$ also makes up the q-1 non-zero elements in GF(q). Thus

$$\begin{aligned}(\alpha \times a_1) \times (\alpha \times a_2) \times \ldots \times (\alpha \times a_{q-1}) &= a_1 a_2 \ldots a_{q-1} \\ \alpha^{q-1}(a_1 a_2 \ldots a_{q-1}) &= a_1 a_2 \ldots a_{q-1}\end{aligned}$$

Since $a_1 a_2 \ldots a_{q-1}$ must be a non-zero element in GF(q), α^{q-1} must be 1.

Theorem 7

Let α be an element in GF(q). Then ord(α) divides q-1. (ord(α)|q-1)

Proof

Suppose that ord(α) does not divide q-1. Therefore q-1 = $k$ord(α) + r, where $0 < r <$ ord(α).

Then $\alpha^{q-1} = \alpha^{k\text{ord}(\alpha)+r} = \alpha^{k\text{ord}(\alpha)}\alpha^r$. Since $\alpha^{q-1} = 1$ and $\alpha^{k\text{ord}(\alpha)} = 1$, then $\alpha^r = 1$ as well. However, since $r <$ ord(α), α^r cannot equal 1. Thus ord(α) must divide q-1.

Primitive elements

Any element in GF(q) whose order is q-1 is a primitive element in GF(q). For example, in GF(3), element 2 has order 2. Thus 2 is a primitive element in GF(3). Let α be a primitive element in GF(q), then the series $\alpha^1, \alpha^2, \ldots, \alpha^{q-1}$ produces q-1 distinct non-zero elements in GF(q). In other words, the q-1 successive powers of a produce all of the non-zero elements in GF(q). Thus GF(q) = $\{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.

Polynomials over GF(q)

The polynomial $f(X) = f_0 + f_1 X + f_2 X^2 + \ldots + f_n X^n$ is a polynomial of degree n over GF(q) if the coefficients f_i come from GF(q) and obey GF(q) arithmetic.

Suppose $f(X)$ and $g(X)$ are two polynomials over GF(q) and are given by:

$$\begin{aligned} f(X) &= f_o + f_1 X + \ldots + f_n X^n \\ g(X) &= g_o + g_1 X + \ldots + g_m X^m \end{aligned}$$

and $m < n$. Then $f(X) + g(X)$ is given by

$$f(X) + g(X) = (f_o + g_o) + (f_1 + g_1)X + \ldots + (f_m + g_m)X^m + f_{m+1}X^{m+1} + \ldots + f_n X^n$$

where all additions are performed as defined in GF(q).

Also, $f(X)g(X) = c_0 + c_1X + \ldots c_{n+m}X^{n+m}$, where the coefficients are given by:

$$\begin{aligned} c_0 &= f_0 g_0 \\ c_1 &= f_0 g_1 + f_1 g_0 \\ c_2 &= f_0 g_2 + f_1 g_1 + f_2 g_0 \\ \vdots & \;\vdots\; \vdots \\ c_{n+m} &= f_n g_m \end{aligned}$$

Examples

1) Consider the following polynomials over GF(2):

$$\begin{aligned} f(X) &= 1 + X + X^3 \\ g(X) &= 1 + X^2 \end{aligned}$$

Then $f(X)+g(X) = (1+1) + (1+0)X + (0+1)X^2 + (1+0)X^3 = X + X^2 + X^3$ and $f(X)g(X) = (1+X+X^3) \times (1+X^2) = 1 + X^2 + X + X^3 + X^3 + X^5 = 1 + X + X^2 + (1+1)X^3 + X^5 = 1 + X + X^2 + X^5$.

2) Let us consider GF(4) which is the set of elements $\{0, 1, \alpha, \alpha^2\}$ on which addition and multiplication are defined as follows:

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

GF(4) Addition

×	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

GF(4) Multiplication

Consider the two polynomials $f(X)$ and $g(X)$ over GF(4) which are given as:

$$\begin{aligned} f(X) &= 1 + \alpha X + \alpha X^2 \\ g(X) &= 1 + \alpha^2 X \end{aligned}$$

Then $f(X) + g(X) = X + \alpha X^2$ and $f(X)g(X) = 1 + X + \alpha^2 X^2 + X^3$.

It is clear that $f(X)\times 0 = f(X)g(X)|_{g(X)=0}$, therefore $g_i = 0$ and thus $c_i = 0$. Thus $f(X)\times 0 = 0$.

Properties of Polynomials over GF(q)

It can be easily verified that polynomials over GF(q) satisfy the following properties and conditions:

1) Commutative

   $a(X) + b(X) = b(X) + a(X)$
   $a(X)b(X) = b(X)a(X)$

2) Associative

   $a(X) + [b(X) + c(X)] = [a(X) + b(X)] + c(X)$
   $a(X)[b(X)c(X)] = [a(X)b(X)]c(X)$

3) Distributive
   $a(X)[b(X) + c(X)] = a(X)b(X) + a(X)c(X)$

Polynomial Division

When we divide $f(X)$ by $g(X)$, we get two new polynomials; $q(X)$ is the quotient and $r(X)$ is the remainder. The remainder, $r(X)$ has a smaller degree than $g(X)$. Thus:

$$f(X) = q(X)g(X) + r(X)$$

Example

Consider the division of $f(X) = 1 + X^2 + X^5$ by $g(X) = 1 + X^3$ on GF(2). By long division:

$$\begin{array}{r|lllll}
 & X^2 & & +1 & & \\
\cline{2-6}
X^3+1 & X^5 + & & & +X^2 & +1 \\
 & X^5 & & +X^3 & & \\
\cline{2-6}
 & & & X^3 & +X^2 & +1 \\
 & & & X^3 + & & +1 \\
\cline{4-6}
 & & & & X^2 &
\end{array}$$

Therefore $1+X^2+X^5 = (1+X^2)(1+X^3) + X^2$.

When $f(X)$ is divided by $g(X)$ and $r(X) = 0$, then $g(X)$ is a factor of $f(X)$ and we say that $f(X)$ is divisible by $g(X)$. If a polynomial $f(X)$ has no factors other than 1 and itself, then we say that the polynomial is irreducible. Furthermore, any reducible polynomial can be expressed as the multiplication of a group of irreducible polynomials much like any number can be factored into a multiplication of primes. For $f(X)$ on GF(q) and $\beta \in$ GF(q), if $f(\beta) = 0$, then β is a root of $f(X)$ and $f(X)$ is divisible by X-β.

Example

On GF(2), if $f_0 = 0$ for any polynomial, then it is divisible by X. If $f_0 = 1$ and $f(X)$ has an even number of terms, then $f(1) = 0$ and thus $f(X)$ is divisible by X+1. Consider all polynomials of degree 2 where $f_0 = 1$. These are $f_1(X) = 1+X^2$ and $f_2(X) = 1+X+X^2$. $f_1(1) = 0$, thus $f_1(X)/(X+1)$ has no remainder. In fact $1+X^2 = (1+X)(1+X)$. The polynomial $f_2(X)$ has an odd number of terms, thus $f_2(1) = 1$ and $f_2(0) = 0$. Thus it is neither divisible by 1 or X. Any polynomial of degree 2 that is not equal to $f_2(X)$ will have a non-zero remainder, thus $1+X+X^2$ is irreducible in GF(2).

Suppose we define $f(X) = 1+X+X^2$ over GF(4). Then $f(0) = 1$, $f(1) = 1$, $f(\alpha) = 1+\alpha+\alpha^2 = \alpha^2+\alpha^2 = 0$ and $f(\alpha^2) = 1+\alpha^2+(\alpha^2)^2 = 1+\alpha^2+\alpha = 0$. Thus α and α^2 are roots of $1+X+X^2$ in GF(4). Thus $1+X+X^2 = (X-\alpha)(X-\alpha^2) = (X+\alpha)(X+\alpha^2)$.

The conclusion here is that a polynomial that is irreducible in GF(p), might not be irreducible in GF(p^m).

Theorem 8

An irreducible polynomial on GF(p) of degree m divides $X^{p^m-1}-1$.

This will become apparent when we discuss minimal polynomials. A proof of theorem 8 can be found in R.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Boston: Kluwer Academic Publishers, 1988.

Example

We have seen that $1+X+X^2$ is irreducible in GF(2). Therefore according to Theorem 8, it must divide $1+X^3$.

$$
\begin{array}{r|l}
 & X+1 \\
\hline
X^2+X+1 & X^3 \qquad\qquad +1 \\
 & \underline{X^3+X^2+X} \\
 & \quad X^2+X+1 \\
 & \quad \underline{X^2+X+1} \\
 & \qquad\qquad 0
\end{array}
$$

An irreducible polynomial on GF(p), $f(X)$, is said to be primitive if the smallest value of n for which it divides X^n-1 is $n = p^m$-1. In other words, although all irreducible polynomials divide X^n-1 where $n = p^m$-1, some polynomials also divide X^n-1 where $n < p^m$-1. These polynomials are not primitive.

Example

It can be shown that $1+X+X^4$ is irreducible. Because of this, we know that it divides $1+X^{15}$. By exhaustive search, we can show that this polynomial does not divide $1+X^n$ for any value of $n < 15$. Therefore $1+X+X^4$ is primitive.

$1+X+X^2+X^3+X^4$ is also irreducible, and it also divides $1+X^{15}$, however, it also divides $1+X^5$. Therefore it is not primitive.

Theorem 9

An irreducible polynomial of degree m in GF(p) has roots in GF(p^m) that all have the same order. In other words, if $f(X)$ is a polynomial of degree m and is irreducible in GF(p), and if $f(\alpha_1) = f(\alpha_2) = 0$ in GF(p^m), then $\text{ord}(a_1) = \text{ord}(\alpha_2)$.

Proof is long and can be found in S.B. Wicker, *Error Control Systems for Digital Communications and Storage*, Upper Saddle River, NJ: Prentice Hall, 1995.

Theorem 10

Primitive polynomials of degree m in GF(p) have roots in GF(p^m) which have order p^m-1. In other words, if $f(X)$ is primitive in GF(p), and $f(\alpha) = 0$ in GF(p^m), then α has order p^m-1.

Proof

Since $f(X)$ divides $X^{p^m-1}-1$, and α is a root of $f(X)$, then it is also a root of $X^{p^m-1}-1$. In other words, $\alpha^{p^m-1}-1=0$ or $\alpha^{p^m-1}=1$. This means that ord(α) divides p^m-1, or $\alpha^{\text{ord}(\alpha)}-1 = 0$. This in turn implies that all of the roots in $X^{\text{ord}(\alpha)}-1$ are also in $X^{p^m-1}-1$, thus $X^{\text{ord}(\alpha)}-1$ divides $X^{p^m-1}-1$.

Since $f(X)$ is primitive, it must also be irreducible in GF(p). Therefore, all of its roots have the same order, thus all of the roots in $f(X)$ are in $X^{\text{ord}(\alpha)}-1$, thus $f(X)$ divides $X^{\text{ord}(\alpha)}-1$ which divides $X^{p^m-1}-1$, but the smallest value of n for which $f(X)$ divides X^n-1 is $n = p^m-1$, thus ord(α) must equal p^m-1.

If α is a root of $f(X)$ in GF(p^m) and α has order p^m-1, then the series $\alpha, \alpha^2, ..., \alpha^{p^m-1}$ produces all of the non-zero elements of GF(p^m).

Examples

GF(4) as an extension field of GF(2)

$p(X) = 1+X+X^2$ is a primitive polynomial in GF(2)[X] of degree 2. Thus its root in GF(4) has order 2^2-1 = 3. The successive powers of the root of $p(X)$ can then be used to represent the 3 non-zero elements in GF(4).

Let α be the root of $p(X)$. Therefore $p(\alpha) = 0$, or $1+\alpha+\alpha^2 = 0$, which means $\alpha^2 = \alpha+1$. Also, $\alpha^3 = \alpha^2 \times \alpha = (\alpha+1)\alpha = \alpha^2+\alpha = \alpha+1+\alpha = 1$.

Thus GF(4) = $\{0, 1, \alpha, \alpha^2 = \alpha+1\}$. Addition and multiplication over GF(4) is shown on page 7. It is left to the reader to verify that the addition and multiplication tables of page 7 can be obtained using the definition $\alpha^2 = \alpha+1$.

If we consider GF(4) to be binary vectors of length 2 with a 1's position and an α's position, we can show that $0 = 0\alpha+0$, $1 = 0\alpha+1$, $\alpha = 1\alpha+0$ and $\alpha^2 = 1\alpha+1$, or 0 = (0,0), 1 = (0,1), α = (1,0) and a^2 = (1,1). In other words, GF(4) = GF(2^2) is simply two dimensional GF(2).

GF(8) as an extension field of GF(2)

$p(X) = 1+X+X^3$ is a primitive polynomial of degree 3 over GF(2). Therefore its root can be used to describe GF(8).

Let $p(\alpha) = 0$, thus $1+a+\alpha^3 = 0$, or $\alpha^3 = \alpha+1$. Thus the non-zero elements of GF(8) are α, α^2, $\alpha^3 = \alpha+1$, $\alpha^4 = (\alpha+1)\alpha = \alpha^2+\alpha$, $\alpha^5 = (\alpha^2+\alpha)\alpha = \alpha^3+\alpha^2 = \alpha^2+\alpha+1$, $\alpha^6 = \alpha^3+\alpha^2+\alpha = \alpha^2+1$, $\alpha^7 = \alpha^3+\alpha = 1$.

$0 = (0,0,0)$, $1 = (0,0,1)$, $\alpha = (0,1,0)$, $\alpha^2 = (1,0,0)$, $\alpha^3 = (0,1,1)$, $\alpha^4 = (1,1,0)$, $\alpha^5 = (1,1,1)$, $\alpha^6 = (1,0,1)$.

From the above vectors, we can see that, for example, $\alpha+\alpha^6 = \alpha^5$. Also, $\alpha^x = \alpha^{x\bmod(7)}$. For example, $\alpha^6\alpha^2 = \alpha^{8\bmod(7)} = \alpha$.

Minimal Polynomials and Conjugate Elements

A minimal polynomial is defined as follows:

Let a be an element in the field GF(q^m). The minimal polynomial of α with respect to GF(q) is the smallest degree non-zero polynomial $p(X)$ in GF(q)[X] such that $p(\alpha) = 0$ in GF(q^m).

Properties of minimal polynomials

For each element α in GF(q^m) there exists a unique, non-zero polynomial $p(X)$ of minimal degree in GF(q)[X] such that the following are true:

1) $p(\alpha) = 0$
2) The degree of $p(X)$ is less than or equal to m
3) $f(\alpha)=0$ implies that $f(X)$ is a multiple of $p(X)$.
4) $p(X)$ is irreducible in GF(q)[X].

Proof of 1 and 2: Since GF(q^m) is an m-dimensional extension of GF(q), then the $m+1$ elements 1, α, α^2, α^3 … α^m are linearly dependent. Therefore, there exists at least one linear combination in GF(q) of the form $a_0+a_1\alpha+a_2\alpha^2+\ldots a_m\alpha^m = 0$.

Uniqueness: We know that there exists at least one polynomial of minimal degree $p(X)$ such that $p(\alpha) = 0$. Suppose we have another polynomial of the same degree, $g(X)$, such that $g(\alpha) = 0$ that is not equally to $p(X)$. This means $p(X) = g(X) + r(X)$, where $r(X)$ has a smaller degree than $p(X)$ and $g(X)$. Thus $p(\alpha) = 0 = g(\alpha)+r(\alpha)$. But $g(\alpha) = 0$, thus $r(\alpha) = 0$. But this means that a smaller degree polynomial has α as its root, which means that $p(X)$ is not the minimal polynomial of α. Thus $p(X)$ must be unique.

Proof of 3:

Let $f(X) = p(X)g(X) + r(X)$, where the degree of $r(X)$ is less than that of $p(X)$, and $f(\alpha) = 0$. Thus we have $0 = p(\alpha)g(\alpha) + r(\alpha) = 0g(\alpha) + r(\alpha) = r(\alpha) = 0$. Yet $r(X)$ cannot be a non-zero polynomial of degree less than the degree of $p(X)$ while satisfying $r(\alpha) = 0$. Thus $r(X)=0$ and $f(X) = p(X)g(X)$.

Proof of 4: If $p(X) = f(X)g(X)$where $f(X)$ and $g(X)$ have lower degrees than $p(X)$, then $p(\alpha) = 0$ means that either $f(\alpha)$ or $g(\alpha) = 0$, and thus $p(X)$ isn't the minimal polynomial of α. Thus $p(X)$ is irreducible.

Since primitive elements are the roots of primitive polynomials, then primitive polynomials are the minimal polynomials for primitive elements in a Galois field.

Minimal polynomials and their relationship to higher order fields are important to the understanding of cyclic codes.

Conjugates of field elements

Let β be an element in GF(q^m). The conjugates of β with respect to GF(q) are $\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \ldots$

The set made up of an element α and all of its conjugates with respect to GF(q) is called the conjugacy class of α.

Theorem 11

The conjugacy class of $\beta \in$ GF(q^m) with respect to GF(q) contains d elements, where $\beta^{q^d} = \beta$ is the first element in the sequence to repeat and d divides m.

See S.B. Wicker, *Error Control Systems for Digital Communication and Storage,* Upper Saddle River, NJ: Prentice Hall, 1995, pages 55-56 for proof.

Example

Take GF(8) = GF(2^3) on page 11. Let $\beta = \alpha^6$. The conjugacy class of α^6 is α^6, $(\alpha^6)^2 = \alpha^{12\text{mod}7} = \alpha^5$, $(\alpha^6)^4 = ((\alpha^6)^2)^2 = \alpha^{10\text{mod}7} = \alpha^3$, $(\alpha^6)^8 = (((\alpha^6)^2)^2)^2 = (\alpha^3)^2 = \alpha^6$.

Thus the conjugacy class of $\alpha^6 = \{\alpha^3, \alpha^5, \alpha^6\}$. It can be shown that the conjugacy class of α^3 and α^5 is also given by this set.

It is left for the reader to verify that the conjugacy class of $\alpha \in$ GF(8) with respect to GF(2) is $\{\alpha, \alpha^2, \alpha^4\}$, while the conjugacy class of 1 = {1}.

Theorem 12

Let $\beta \in$ GF(q^m) have a minimal polynomial p(X) with respect to GF(q). The roots of p(X) are the conjugates of β with respect to GF(q).

Proof:

If p is a prime, then p divides $\binom{p}{k}$. Thus $\binom{p}{k}\text{mod}p = 0$. Thus we can show that $(\alpha_1 + \alpha_2 + \ldots \alpha_t)^{p^r} = (\alpha_1^{p^r} + \alpha_2^{p^r} + \ldots \alpha_t^{p^r})$. Since $q = p^r$, $p(\beta) = 0$ implies that:

$$\sum_{i=0}^{w} p_i \beta^i = 0 = \left(\sum_{i=0}^{w} p_i \beta^i\right)^q = \sum_{i=0}^{w} p_i \left(\beta^i\right)^q = \sum_{i=0}^{w} p_i \beta^{qi}$$

Therefore, if β is a root of $p(X)$, so is β^q. We can show the same if we replace q in the above equation by q^x. Thus the conjugates of β are also roots of $p(X)$.

Therefore, if $p(X)$ is a minimal polynomial with respect to GF(q) of $\beta \in$ GF(q^m), then:

$$p(X) = \prod_{i=0}^{d-1} (X - \beta^{q^i})$$

Example

The minimal polynomial of α, α^2, and α^4 in GF(8) with respect to GF(2) is $(X+\alpha)(X+\alpha^2)(X+\alpha^4) = X^3+X^2(\alpha+\alpha^2+\alpha^4)+X(\alpha^6+\alpha^5+\alpha^3)+(\alpha^7) = X^3+X+1$.

Factoring X^n-1

The expression X^n-1 has n roots. The roots, β_i, of this expression have order, ord(β_i), which divides n. Specifically, if $n = p^m$-1, then the p^m-1 roots of the expression must have an order that divides p^m-1. The p^m-1 non-zero elements of GF(p^m) all have order which divides p^m-1. Thus the roots of X^n-1 where $n = p^m$-1 are the non-zero elements of GF(p^m). Since each non-zero element in GF(p^m) has a primitive polynomial associated with it, then $X^{p^m-1} - 1$ can be factored into the minimal polynomials of GF(p^m).

Example

X^{15}-1 in GF(2) has 15 roots of order that divides 15. All non-zero elements of GF(16) have order which divides 15. Thus we can factor X^{15}+1 into the minimal polynomials of GF(16).

GF(16) is an extension field of GF(2). One primitive polynomial that we can use to define GF(16) is X^4+X+1. This implies that the primitive element, α, is defined by $\alpha^4 = \alpha+1$.

The conjugacy classes of GF(16) with respect to GF(2) are:
$\{1\}$, $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$, $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$, $\{\alpha^5, \alpha^{10}\}$, $\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$. It can be shown that the elements in these conjugacy classes have order 1, 15, 5, 3 and 15 respectively.

The minimal polynomials for each conjugacy class are:

Conjugacy Class	**Minimal Polynomial**
$\{1\}$	$X+1$
$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$	X^4+X+1
$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$	$X^4+X^3+X^2+X+1$
$\{\alpha^5, \alpha^{10}\}$	X^2+X+1
$\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$	X^4+X^3+1

We can show that $X^{15}+1 = (X+1)(X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1)(X^4+X^3+1)$.

In the general case, X^n-1 has n roots with order that divides n. GF(p^m) has elements with order that divides n if n divides p^m-1. For example, if we wish to factor X^5+1 in GF(2), then we know that GF(16) has elements with order that divides 5. Specifically, the conjugacy class $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$ all have order 5 and the element 1 has order 1 which divides 5. Thus the five roots of X^5+1 in these two conjugacy classes. Thus $X^5+1 = (X+1)(X^4+X^3+X^2+X+1)$.

Example

If we wish to factor X^9+1 in GF(2), we need to find a Galois field, GF(2^m) such that 9 divides 2^m-1. Since 9 divides 63 = 2^6-1, we must go to GF(64) to find elements with order that divides 9. In GF(64), α^7 has order 9. The conjugacy class of α^7 is $\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}\}$, thus all of these elements have order 9. The minimal polynomial associated with this conjugacy class is X^6+X^3+1. In GF(64), α^{21} has order 3. The conjugacy class of α^{21} is $\{\alpha^{21}, \alpha^{42}\}$ which has minimal polynomial X^2+X+1. Finally, the element 1 has order 1 which also divides 9. Therefore, $X^9+1 = (X^6+X^3+1)(X^2+X+1)(X+1)$.

Squaring Polynomials in GF(2)[x]

Let $p(X) = a_0+a_1X+\ldots A_mX^m$, where $a_i \in$ GF(2). Then $p^2(X) = (a_0+a_1X+\ldots A_mX^m)^2 = (a_0)^2 + a_0(a_1X+\ldots A_mX^m) + a_0(a_1X+\ldots A_mX^m) + (a_1X+\ldots A_mX^m)^2$. In GF(2), $(a_i)^2 = a_i$ and $x + x = 0$. Therefore $p^2(X) = a_0 + (a_1X+\ldots A_mX^m)^2$. Furthermore, $(a_1X+\ldots A_mX^m)^2 = (a_1X)^2 + a_1X(a_2X^2+...+a_mX^m) + a_1X(a_2X^2+...+a_mX^m) + (a_2X^2+\ldots a_mX^m)^2 = a_1X^2 + (a_2X^2+\ldots a_mX^m)^2$. Therefore, by induction, $p^2(X) = a_0 + a_1\mathrm{X}^2 + a_2X^4 + \ldots\ a_mX^{2m}$.

Suppose we wish to factor X^6+1 in GF(2). The roots of this polynomial must divide 6. However 6 does not divide 2^m-1 for any m. Therefore, the roots of X^6+1 must have order 3, 2 or1. From the above discussion, we know that $(X^3+1)^2 = X^6+1$. We can factor X^3+1 by employing the three non-zero elements of GF(4). Thus $X^3+1 = (X+1)(X^2+X+1)$ and consequently, $X^6+1 = (X+1)^2(X^2+X+1)^2$.