符号理論･暗号理論

- No.7 有限体と拡大体 -

渡辺　裕

Coding Theory / Cryptography

- No.7 Finite Field and Extension Field -

Hiroshi Watanabe

群

- 半群の定義
  - 集合G, 算法@のとき代数系<G,@>が
    - 算法@について閉じている
    - 算法@に対して結合律が成立する
  - 閉じているとは?
    - 集合Gの元素x, yに関して算法@を適用した演算結果(x@y)も集合Gに属する
  - 結合律とは?
    - 集合Gの元素x,y,zに対して, (x@y)@z=x@(y@z)が成り立つ

Group

- Definition of Semi-group
  - For Set “G”, operation “@”, Algebra <G,@> is called “Semi-group” when the followings hold
    - Close for operation “@”
    - Associative law holds in operation “@”
  - What is closed?
    - For element x, y in set G, result of an operation (x@y) also blongs to G
  - What is associative law?
    - For elements x,y,z in set G, (x@y)@z=x@(y@z)

群 (2)

- 群の定義
  - 半群かつ下記の条件を満足する群
    - 単位元素eが存在する

      $x@e=x$
    - 逆元素$\underline{x}$が存在する

      $x@\underline{x}=e$

- 可換群の定義
  - 算法@が可換である群, アーベル群とも呼ばれる
    - $x@y=y@x$

Group (2)

- Definition of Group
  - Semi-group that satisfies the following
    - Identity element “e” exists

      x@e=x
    - Inverse element <u>x</u> exists

      x@<u>x</u>=e

- Definition of Commutative group
  - Commutative for operation “@”, sometimes called “Abelian group”
    - x@y=y@x

環

- 環の定義
  - 代数系<G,+,*>において
    - <G,+>は可換群
    - <G,*>は半群
    - 算法*は算法+に関して, 右側および左側分配的
  - 右側分配的とは?
    - $(x+y)*z=(x*z)+(y*z)$
  - 左側分配的とは?
    - $z*(x+y)=(z*x)+(z*y)$

Ring

- Definition of Ring
  - At algebra <G,+,*>, Ring satisfies follows
    - <G,+> is Commutative Group
    - <G,*> is Semi-group
    - Operation "*" is right and left distributive to operation "+"
  - What is right distributive?
    - $(x+y)*z=(x*z)+(y*z)$
  - What is left distributive?
    - $z*(x+y)=(z*x)+(z*y)$

環 (2)

- 注意
  - 環<G,+,*>における可換群<G,+>を加群と呼ぶ
  - 加群における単位元素を, 零元素と呼び, 0で表す
  - <G,*>は半群であるから単位元素があるとは限らない
    - 単位元素が存在するとき, 単位環と呼ぶ
    - <G,*>が可換であるとき, この環を可換環と呼ぶ
  - 環の算法は通常の代数と矛盾しない

Ring (2)

- Note
  - Commutative Group <G,+> at Ring <G,+,*> is called “G-module”
  - Additive identity element at Commutative Group <G,+> is called “null element, ” and noted as “0”
  - <G,*> is Semi-group. Thus, there may not be “identity element.”
    - If identity element exists, it is called “Ring with identity.”
    - If <G,*> is commutative, this Ring is called “Commutative Ring.”
  - Operation in Ring does not contradict to the normal algebra.

環 (3)

- 環の例 <Z(6), +(mod N), *(mod N)>
  - <Z(6), +(mod N)> は閉じている, 結合律が成立, 算法が可換
    - 単位元素が存在

      0+i=i+0=i　for i=0,1,2,3,4,5
    - 逆元素が存在

      i+(6-i)=(6-i)+i=0　for i=0,1,2,3,4,5
  - <Z(6), *(mod N)> は閉じている, 結合律が成立, 算法が可換
    - 単位元素が存在

      1*i=i*1=i　for i=0,1,2,3,4,5
    - 逆元素が存在

      0*i=i*0=i　for i=0,1,2,3,4,5

      2*3=3*2=0　2*4=4*2=2　2*5=5*2=4

      3*4=4*3=0　3*5=5*3=3　4*5=5*4=2

Ring (3)

- Example: <Z(N), +(mod N), *(mod N)>
  - <Z(6), +(mod 6)> is closed, associative, commutative
    - Identity element exists

      0+i=i+0=i   for i=0,1,2,3,4,5
    - Inverse elements exist

      i+(6-i)=(6-i)+i=0   for i=0,1,2,3,4,5
  - <Z(6), *(mod 6)> is closed, associative, commutative
    - Identity element exists

      1*i=i*1=i   for i=0,1,2,3,4,5
    - Inverse elements exist

      0*i=i*0=i   for i=0,1,2,3,4,5

      2*3=3*2=0   2*4=4*2=2   2*5=5*2=4

      3*4=4*3=0   3*5=5*3=3   4*5=5*4=2

問題

- 環において, i*j=0 (i,j≠0)が成立するとき, iとjはお互いに零因子の関係にあるという. ところで, <G(N), +(mod N), *(mod N)>において, Nが素数の場合には零因子が存在するかどうかを示せ.

Quiz

- When i*j=0 (i,j≠0) holds at Ring, i and j are called "zero divisor" each other. Show the existence of "zero divisor" when N is a prime number at Ring <G(N), +(mod N), *(mod N)> .

体

- 体の定義
  - 環<R,+,*>において, 0以外のすべての元素が可逆元素であるとき, この環を体という
  - 乗法において可換である体を可換体という
  - Q: 有理数全体, R: 実数全体, C: 複素数全体に対して, 有理数体<Q,+,*>, 実数体<R,+,*>, 複素数体<C,+,*>は可換体
  - Rの大きさを代数系の位数という

Field

- Definition of Field
  - If all elements except for 0 are inverse elements, this Ring <R,+,*> is called “Field”
  - If <R,*> is commutative, the field is called “Commutative Field”
  - For Q: Rational number, R: Real number, C: Complex number, Rational number field<Q,+,*>, Real number field<R,+,*>, Complex number field<C,+,*> are commutative field
  - Size of R is called “Order” in algebra

整数環

- イデアル, 剰余類, 剰余類環
  - イデアルIとは環Rの部分集合で, 次の性質を満たす
    - IはRの加法に関する部分群である
    - Iの任意の元aとRの任意の元rに対して, ar及びraはIに属する
  - Ex. 0及び正負の整数全体の集合は環をなす. 部分集合として0を含む3の倍数はイデアルとなる. イデアルは加法に関しては部分群であるから, 環RをIによって剰余類展開できる.
    - I={0}: 0, 3, -3, 6, -6, 9, -9, …
    - 剰余類{1}: 1, 4, -2, 7, -5, 10, -8, …
    - 剰余類{2}: 2, 5, -1, 8, -4, 11, -7, …

Integer Ring

- Ideal, Residue Class, Residue Class Ring
  - Ideal “I” is a subset or Ring “R” satisfies follows
    - I is sub-group of “R” with regard to addition
    - For a∈I and r∈R, ar∈I, ra∈I
  - Ex. Positive and negative integer and 0 are Ring. Multiple number of 3 including 0 as a sub-group are ideal. Ideal is sub-group with regard to addition, thus, Ring “R” can be expanded to Residue Class Ring.
    - I={0}: 0, 3, -3, 6, -6, 9, -9, …
    - Residue class{1}: 1, 4, -2, 7, -5, 10, -8, …
    - Residue class{2}: 2, 5, -1, 8, -4, 11, -7, …

整数環 (2)

- 整数環のイデアルと剰余類環
  - 整数環においてある部分集合がイデアルであるための必要かつ十分条件はその部分集合がある整数のすべての倍数からなる
    - 十分条件は明らか
    - 必要条件の証明はユークリッドの整除法による．整数a, bに対して次式を満たす商qと剰余rが一意に定まる．
      $a=bq+r\ (0 \leqq r < |b|)$
      このとき整数r, sの最大公約数dが必ず　d=ar+bsの形に書ける. rをイデアル中の正の最小の整数とし, sをイデアル中の他の任意の整数とすると, 最大公約数dは d=ar+bs から r∈I, s∈I から d∈I となる. dはrの約数だから d≦r, しかしrはイデアル中の正の最小の整数だからr<d, ゆえにr=d. イデアルの任意の元sは最小元rの倍数.

Integer Ring(2)

- Ideal of Integer Ring and Residue Class Ring
  - A necessary and sufficient condition for that a subset is ideal at Integer Ring, is that the subset consists of multiple numbers of a certain integer number
    - Sufficient condition is clear
    - Necessary condition is proved by Euclidean division algorithm. For integer a, b, quotion q and residual r are uniquely determined $a=bq+r$ $(0 \leqq r<|b|)$
in this case, greatest common divisor d can be written by $d=ar+bs$. Let r be the smallest positive integer in ideal, s be other integer in ideal, GCD $d \in I$ because $r \in I$, $s \in I$ from $d=ar+bs$. d is a divisor of r. Thus, $d \leqq r$, but r is the smallest integer in ideal. Thus, $r<d$, $r=d$. Therefore, an element s of ideal is a multiple number of the minimum element r.

整数環 (3)

- 主イデアル(単項イデアル): 環Rの一つの元の倍数全体よりなるイデアル
  - 環のどのイデアルも主イデアルである環を, 主イデアル環(単項イデアル環)とよぶ
  - 整数rの整数倍の全体からなるイデアルを(r)とかく. (r)の剰余類が作る剰余類環をrを法とする整数環とよぶ
- 整数rを法とする整数環(rを法とする整数の剰余類環)が体をなすための必要十分条件は, rが素数であることである
- 素数pを法とする整数環が形成する体を, 位数pの素体, あるいはp個の元をもつガロア体または有限体とよび, GF(p)であらわす

Integer Ring (3)

- Principal Ideal: Ideal consists of multiple numbers of one element in ring R
  - A ring is called principal ideal ring if any ideal in Ring is principal ideal
  - Ideal is noted as (r) if it consists of multiple of integer r. Residue class ring created by residue class of (r) is called integer ring with modulo r

- A necessary and sufficient condition for that Integer Ring (residue class ring with modulo r) becomes field is that r is a prime number

- Field, in which integer ring creates with modulo prime number p, is called Galois Field having order p, Noted GF(p)

有限体

- 有限体とは?
  - 加算と乗算の結果が有限個の元からなる
  - ガロア体とも呼ぶ
  - GF(q)で表す
  - qを位数を呼ぶ
  - 有限体は位数qが素数あるいはそのべき乗のときに成り立つ

Finite Field

- What is finite field?
  - Addition and multiplication result in finite number of element
  - Finite field is also called “Galois field”
  - Represented by GF(q)
  - “q” is called “order”
  - Finite field exists when order q is prime number or its power

有限体 (2)

- 有限体の例
  - GF(3)　mod3 の演算，逆元の存在が必要

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

x	-x
0	0
1	2
2	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

x	x^{-1}
0	-
1	1
2	2

Finite Field (2)

- Example of finite field
  - GF(3)　mod3 operation, needs existence of inverse element

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

x	-x
0	0
1	2
2	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

x	x^{-1}
0	-
1	1
2	2

多項式環のイデアルと剰余類

- 多項式環と規約多項式
  - 体Fの元を係数とする未知数xの多項式F(x)を, 体Fの上の多項式とよぶ
    - $F(x)=f_0+f_1x+f_2x^2+\ ...\ +\ f_nx^n$

      $f_0,\ f_1,\ f_2,\ ...,\ f_n \in F$
  - 非零の係数を有するxの最高次数を多項式の次数という. 最高次数の係数が1の多項式をモニック多項式とよぶ

- 既約多項式
    - $C(x)=A(X)B(x)$

      割り切れるとき A(x), B(x)はC(x)の因数

      多項式の次数がnで, 次数n-1以下のいかなる多項式でも

      割り切れないときに, 既約多項式とよぶ

Ideal of Polynomial Ring and Residue Class

- Polynomial Ring and Irreducible polynomial
  - Polynomial on Field F is defined as follows
    - $F(x)=f_0+f_1x+f_2x^2+ \dots + f_nx^n$

      $f_0, f_1, f_2, \dots, f_n \in F$
  - The highest n of the nonzero f is called order. If the number for highest order is 1, it is called monic polynomial

- Irreducible polynomial
    - $C(x)=A(X)B(x)$

      If divisible, A(x), B(x) is a factor of C(x)

      It is called irreducible when polynomial order is n, and cannot be divided by any polynomial with order less than n-1

多項式環のイデアルと剰余類 (2)

- ユークリッドの整除法の拡張
  - $A(x)=B(x)Q(x)+R(x)$
    - Q(x): 商多項式
    - R(x): 剰余多項式

- 多項式環のイデアル
  - 多項式環において，ある部分集合がイデアルであるための必要かつ十分条件は，その部分集合がある多項式のすべての倍数(多項式倍)からなることである
    - 多項式環は主イデアル環
    - 多項式環のイデアルは非零の最小次数のモニック多項式
    - そのイデアルに属する多項式はすべてのこのモニック多項式(生成多項式とよばれる)の倍数

Ideal of Polynomial Ring and Residual Class (2)

- Extension of Euclidean division algorithm
  - $A(x)=B(x)Q(x)+R(x)$
    - $Q(x)$: quotient polynomial
    - $R(x)$: Residue polynomial

- Ideal of polynomial ring
  - At polynomial ring, a necessary and sufficient condition of that subset is ideal, is that they all are multiple of one polynomial.
    - Polynomial ring is principal ideal ring
    - Ideal of polynomial ring is nonzero least order monic polynomial
    - All polynomials are multiples of monic polynomial

問題

- GF(2)の多項式全体Rを示せ
  - 低次の項のみ R={0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+x^2, x^3+x, x^3+x^2+x, x^3+x^2+x+1, … }
- F(x)= x^2+1の倍数の多項式を示せ
  - I={0, x^2+1, x(x^2+1), (x+1)(x^2+1), x^2(x^2+1), (x^2+1)(x^2+1), (x^2+x+1)(x^2+1), …. }

    = {0, x^2+1, x^3+x^2, x^3+x^2+x+1, x^4+x^2, … }
  - これはイデアルか?

Quiz

- Show all element of R which is polynomials on GF(2)
  - Only low term R={0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+x^2, x^3+x, x^3+x^2+x, x^3+x^2+x+1, … }
- Show multiple polynomials of $F(x)= x^2+1$
  - I={0, x^2+1, $x(x^2+1)$, $(x+1)(x^2+1)$, $x^2(x^2+1)$, $(x^2+1)(x^2+1)$, $(x^2+x+1)(x^2+1)$, …. }
    = {0, x^2+1, x^3+x^2, x^3+x^2+x+1, x^4+x^2, … }
  - Is this Ideal?

多項式環の剰余類環

- GF(2)においてF(x)= x^2+1はイデアルIの最小次数のモニック多項式
- F(x)で割ったときの剰余によりRは4種類に分類される
  - {0}: イデアルそのもの, {1}, {x}, {x+1}

- 剰余類環の加算と乗算

+	{0}	{1}	{x}	{x+1}
{0}	{0}	{1}	{x}	{x+1}
{1}	{1}	{0}	{x+1}	{x}
{x}	{x}	{x+1}	{0}	{1}
{x+1}	{x+1}	{x}	{1}	{0}

X	{0}	{1}	{x}	{x+1}
{0}	{0}	{0}	{0}	{0}
{1}	{0}	{1}	{x}	{x+1}
{x}	{0}	{x}	{1}	{x+1}
{x+1}	{0}	{x+1}	{x+1}	{0}

Residue Class Ring for Polynomial Ring

- $F(x) = x^2+1$ is the least order monic polynomial at GF(2)
- Residue divided by F(x) is classified into 4 groups
  - {0}: Ideal itself, {1}, {x}, {x+1}

- Addition and multiplication of residual class ring

+	{0}	{1}	{x}	{x+1}
{0}	{0}	{1}	{x}	{x+1}
{1}	{1}	{0}	{x+1}	{x}
{x}	{x}	{x+1}	{0}	{1}
{x+1}	{x+1}	{x}	{1}	{0}

X	{0}	{1}	{x}	{x+1}
{0}	{0}	{0}	{0}	{0}
{1}	{0}	{1}	{x}	{x+1}
{x}	{0}	{x}	{1}	{x+1}
{x+1}	{0}	{x+1}	{x+1}	{0}

ベクトル表現

- 多項式環の剰余類のベクトル表現

剰余類環	線形結合	ベクトル表現
{0}	0S+0	(0 0)
{1}	0S+1	(0 1)
{x}	1S+0	(1 0)
{x+1}	1S+1	(1 1)

Vector Representation

- Vector representation for polynomial ring

剰余類環	線形結合	ベクトル表現
{0}	0S+0	(0 0)
{1}	0S+1	(0 1)
{x}	1S+0	(1 0)
{x+1}	1S+1	(1 1)

多項式環の剰余類環 (2)

- GF(2)における$F(x)=x^4+1$を法とする多項式の代数系
  - R={0}, {1}, {x}, {x+1}, {x^2}, {x^2+1}, {x^2+x}, {x^2+x+1}, {x^3}, {x^3+1}, {x^3+x}, {x^3+x+1}, {x^3+x^2}, {x^3+x^2+1}, {x^3+x^2+x}, {x^3+x^2+x+1}

- 環を形成
  - 加法の例
    - {x^2}+{x^2+1}={1}
    - {x^3}+{x^3+x^2+1}= {x^2+1}
  - 乗法の例
    - {x^2} {x^2+1}={x^4+x^2}={x^2+1}
    - {x^3}{x^3+x^2+1}={$x^6+x^5+x^3$}={x^2+x+x^3}

Residual Class Ring for Polynomial Ring (2)

- Polynomial algebra with modulo F(x)=x4+1 at GF(2)
  - R={0}, {1}, {x}, {x+1}, $\{x^2\}$, $\{x^2+1\}$, $\{x^2+x\}$, $\{x^2+x+1\}$, $\{x^3\}$, $\{x^3+1\}$, $\{x^3+x\}$, $\{x^3+x+1\}$, $\{x^3+x^2\}$, $\{x^3+x^2+1\}$, $\{x^3+x^2+x\}$, $\{x^3+x^2+x+1\}$

- Generate Ring
  - Example of addition
    - $\{x^2\}+\{x^2+1\}=\{1\}$
    - $\{x^3\}+\{x^3+x^2+1\}= \{x^2+1\}$
  - Example of multiplication
    - $\{x^2\}\ \{x^2+1\}=\{x^4+x^2\}=\{x^2+1\}$
    - $\{x^3\}\{x^3+x^2+1\}=\{x^6+x^5+x^3\}=\{x^2+x+x^3\}$

多項式環の剰余類環 (3)

- 部分集合がイデアルとなる
  - $I=\{0\}, \{x+1\}, \{x^2+1\}, \{x^2+x\}, \{x^3+1\}, \{x^3+x\}, \{x^3+x^2\}, \{x^3+x^2+x+1\}$
  - このイデアルに属する最小次数の多項式を含むものは
    - $G(x)=x+1$
    - $G(x)$は$F(x)$を割り切る
    - Iの元$\{H(x)\}$はすべて$G(x)$の倍数
    - $G(x)$は生成多項式とよばれる
  - $G_1(x)=x+1$を生成多項式とするイデアル
    - $F(x)=x^4+1$
      $=(x+1)(x+1)(x+1)(x+1)$

Residual Class Ring for Polynomial Ring (3)

- Subset becomes Ideal
  - $I=\{0\}, \{x+1\}, \{x^2+1\}, \{x^2+x\}, \{x^3+1\}, \{x^3+x\}, \{x^3+x^2\}, \{x^3+x^2+x+1\}$
  - The minimum order polynomial in this Ideal
    - $G(x)=x+1$
    - G(x) is divisible to F(x)
    - Elements of I {H(x)} are all multiple of G(x)
    - G(x) is called Generator Polynomial
  - Ideal based on generator polynomial $G_1(x)=x+1$
    - $F(x)=x^4+1$
      $=(x+1)(x+1)(x+1)(x+1)$

多項式環の剰余類環 (4)

- 次に小さい次数の生成多項式
  - $G_2(x)=(x+1)(x+1)=x^2+1$を生成多項式とするイデアル
    - このイデアルの元は$G_2(x)$の倍数
    - $I_2=\{0\}\{x^2+1\}\{x^3+1\}\{x^3+x^2+x+1\}$
- もうひとつの生成多項式
  - $G_3(x)=(x+1)(x+1)(x+1)=x^3+x^2+x+1$を生成多項式とするイデアル
    - $I_3=\{0\}\{x^3+x^2+x+1\}$

Residue Class Ring for Polynomial Ring (4)

- Next, small order generation polynomial
  - Ideal based on $G_2(x)=(x+1)(x+1)=x^2+1$
    - Elements of this ideal is multiples of $G_2(x)$
    - $I_2=\{0\}\{x^2+1\}\{x^3+1\}\{x^3+x^2+x+1\}$

- Last generation polynomial
  - Ideal based on $G_3(x)=(x+1)(x+1)(x+1)=x^3+x^2+x+1$
    - $I_3=\{0\}\{x^3+x^2+x+1\}$

ガロア体

- $P(x)$を体Fの上の多項式とする．このとき$P(x)$が体Fの上で既約ならば，$P(x)$を法とする体Fの上の多項式環の剰余類環は体をなす

- Fをp個の元を有する体GF(p)とし，$P(x)$の次数をmとすれば，p^m個の元を有する体ができる．これをガロア体あるいは有限体とよび，GF(p^m)で表す．素数のべき乗個の元を有する体となる．有限体の元の数を位数とよぶ.

- 体Fを基礎体とよび，これから導かれる体を拡大体とよぶ．$P(x)$の次数をmとしたときに，m次の拡大体とよぶ.

Galois Field

- Let P(x) be polynomial on field F. If P(x) is irreducible on field F, residue class ring of polynomial ring on field F with modulo P(x) becomes field

- Let F be GF(p) having p elements. Let an order of P(x)be m. Field having p^m elements can be created. This is called Galois Field or Finite Field, noted by $F(p^m)$. It has a field having m-power of prime number elements. Number of elements of GF is called order.

- On the above, F is called ground field. Derived one is called Extension Field. When the order of P(x) is m, it is called m-th order Extension Field.

拡大体

- 拡大体とは
  - 有限体 GF(P) を拡大したもの
  - GF(2) に対して GF(2^m) は拡大体
  - 拡大体では，元は整数だけではなく，m次既約多項式の根を付加

- 拡大体の例
  - GF(2^2)=GF(4) は GF(2) の拡大体
  - 既約多項式の根を元に加える
  - $x^2+x+1=0$ は2次既約多項式であり，この根αを元に加える

Extension Field

- What is extension field?
  - Finite field GF(P) is extended
  - GF(2^m) is extension field for GF(2)
  - In extension field, element is not only integer but root of m-th degree irreducible polynomial

- Example of extension field
  - GF(2^2)=GF(4) is an extension field for GF(2)
  - Root of irreducible polynomial is added
  - $x^2+x+1=0$ is 2nd degree irreducible polynomial, thus this equation's root α is added to the element

拡大体 (2)

- 拡大体の例(続き)
  - 0, 1, αから他の元を求める
  - 体では積も同じ体の元に含まれる

$$\alpha^0 = 1$$

$$\alpha^1 = \alpha$$

$$\alpha^2 = \alpha + 1 \quad (\alpha^2 + \alpha + 1 = 0, \alpha = -\alpha)$$

$$\alpha^3 = \alpha\alpha^2 = \alpha(\alpha + 1) = \alpha + 1 + \alpha = 1$$

Extension Field (2)

- Example of extension field(cntd.)
  - Obtain other element from 0, 1, α
  - In field, product of elements is included in the elements of the same filed

$$\alpha^0 = 1$$

$$\alpha^1 = \alpha$$

$$\alpha^2 = \alpha + 1 \quad (\alpha^2 + \alpha + 1 = 0, \alpha = -\alpha)$$

$$\alpha^3 = \alpha\alpha^2 = \alpha(\alpha + 1) = \alpha + 1 + \alpha = 1$$

拡大体 (3)

- 拡大体の例(続き)
  - GF(4) 0, 1, α, α^2 を元とする

+	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

x	-x
0	0
1	1
α	α
α^2	α^2

x	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

x	-x
0	-
1	1
α	α^2
α^2	α

Extension Field (3)

- Example of extension field(cntd.)
  - GF(4) has element 0, 1, α, α^2

+	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

x	-x
0	0
1	1
α	α
α^2	α^2

x	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

x	-x
0	-
1	1
α	α^2
α^2	α

拡大体 (4)

- 一般に GF(2) のm次拡大体 GF(2^m)
  - 0 および m次既約多項式の根

$$\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{2^m-2}$$

  を GF(2^m) の原始元と呼ぶ
  - なお, αは 2^m-1 乗で1に戻る

$$\alpha^{2^m-1} = 1$$

  - GF(2^m) の原始元のべきによる表現を“べき表現”という

Extension Field (4)

- In general, m-th degree extension field GF(2^m) for GF(2)
  - We call 0 and root of m-th degree irreducible polynomial

$$\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{2^m-2}$$

primitive element of GF(2^m)

  - Here, α to the power of 2^m-1 result in 1

$$\alpha^{2^m-1} = 1$$

  - Representation of GF(2^m) by primitive element is called "power representation"

拡大体 (5)

- べき表現とベクトル表現
- GF(2^4), 既約多項式 x^4+x+1 の根をαとした場合

べき表現	α^3, α^2, α, 1 による展開				ベクトル表現
0				0	0000
1				1	0001
α			α		0010
α^2		α^2			0100
α^3	α^3				1000
α^4			α	$+1$	0011
α^5		α^2	$+\alpha$		0110

Extension Field (5)

- Power and vector representation
- GF(2^4), let root of irreducible polynomial x^4+x+1 be α

Power Rep.	Extension by α^3, α^2, α, 1				Vector Rep.
0				0	0000
1				1	0001
α			α		0010
α^2		α^2			0100
α^3	α^3				1000
α^4			α	$+1$	0011
α^5		α^2	$+\alpha$		0110

拡大体 (6)

べき表現	α^3, α^2, α, 1 による展開				ベクトル表現
α^6	α^3	$+\ \alpha^2$			1100
α^7	α^3		$+\ \alpha$	+1	1011
α^8		α^2		+1	0101
α^9	α^3		$+\ \alpha$		1010
α^{10}		α^2	$+\ \alpha$	+1	0111
α^{11}	α^3	$+\ \alpha^2$	$+\ \alpha$		1110
α^{12}	α^3	$+\ \alpha^2$	$+\ \alpha$	+1	1111
α^{13}	α^3	$+\ \alpha^2$		+1	1101
α^{14}	α^3			+1	1001

Extension Field (6)

Power Rep.	Extension by α^3, α^2, α, 1				Vector Rep.
α^6	α^3	$+ \alpha^2$			1100
α^7	α^3		$+ \alpha$	+1	1011
α^8		α^2		+1	0101
α^9	α^3		$+ \alpha$		1010
α^{10}		α^2	$+ \alpha$	+1	0111
α^{11}	α^3	$+ \alpha^2$	$+ \alpha$		1110
α^{12}	α^3	$+ \alpha^2$	$+ \alpha$	+1	1111
α^{13}	α^3	$+ \alpha^2$		+1	1101
α^{14}	α^3			+1	1001