Introduction to Algebra

Def 2.0 (G , $*$) G: a set
A binary operation $*$ on G : $a * b \in G \ \forall a,b \in G$

(G is closed under the operation $*$)

Def 2.1 Group : (G, $*$)

(i) $a*(b*c) = (a*b)*c$ associative

(ii) $\exists\ e \in G$ s.t. $\forall\ a \in G,\ a*e = e*a = a$ e: identity element of G

(iii) $\forall\ a \in G, \exists\ a' \in G$ s.t. $a*a' = a'*a = e$ a': inverse of a

Communicative group : (iv) $\forall\ a, b \in G,\ a*b = b*a$

Thm 2.1 identity element is unique

pf: $e' = e' * e = e$

Thm 2.2 inverse is unique

pf: suppose a' & a'' are inverse of a

$a' = a'*e = a'*(a*a'') = (a'*a)*a'' = e*a'' = a''$

Examples: communicative group

1. (Z , +) e = 0 i -i
2. (Q-{0} , ·) e = 1 b/a a/b
3. (G={0,1} , $\oplus$)

Infinite group

finite group

order of the group : the number of elements in a group

4. additive group

(G={0,1,2, ... ,m-1} , $\boxplus$) , where $m \in Z^+$, $i \boxplus j \equiv i + j \bmod m$

Q: (i) $(i \boxplus j) \boxplus k = i \boxplus (j \boxplus k)$
(ii) e = 0
(iii) $\forall\ 0 < i < m$ m – i is an inverse of i
(iv) $i \boxplus j = j \boxplus i$

5. multiplicative group

(G = { 1,2,3, … ,p-1} , $\boxdot$) p : prime

i $\boxdot$ j ≡ i · j mod p

Pf:

(iii) Let i ∈ G (<p) ∵ p is a prime ∴ (i , p) = 1

Q: ∴ ∃ a, b ∈ Z s.t. a·i + b·p = 1 & (a, p) = 1 (Euclid's theorem)

⇒ a·i = -b·p + 1

(1) if 0 < a < p i.e. a ∈ G ∴ a $\boxdot$ i = i $\boxdot$ a = 1

(2) if a ∉ G, say a = q·p + r ∵(a, p) = 1 ∴r ≠ 0

⇒ r · i = -(b + q·i)p + 1 ∴ r $\boxdot$ i = i $\boxdot$ r = 1

H is said to be a subgroup of G if

(i) H ⊂ G & H ≠ Ø

(ii) H is closed under the group operation of G & satisfies all the conditions of a group

Q: Ref. pp. 29-31

(解讀standard array)

e.g. G = (Q, +)

H = (Z, +)

⇒ Z is a subgroup of Q under the operation "+"

Def 2.2 Field : (F, +, ·)

(i) (F, +) F is a communicative group under "+"

(ii) (F-{0}, ·) F-{0} is a communicative group under "·"

(iii) "·" is distributive over "+"

i.e. a · (b + c) = a · b + a · c ∀a, b, c ∈ F

Q: Does it imply (a + b) · c = a · c + b · c

pf: ∵(a + b) · c = c · (a + b) = c · a + c · b = a · c + b · c

(1) order of the field : # of elements in a field

(2) finite field : order is finite

(3) a – b ≡ a + (-b) -b : additive inverse of b

a ÷ b ≡ a · b^{-1} b^{-1} : multiplicative inverse of b

(4) ∀ a ∈ F, a · 0 = 0 · a = 0

pf: a = a · 1 = a · (1 + 0) = a + a · 0

➔ -a + a = -a + a + a · 0 ➔ 0 = 0 + a · 0 = a · 0

(5) ∀ a, b ∈ F & a, b ≠ 0 ⇒ a · b ≠ 0

pf: if a · b = 0

then (a^{-1} · a) · b= a^{-1} · 0 ➔ b = 0 (→←)

(6) $a \cdot b = 0$ & $a \neq 0$ imply that $b = 0$

(7) $\forall\ a, b \in F$, $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

pf: $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$

(8) For $a \neq 0$, $a \cdot b = a \cdot c$ imply that $b = c$

pf: 兩邊乘上a^{-1} $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$

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

Examples:

1. $(R, +, \cdot)$
2. $(F=\{0, 1\}, \boxplus, \boxdot)$ binary field GF(2)
3. $(F=\{0, 1, 2, \ldots, p-1\}, \boxplus, \boxdot)$ prime field GF(p) p : prime

* In a field, we can do the operations + - × ÷ in a manner similar to ordinary arithmetic

4. extension field of GF(p) : $GF(p^m)$ $m \in Z^+$

Q: the order of any finite field is a power of a prime

* finite fields are also called Galois fields

- Next, consider a finite field of q elements, GF(q).

(9) 1 : unit element in GF(q)

$$\text{If } \sum_{i=1}^{m} 1 = \sum_{i=1}^{n} 1 \ \ (n > m) \text{ then } \sum_{i=1}^{n-m} 1 = 0$$

Characteristic (λ) of the field GF(q) :

$$\text{smallest } \lambda \in Z^+ \ \text{ s.t. } \sum_{i=1}^{\lambda} 1 = 0$$

e.g. n = 4, m = 2
1+1+1+1 = 1+1
兩邊加 "1" 之 inverse "-1"
(-1+1)+1+1+1 = (-1+1)+1
0+1+1+1 = 0+1
1+1+1 = 1
…
1+1 = 0

Q: e.g. For GF(P), P:prime, λ= P

(10) λ is prime

pf: suppose not $\lambda = km,\ k, m \in Z^+$

$$\left(\sum_{i=1}^{k} 1\right) \bullet \left(\sum_{i=1}^{m} 1\right) = \sum_{i=1}^{km} 1 \in F. \text{ Since } \sum_{i=1}^{km} 1 = 0, \text{then}$$

$$\text{either } \sum_{i=1}^{k} 1 = 0 \text{ or } \sum_{i=1}^{m} 1 = 0 \ (\rightarrow\leftarrow)$$

(11) $\sum_{i=1}^{k} 1 \neq \sum_{i=1}^{m} 1$ for any $k, m < \lambda$ & $k \neq m$

pf : suppose $\sum_{i=1}^{k} 1 = \sum_{i=1}^{m} 1 \Rightarrow \sum_{i=1}^{m-k} 1 = 0$ (if $m > k$)

$\because m - k < \lambda \rightarrow\leftarrow$

(12) $1 = \sum_{i=1}^{1} 1, \sum_{i=1}^{2} 1, \ldots, \sum_{i=1}^{\lambda-1} 1, \sum_{i=1}^{\lambda} 1 = 0$ GF(λ)

Q: GF(λ) is called a subfield of GF(q)

(13) For any finite field GF(q) if λ ≠ q then q is a power of λ

Q: proof

- Let a be a nonzero element in GF(q).

a′ = a, a^2 = a·a, a^3 = a·a·a, … a: nonzero elements of GF(q)
Since finite field, so $a^k = a^m$ suppose m > k
a^{-k}(≡ $(a^{-1})^k$) is the multiplicative inverse of a^k
[$(a^{-1} \cdot a^{-1}) \cdot (a \cdot a) = a^{-1} \cdot 1 \cdot a = a^{-1} \cdot a = 1$]
∴ $1 = a^{m-k}$ [$a^3 \cdot a^{-2} = a \cdot a \cdot a \cdot a^{-1} \cdot a^{-1} = a = a^{3-2}$]

order of the field element a : smallest Z^+ n, s.t. $a^n = 1$.

Thm { $a^1, a^2, \ldots, a^{n-1}, a^n = 1$ } : form a group under the multiplication of GF(q)

Q: $a^i \neq a^j$

pf: (ii) unit element : 1
考慮 $a^i \cdot a^j$
(1) $i + j \leq n$ $a^i \cdot a^j = a^{i+j}$
(2) $i + j > n$, say $i + j = n + r$ $0 < r \leq n$
$a^i \cdot a^j = a^{i+j} = a^n \cdot a^r = a^r$

closed

(iii) For $1 \leq i \leq n$ a^{n-i} is the multiplicative inverse of a^i

* A group is said to be cyclic if there exists an element in the group whose powers constitute the whole group

Thm 2.4 $a \in GF(q)$ & $a \neq$ zero element. Then $a^{q-1} = 1$

pf: let $b_1\ b_2 \ldots b_{q-1}$ be the q-1 nonzero elements
$\therefore a \cdot b_1, a \cdot b_2, \ldots, a \cdot b_{q-1}$ are nonzero & distinct
$(a \cdot b_1) \cdot (a \cdot b_2) \ldots (a \cdot b_{q-1}) = b_1 \cdot b_2 \ldots \cdot b_{q-1}$
$a^{q-1} \cdot (b_1 \cdot b_2 \ldots \cdot b_{q-1}) = b_1 \cdot b_2 \ldots \cdot b_{q-1}$
$\because (b_1 \cdot b_2 \ldots \cdot b_{q-1}) \neq 0 \rightarrow \therefore a^{q-1} = 1$

If $a \cdot b_i = a \cdot b_j$ Then $b_i = b_j$ ⨯

Thm 2.5 $a \in GF(q)$ $a \neq 0$ if n is the order of a, then $n \mid q-1$

pf: Suppose not $q-1 = kn + r$ $0 < r < n$
$a^{q-1} = a^{kn+r} = a^{kn} \cdot a^r = (a^n)^k \cdot a^r$
$\because a^{q-1} = 1$ & $a^n = 1$ $\therefore a^r = 1$ ⨯

* In GF(q), a nonzero element a is said to be primitive if the order of a q-1

Thm: Every finite field has a primitive element Q: proof

e.g. GF(7)
$3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$
3 : primitive element
$4^1 = 4, 4^2 = 2, 4^3 = 1$ order of "4" is 3 $\Rightarrow$ 3| 7-1

Binary Field Arithmetic

Let $f(x) = \sum_{i=1}^{n} f_i x^i$ and $g(x) = \sum_{j=0}^{m} f_j x^j$, where $f_i, f_j \in GF(2)$

$f(x) \boxplus g(x) \equiv f(x)+g(x)$ modulo 2 (相加後係數再 mod 2)

$f(x) \odot g(x) \equiv f(x) \cdot g(x)$ modulo 2

Q: Is it a field? No
$(GF(2)[x], \boxplus, \odot)$
or $Z_2[x]$

(i) $f(x) \odot 0 = 0$

(ii) f(x) said to be irreducible if it is not divisible by any polynomial over GF(2) of degree less than *n* but greater than zero.

e.g. x^2 , x^2+1, x^2+x are reducible over GF(2)
$x+1$, x^2+x+1, x^3+x+1 are irreducible over GF(2)

e.g. $x^3 - 2$ is irreducible over Q
$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ *over* R
$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$ *over* C, where
$\omega = e^{2i\pi/3} = -(1/2) + (i\sqrt{3}/2)$ satisfies $\omega^3 = 1$.

e.g. $x^4+3x^3+2x+4 = (x+4)^3(x+1)$ over Z_5

non-binary field

Thm: In GF(2)[x], $\forall m \geq 1$, $\exists$ an irreducible polynomial of degree m

pf: exercise

Thm 2.6 Any irreducible polynomial over GF(2) of degree *m* divides $x^{2^m-1}+1$

pf: exercise

e.g. $x^3 + x + 1 \mid x^7+1$ i.e. $x^7+1 = (x^4 + x^2 + x + 1)(x^3 + x + 1)$

*An irreducible polynomial p(x) of degree m is said to be primitive if the smallest positive integer n for which p(x) divides $x^n + 1$ is $n = 2^m - 1$

i.e. $p(x) \mid x^{2^m-1}+1$

e.g. $x^4 + x + 1 \mid x^{15} + 1$ $\quad x^4 + x^3 + x^2 + x + 1 \mid x^5 + 1$

primitive non-primitive

* For a given m, there may be more than one primitive polynomial of degree m.

$$Thm: \forall l \geq 0 \ \ [f(x)]^{2^l} = f(x^{2^l}), \text{ where } f(x) \in GF(2)[x]$$

pf: $f^2(x) = (f_0 + f_1x + \ldots + f_nx^n)^2$

$= [f_0 + (f_1x + f_2x^2 + \ldots + f_nx^n)]^2$

$= f_0^2 + (f_1x + f_2x^2 + \ldots + f_nx^n)^2$

$\vdots$

$\because f_i \in 0 \text{ or } 1$ $\quad = f_0^2 + (f_1x)^2 + (f_2x^2)^2 + \ldots + (f_nx^n)^2$

$\therefore f_i^2 = f_i$ $\quad = f_0 + f_1(x^2)^1 + f_2(x^2)^2 + \ldots + f_n(x^2)^n = f(x^2)$

Construction of Galois Field GF(2^m), m > 1

Initially, we have two elements 0 and 1, from GF(2) and a new symbol α, and define a multiplication "$\cdot$" as follows

(i) $0\cdot0=0 \quad 0\cdot1=1\cdot0=0 \quad 1\cdot1=1$
$0\cdot\alpha=\alpha\cdot0=0 \quad 1\cdot\alpha=\alpha\cdot1=\alpha$

(ii) $\alpha^2=\alpha\cdot\alpha \quad \alpha^3=\alpha\cdot\alpha\cdot\alpha \ldots \alpha^j=\alpha\cdot\alpha\cdot\ldots\cdot\alpha$(j times)

(iii) $F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^j, \ldots\}$

(1) Let p(x) be a primitive polynomial of degree m over GF(2)

(2) assume that $p(\alpha) = 0$

$\because P(x) \mid x^{2^m-1}+1$ (by Thm 2.6)

$\therefore x^{2^m-1} + 1 = q(x)p(x)$

➔ $\alpha^{2^m-1} + 1 = q(\alpha)p(\alpha) = q(\alpha)\cdot0 = 0$ (zero polynomial)

➔ 兩邊加1 (mod 2)

➔ $\alpha^{2^m-1} = 1$

$F^* = \{ 0, 1(\equiv \alpha^0), \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$

(A) Commutative group under "$\cdot$"

(1) Closed

let $0 \le i, j < 2^m - 1$

(i) $i + j < 2^m - 1 \quad \alpha^i\cdot\alpha^j = \alpha^{i+j} \in F^*$

(ii) $i + j \ge 2^m - 1 \quad i + j = (2^m - 1) + r \quad 0 \le r < 2^m-1$

$\therefore \alpha^i \cdot \alpha^j = \alpha^{2^m-1} \cdot \alpha^r = \alpha^r \in F^*$

(2) 1 : unit element

(3) "$\cdot$" is communicative & associative

(4) $\forall\ 0 < i < 2^m-1$, α^{2^m-i-1} is the multiplicative inverse of α^i

$(F^*-\{0\}, \cdot)$ commutative group under "$\cdot$" with order $2^m - 1$

Q: 證$\alpha^i \ne \alpha^j \quad 0 \le i \ne j < 2^m - 1$

(B) Commutative group under "+"

For $0 \le i < 2^m-1$, we have $x^i = q_i(x)p(x) + a_i(x)$ ----- (*)
where $a_i(x) = a_{i0} + a_{i1}x + a_{i2}x^2 + \dots + a_{i,m-1}x^{m-1}$
$\because (x, p(x)) = 1 \therefore a_i(x) \neq 0$

* $a_i(x) \neq a_j(x)$ $0 \le i \neq j < 2^m - 1$

pf: suppose $a_i(x) = a_j(x)$
$x^i + x^j = [q_i(x) + q_j(x)]p(x) + \underbrace{a_i(x) + a_j(x)}_{=0}$
$\therefore p(x) \mid x^i + x^j = x^i(1 + x^{j-i})$ (assume $j > i$)
$\because (p(x), x^i) = 1 \therefore p(x) \mid 1 + x^{j-i}$ $\rightarrow\leftarrow$ $\because j - i < 2^m - 1$

$\Rightarrow$ We have 2^m-1 distinct nonzero polynomials $a_i(x)$ of degree m-1 or less.

Replace x by α in equation (*), we have ($\because p(\alpha)=0$)
(1) $\alpha^i = a_i(\alpha) = a_{i0} + a_{i1}\alpha + a_{i2}\alpha^2 + \dots + a_{i,m-1}\alpha^{m-1}$, $0 \le i \le 2^m - 2$
(2) 0 用 zero polynomial 表示

Define (i) $0 + 0 = 0$
(ii) $0 + \alpha^i = \alpha^i + 0 = \alpha^i$
(iii) $\alpha^i + \alpha^j \in F^*$, $0 \le i, j < 2^m - 1$: 一般多項式相加，係數取module 2

$(F^*, +)$ commutative group under "+"

(C) polynomial multiplication satisfies distribution law
$a(x) \cdot [b(x)+c(x)] = [a(x) \cdot b(x)] + [a(x) \cdot c(x)]$

$\Rightarrow$ F^* : a Galois field of 2^m element, $GF(2^m)$

GF(2^4), p(x) = 1 + x + x^4 ($p(\alpha) = 1 + \alpha + \alpha^4 = 0$)

Power representation	Polynomial representation	4-Tuple representation	Decimal representation
0	0	(0 0 0 0)	0
1	1	(1 0 0 0)	8
α	α	(0 1 0 0)	4
α^2	α^2	(0 0 1 0)	2
α^3	α^3	(0 0 0 1)	1
α^4	1+α	(1 1 0 0)	12
α^5	$\alpha+\alpha^2$	(0 1 1 0)	6
α^6	$\alpha^2+\alpha^3$	(0 0 1 1)	3
α^7	$1+\alpha+\alpha^3$	(1 1 0 1)	13
α^8	$1+\alpha^2$	(1 0 1 0)	10
α^9	$\alpha+\alpha^3$	(0 1 0 1)	5
α^{10}	$1+\alpha+\alpha^2$	(1 1 1 0)	14
α^{11}	$\alpha+\alpha^2+\alpha^3$	(0 1 1 1)	7
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	(1 1 1 1)	15
α^{13}	$1+\alpha^2+\alpha^3$	(1 0 1 1)	11
α^{14}	$1+\alpha^3$	(1 0 0 1)	9

$\alpha^{15} = 1$

$$\alpha^7 = \alpha\alpha^6 = \alpha(\alpha^2+\alpha^3) = \alpha^3+\alpha^4 = \alpha^3+1+\alpha$$

係數相加後mod 2

modulo

GF(2)[α]

$\alpha^4+\alpha+1$

$\alpha\ \alpha^2\ \alpha^4\ \alpha^8\ \alpha^{16} \equiv \alpha$

$\alpha^3\ \alpha^6\ \alpha^{12}\ \alpha^{24}\ \alpha^{48} \equiv \alpha^3$

$\equiv \alpha^9$

Table 7.1 Representations of GF(2^4). $p(z) = z^4 + z + 1$

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	0000	0	x
α^0	1	0001	1	x + 1
α^1	z	0010	2	$x^4 + x + 1$
α^2	z^2	0100	4	$x^4 + x + 1$
α^3	z^3	1000	8	$x^4 + x^3 + x^2 + x + 1$
α^4	z + 1	0011	3	$x^4 + x + 1$
α^5	$z^2 + z$	0110	6	$x^2 + x + 1$
α^6	$z^3 + z^2$	1100	12	$x^4 + x^3 + x^2 + x + 1$
α^7	$z^3 + z + 1$	1011	11	$x^4 + x^3 + 1$
α^8	$z^2 + 1$	0101	5	$x^4 + x + 1$
α^9	$z^3 + z$	1010	10	$x^4 + x^3 + x^2 + x + 1$
α^{10}	$z^2 + z + 1$	0111	7	$x^2 + x + 1$
α^{11}	$z^3 + z^2 + z + 1$	1110	14	$x^4 + x^3 + 1$
α^{12}	$z^3 + z^2 + z + 1$	1111	15	$x^4 + x^3 + x^2 + x + 1$
α^{13}	$z^3 + z^2 + 1$	1101	13	$x^4 + x^3 + 1$
α^{14}	$z^3 + 1$	1001	9	$x^4 + x^3 + 1$

係數相加相乘在數系GF(2)上

GF(2)

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

GF(3)

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

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

GF(2)[α]

$\alpha^2+\alpha+1$

Primitive polynomial over GF(2)

GF(4)

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

*	0	1	2	3
0	0	0	0	0
1	0	3	1	2
2	0	1	2	3
3	0	2	3	1

GF(2^2), p(x) = 1 + x + x^2

($p(\alpha) = 1 + \alpha + \alpha^2 = 0$)

0	0	00	0
1	1	10	2
α	α	01	1
α^2	1+ α	11	3

$\alpha^3 = 1$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

GF(4) →

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

0	0	0	0
1	0	1	1
2	1	0	α
3	1	1	α+1

$\equiv GF(2)[\alpha]/\alpha^2+\alpha+1$

Primitive polynomial over GF(4)

$GF(4^2) \equiv GF(4)[z]/z^2+z+2$, $p(z) = z^2+z+2$

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	00	0	
α^0	1	01	1	x + 1
α^1	z	10	4	x^2 + x + 2
α^2	z + 2	12	6	x^2 + x + 3
α^3	3z + 2	32	14	x^2 + 3x + 1
α^4	z + 1	11	5	x^2 + x + 2
α^5	2	02	2	x + 2
α^6	2z	20	8	x^2 +2x + 1
α^7	2z + 3	23	11	x^2 + 2x + 2
α^8	z + 3	13	7	x^2 + x + 3
α^9	2z + 2	22	10	x^2 + 2x + 1
α^{10}	3	03	3	x + 3
α^{11}	3z	30	12	x^2 + 3x + 3
α^{12}	3z + 1	31	13	x^2 + 3x + 1
α^{13}	2z + 1	21	9	x^2 + 2x + 2
α^{14}	3z + 3	33	15	x^2 + 3x + 3

係數相加
相乘在數系
GF(4)上

α = z

$\alpha^{15} = 1$

Basic properties of Galois Field $GF(2^m)$

In $GF(2)$ $x^4 + x^3 + 1$: irreducible
In $GF(2^4)$ $x^4 + x^3 + 1 = (x + \alpha^7)(x + \alpha^{11})(x + \alpha^{13})(x + \alpha^{14})$

In **R** $x^2 + 1$無根
C $x^2 + 1$ 有 $\pm i$ 根

Thm 2.7 $f(x) \in GF(2)[x]$ let β be an element in an extension field of $GF(2)$. If β is a root of $f(x)$, then for any $l \geq 0$, β^{2^l} is also a root of $f(x)$.

pf: $f(\beta) = 0$
$\because [f(x)]^{2^l} = f(x^{2^l}) \quad \therefore f(\beta^{2^l}) = [f(\beta)]^{2^l} = 0$

- β^{2^l} is called a conjugate of β
- In $GF(2^4)$, α^7 $(\alpha^7)^2 = \alpha^{14}$ $(\alpha^7)^{2^2} = \alpha^{13}$ $(\alpha^7)^{2^3} = \alpha^{11}$ $(\alpha^7)^{2^4} = \alpha^7$
- Let $\beta \in GF(2^m)$ & $\beta \neq 0$ By Thm 2.4 $\beta^{2^m-1} = 1$
  $\therefore \beta^{2^m-1} + 1 = 0$ in $GF(2^m)$, i.e. β is a root of $x^{2^m-1} + 1$.

Thm 2.8 The $2^m - 1$ nonzero element of $GF(2^m)$ form all the roots of $x^{2^m-1} + 1$

Cor. 2.8.1 The elements of $GF(2^m)$ form all the roots of $x^{2^m} + x$ ($\because$ 0 is the root of x)

$\varphi(x)$: minimal polynomial of β, the polynomial of smallest degree over $GF(2)$ s.t. $\varphi(\beta) = 0$ Q : $\varphi(x)$ is unique

Thm 2.9 $\varphi(x)$ is irreducible
pf : $\varphi(x) = \varphi_1(x)\varphi_2(x)$ $\because \varphi(\beta) = 0 \therefore$ either $\varphi_1(\beta) = 0$ or $\varphi_2(\beta) = 0$ ($\rightarrow\leftarrow$)

Thm 2.10 $f(x) \in GF(2)[x]$ if β is also a root of $f(x)$ then $\varphi(x) \mid f(x)$
pf : $f(x) = a(x)\varphi(x) + r(x)$
$\because f(\beta) = \varphi(\beta) = 0 \therefore r(\beta) = 0$ ➔ if $r(x) \neq 0$ ($\rightarrow\leftarrow$) $\therefore r(x) = 0$

Thm 2.11 $\varphi(x) \mid x^{2^m} + x$
pf : By Cor 2.8.1 & Thm 2.10
⇒ (1) all the roots of $\varphi(x)$ are from $GF(2^m)$
(2) what are the roots of $\varphi(x)$?

Thm 2.12 Let $f(x)$ be an irreducible polynomial aver $GF(2)$
if $f(\beta) = 0$ then $\varphi(x) = f(x)$
pf : By Thm 2.10 $\varphi(x) \mid f(x)$ $\because \varphi(x) \neq 1$ & $f(x)$ is irreducible $\therefore \varphi(x) = f(x)$

By Thm 2.7 $\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^l}, \ldots$ are roots of $\varphi(x)$
Let e be the smallest integer, s.t. $\beta^{2^e} = \beta$
Q : Then $\beta^{2^1}, \beta^{2^2}, \ldots, \beta^{2^{e-1}}$ are all the distinct conjugates of β
$\because \beta^{2^m} = \beta \therefore e \leq m$

Thm 2.13 $f(x) = \prod_{i=0}^{e-1}\left(x+\beta^{2^i}\right)$ is irreducible over GF(2)

pf:

$$(1)\left[f(x)\right]^2 = \left[\prod_{i=0}^{e-1}\left(x+\beta^{2^i}\right)\right]^2 = \prod_{i=0}^{e-1}\left(x+\beta^{2^i}\right)^2 \because \left(x+\beta^{2^i}\right)^2 = x^2+\beta^{2^{i+1}}$$

$$\therefore \left[f(x)\right]^2 = \prod_{i=0}^{e-1}\left(x^2+\beta^{2^{i+1}}\right) = \prod_{i=1}^{e}\left(x^2+\beta^{2^i}\right)$$

$$= \left[\prod_{i=1}^{e-1}\left(x^2+\beta^{2^i}\right)\right]\left(x^2+\beta^{2^e}\right) \overset{\because \beta^{2^e}=\beta}{=} \prod_{i=0}^{e-1}\left(x^2+\beta^{2^i}\right) = f\left(x^2\right) \quad (*)$$

Let $f(x) = f_0 + f_1 x + \ldots + f_e x^e$ where $f_0 = 1$ ⟵ $f_i \in GF(2^4)$

$$\left[f(x)\right]^2 = \sum_{i=0}^{e} f_i^2 x^{2i} + (1+1)\sum_{i=0}^{e}\sum_{\substack{j=0 \\ i\neq j}}^{e} f_i f_j x^{i+j} = \sum_{i=0}^{e} f_i^2 x^{2i} \quad (**)$$

By $(*)$ & $(**)$ $\sum_{i=0}^{e} f_i x^{2i} = \sum_{i=0}^{e} f_i^2 x^{2i}$ $\therefore$ for $0 \le i \le e$ we have $f_i = f_i^2$

$\Rightarrow f_i = 0$ or 1

(2) suppose f(x) (=a(x)b(x)) is not irreducible over GF(2) $\therefore$ f(x) ∈ GF(2)[x]

$\because$ f(β) = 0 $\Rightarrow$ a(β) = 0 $\Rightarrow$ a(x) has β β^2 ... $\beta^{2^{e-1}}$ as roots

$\therefore$ deg[a(x)] = e & a(x)=f(x)

or b(β) = 0 $\Rightarrow$ similarly, b(x) = f(x)

$\therefore$ f(x) must be irreducible

Thm 2.14 Let e be the smallest integer, s.t. $\beta^{2^e} = \beta$ Then $\phi(x) = \prod_{i=0}^{e-1}(x+\beta^{2^i})$

Pf : By Thm 2.12 & 2.13

Thm 2.15 Let e be the degree of φ(x).

Then e is the smallest integer s.t. $\beta^{2^e} = \beta$, moreover e ≤ m

Pf: direct consequence of Thm 2.14.

Minimal polynomials of the elements in GF(2^4) generated by p(x)=x^4+x+1

Conjugate roots	minimal polynomials
0	x
1	x+1
$\alpha, \alpha^2, \alpha^4, \alpha^8$	x^4+x+1
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$x^4+x^3+x^2+x+1$
α^5, α^{10}	x^2+x+1
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	x^4+x^3+1

e.g. $X^{15}+1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$ over GF(2)

$X^{15}+1 = (x+\alpha^0)$ $\underline{(x+\alpha^5)(x+\alpha^{10})}$ $\underline{(x+\alpha^1)(x+\alpha^2)(x+\alpha^4)(x+\alpha^8)}$ over GF(2^4)

$\alpha^{15} = 1$ $\underline{(x+\alpha^7)(x+\alpha^{14})(x+\alpha^{13})(x+\alpha^{11})}$ $\underline{(x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^9)}$

Q: 1. The degree of the minimal polynomial of any element in GF(2^m) divides m

2. In pp.14 (1) $\alpha^i \neq \alpha^j$

(2) α is a primitive element

pf : if $\alpha^i = \alpha^j$, $i \neq j$, $j > i$, $1 \leq i, j < 2^m - 1$

$\Rightarrow \alpha^{j-i} = 1$

ie. $\exists\ n = j - i < 2^m - 1$ s.t. $\alpha^n + 1 = 0$

$\Rightarrow x^n + 1 = q(x)p(x) + r(x)$

$\Rightarrow \alpha^n + 1 = q(\alpha)p(\alpha) + r(\alpha)$

$\because \alpha^n + 1 = 0$ & $p(\alpha) = 0$ $\therefore r(\alpha) = 0$

x以α替代

i.e. $p(\alpha) \mid \alpha^n + 1$

i.e. $p(x) \mid x^n + 1$ ($\rightarrow\leftarrow$)

$\because p(x)$ is primitive

α以x替代

Q : primitive polynomial & minimal polynomial 關係?

Q :
(1) For degree *m* primitive polynomial is not unique
(2) For α, the minimal polynomial of α is unique
(3) If α is primitive, the minimal polynomial of α is primitive

∗ Let n be the order of α^{2^l}, $l > 0$, by Thm 2.5, $n \mid 2^m - 1$ --- (1)

In GF(2^m) i.e. $(\alpha^{2^l})^n = \alpha^{n \cdot 2^l} = 1$

$\because \alpha$ is a primitive element of GF(2^m), its order is $2^m - 1$

$\therefore 2^m - 1 \mid n \cdot 2^l$ $\because (2^m - 1, 2^l) = 1$ $\therefore 2^m - 1 \mid n$ --- (2) By (1)& (2) $n = 2^m - 1$

$\Rightarrow$ If α is primitive, then α^{2^l} is primitive

Thm 2.16 If β is primitive in GF(2^m), all its conjugates β^2, β^{2^2}, … are also primitive

Example 2.10

Q: Thm 2.17 If β is an element of order n in GF(2^m), all its conjugates have the same order n

Example 2.11