■12 群（電子情報通信基礎）- 1 編（解析学・代数学）

3 章 代数系

（執筆者：西島利尚）［2008 年 12 月 受領］

■概要■

情報科学，あるいは情報工学は，計算機そのものを研究の対象とする，あるいは計算機を主たる道具とし，計算機に完全に依存するものを研究の対象とする学問領域である．計算機は，本質的に離散・有限の対象しか取り扱えないことはいうまでもない．従って，基盤となる数学的手法は，必然的に離散数学が重要な位置を占める．そして離散数学の中で，代数学は中心的な位置を占めている．代数学はある集合が与えられ，その集合の元と元の間の演算を考察する．その最も基本的な概念が，群・環・体である．

ディジタル情報の高信頼化を目的とする誤り訂正技術を理論的に支える符号理論は，代数学の中でも，特に有限群，イデアル，そして有限体（ガロア体）を数学的手法の基盤として構築されている．例えば，重要な誤り訂正符号の広範なクラスを含んでいる巡回符号は，イデアルの概念を基盤として構築されている．さらに巡回符号の一クラスで，実用的に極めて重要なリードソロモン符号の復号は，多項式環上のユークリッド互除法が極めて重要な役割を果たす．

また，ディジタル情報の安全性を高めることを目的とする情報セキュリティ技術のある一分野を理論的に支える現代暗号理論は，整数環を数学的手法の基盤として構築されている．例えば，重要な公開鍵暗号のいくつかは，初等整数論の概念を基盤として構築されている．具体的に，RSA 暗号は，十分大きな桁の合成数の素因数分解の困難さを安全性の根拠として，合同演算，フェルマーの小定理などが重要な役割を果たしている．

【本章の構成】

本章では抽象代数の基礎概念（3-1 節），環とガロア体（3-2 節），ガロア体の表現（3-3 節）について述べる．

■12 群 - 1 編 - 3 章

3-1 抽象代数の基礎概念

（執筆者：西島利尚）[2008 年 12 月 受領]

3-1-1 群

群 $\mathcal{G}$ は，次の四つの性質を満たす任意の 2 項演算 $\circ$ をもつ集合である．

G1. $\forall a, b \in \mathcal{G}$ ならば，$a \circ b = c \in \mathcal{G}$ （閉包）．

G2. $\forall a, b, c \in \mathcal{G}$ ならば，$a \circ (b \circ c) = (a \circ b) \circ c$ （結合則）．

G3. $\forall a \in \mathcal{G}$ に対し，$\exists e \in \mathcal{G}, a \circ e = e \circ a = a$ （単位元の存在）．

G4. $\forall a \in \mathcal{G}$ に対し，$\exists b \in \mathcal{G}, a \circ b = b \circ a = e$ （逆元の存在）．

群 $\mathcal{G}$ の元の総数を位数といい，位数が無限のとき無限群，有限のとき有限群という．そして $\forall a, b \in \mathcal{G}$ に対し，$a \circ b = b \circ a$（可換則）が成り立つとき可換群という．演算 $\circ$ を加法とし，記号 “+” で表すとき加法群といい，その単位元 e は “0”（ゼロ元），a の逆元 b は “$-a$” で表す．また，演算 $\circ$ を乗法とし，記号 “$\cdot$” で表すとき乗法群といい，その単位元 e は “1”，a の逆元 b は “a^{-1}” で表す．通常，加法群は可換で，乗法群は非可換である．

$\mathcal{H} \subset \mathcal{G}$ で，$\mathcal{G}$ と同一演算のもとで群をなす $\mathcal{H}$ を $\mathcal{G}$ の部分群という．有限群 $\mathcal{G}$ の部分群 $\mathcal{H}$ を生成する一つの方法は，$\mathcal{G}$ からある一つの元 h を選び，h 自身を繰り返し演算することである．すなわち，$h, h \circ h, h \circ h \circ h, \ldots$ を部分群 $\mathcal{H}$ とすればよい．ここで，$h, h \circ h, h \circ h \circ h, \ldots$ を形式的に $h, h^2, h^3, \ldots$ と表すことにする．$\mathcal{G}$ は有限群であるから，有限の演算回数で必ず最初の h が現れる．すなわち，ある最小の自然数 j に対し，$h^j = h$ となる．ゆえに，$h^{j-1} = e$ である．従って，$\{h, h^2, h^3, \ldots, h^{j-1} = e\} = \mathcal{H}$ とすればよい．ここで，$j - 1$ を元 h の位数という．元 h の位数は，集合 $\mathcal{H}$ の位数 (元の総数) に等しい．このとき，群 $\mathcal{H}$ は，元 h によって生成される巡回群という．

以下，2 項演算 $\circ$ は，加法 + あるいは乗法 $\cdot$ を表す．

3-1-2 環

環 $\mathcal{R}$ は，次の四つの性質を満たす 2 項演算，加法 + 及び乗法 $\cdot$ をもつ集合である．

R1. $\mathcal{R}$ は加法群である．

R2. $\forall a, b \in \mathcal{R}$ ならば，$a \cdot b = c \in \mathcal{R}$ （閉包）．

R3. $\forall a, b, c \in \mathcal{R}$ ならば，$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ （結合則）．

R4. $\forall a, b, c \in \mathcal{R}$ ならば，$a \cdot (b + c) = a \cdot b + a \cdot c$，　$(b + c) \cdot a = b \cdot a + c \cdot a$ （分配則）．

特に，$\forall a, b \in \mathcal{R}$ に対し，$a \cdot b = b \cdot a$（可換則）が成り立つとき可換環という．可換環において，更に $c \neq 0$ かつ $ca = cb$ ならば，$a = b$ であるとき，この可換環は整域をなしているという．

3-1-3 イデアル

環 $\mathcal{R}$ が与えられて，イデアル $\mathcal{I}$ は，次の二つの性質をもつ集合である．

I1. $\mathcal{I}$ は，$\mathcal{I} \subset \mathcal{R}$ であり，$\mathcal{R}$ の加法に関する部分群である．

I2. $\forall a \in \mathcal{I}$，$\forall r \in \mathcal{R}$ ならば，$a \cdot r \in \mathcal{I}$，$r \cdot a \in \mathcal{I}$．

3-1-4 体

体 $\mathcal{F}$ は，次の三つの性質を満たす 2 項演算，加法 + 及び乗法 · をもつ集合である．

F1. $\mathcal{F}$ は加法群である．

F2. $\forall a, b \in \mathcal{F}$ ならば，$a \cdot b = c \in \mathcal{F}$（閉包）であり，非ゼロ元の集合 $\mathcal{F} - \{0\}$ は可換乗法群である．

F3. $\forall a, b, c \in \mathcal{F}$ ならば，$a \cdot (b + c) = (b + c) \cdot a = a \cdot b + a \cdot c$（分配則）．

乗法に関して単位元をもち，すべての非ゼロ元が乗法に関して逆元をもつ可換環が体である．q 個の元からなる体を有限体あるいはガロア体という．符号理論では，通常ガロア体を $GF(q)$ と表す．以下，ガロア体は $GF(q)$ で表す．

$\mathcal{S} \subset \mathcal{F}$ で，$\mathcal{F}$ と同一演算のもとで体をなす $\mathcal{S}$ を $\mathcal{F}$ の部分体という．逆に，$\mathcal{F}$ は $\mathcal{S}$ の拡大体という．

■参考文献

1) 平澤茂一, 西島利尚, “符号理論入門,” 培風館, 1999.
2) 奥川光太郎, 辻吉雄, “現代代数学概論,” 白水社, 1967.

■12 群 - 1 編 - 3 章

3-2 環とガロア体

（執筆者：西島利尚）[2008 年 12 月 受領]

3-2-1 整数環

整数の集合を $\mathbb{Z}$ で表す．$\mathbb{Z}$ は，加法及び乗法に関して環をなす．$\mathbb{Z}$ を整数環という．$\forall m, a, b \in \mathbb{Z}$ に対し，$am = b$*のとき a が b を割り切る．これを $a|b$ と表す．このとき，b は a の倍数，a は b の因数という．a が b を割り切り，かつ b が a を割り切るならば，$a = \pm b$ である．1 より大きい自然数 p が $\pm p$ か，± 1 によってのみ割り切られるとき，自然数 p を素数という．素数でない 1 より大きい自然数を合成数という．a と b の両方を割り切る最大の自然数を最大公約数といい，$\gcd(a, b)$ で表す．特に，$\gcd(a, b) = 1$ のとき，a と b は互いに素であるという．

(1) 整除法

整数環では，除法が成り立たないので消約と余りをともなう演算を考える．すなわち，$\forall a, b \in \mathbb{Z}$ に対し，

$$b = aq + r \tag{3·1}$$

$$0 \le r < |a| \tag{3·2}$$

となる $\exists q, r \in \mathbb{Z}$ が一意に定まる．ここで，q を商，r を剰余という．

以下に合同演算を定義する上で，商より剰余の方が重要な意味をもつ．

(2) 合同演算

$\forall a, b, m \in \mathbb{Z}$ に対し，$m|(a - b)$ であるとき，そしてそのときに限って，m を法として a と b は合同であるという．これを $a \equiv b \pmod{m}$ で表す．これは差 $a - b$ が，m の倍数のすべてを表す集合の中に存在することを意味しており，$\mathbb{Z}$ のすべての整数 a を m で割れば一意に剰余が得られる事実に基づく．

(a) フェルマーの小定理

p が素数で，a は p で割り切れないならば，

$$a^{p-1} \equiv 1 \pmod{p} \tag{3·3}$$

である．

(b) 中国人の剰余定理

$m_1, m_2, \ldots, m_k$ が二つずつ互いに素で，$a_1, a_2, \ldots, a_k$ は任意の整数であるとき，

$$x \equiv a_1 \pmod{m_1} \tag{3·4}$$

$$x \equiv a_2 \pmod{m_2} \tag{3·5}$$

$$\cdots$$

$$x \equiv a_k \pmod{m_k} \tag{3·6}$$

* 乗法の記号 “·” を省略して記述する．

を満たす x は，$M = m_1 m_2 \cdots m_k$ を法としてただ一つ存在する．

(3) 因数分解の一意性

a を自然数とし，$a \neq 1$ とする．このとき，a は有限個の素数の積に一意に分解される．すなわち，

a は有限個の素数の積として表される．

m 個の素数 $p_1, p_2, \ldots, p_m$ と n 個の素数 $q_1, q_2, \ldots, q_n$ について，$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ ならば，$m = n$ であって，しかも $p_1 p_2 \cdots p_m$ の順序を適当に入れ換えれば $q_1 q_2 \cdots q_n$ に完全に一致する．

(4) ユークリッド互除法

整数環における自然数 a，b の最大公約数を求めるアルゴリズム，ユークリッド互除法を以下に示す．

$\forall a, b\ (a \geq b)$ の自然数とし，$a_0 = a, a_1 = b$ とおく．そして自然数 $n \geq 1$ に対し，$a_n > 0$ である限り a_{n+1} を，

$$a_{n-1} = a_n q_n + a_{n+1} \tag{3･7}$$

$$0 \leq a_{n+1} < a_n \tag{3･8}$$

によって定義する．このとき，ある自然数 $N \geq 1$ に対し，$a_{N+1} = 0$ であり，

$$a_N = \gcd(a,\ b) \tag{3･9}$$

である．

さらに，ユークリッド互除法を施すことにより，

$$\gcd(a, b) = ax + by \tag{3･10}$$

と表される $\exists x, y \in \mathcal{Z}$ の整数組の一つを求めることができる．

3-2-2 整数環とガロア体

m を自然数，$\forall a, b \in \mathcal{Z}$ とする．

$$a + b \equiv c \pmod{m} \tag{3･11}$$

$$a \cdot b \equiv d \pmod{m} \tag{3･12}$$

で定義される加法と乗法をもつ集合 $\{0, 1, \ldots, m-1\}$ を剰余類環または商環といい，$\mathcal{Z}_m$ で表す．

p が素数のとき，そしてそのときに限って，剰余類環 $\mathcal{Z}_p$ はガロア体をなす．すなわち，$\mathcal{Z}_p = GF(p)$ である．

3-2-3 多項式環

体 $\mathcal{F}$ 上の任意の多項式 $f(x)$ は,

$$f(x) = f_{n-1}x^{n-1} + f_{n-2}x^{n-2} + \cdots + f_1 x + f_0 \tag{3・13}$$

で表される．ただし，n は自然数，$f_{n-1} \neq 0$，x は不定元，係数 $f_i \in \mathcal{F}$，$i = 0, 1, \ldots, n-1$ である．$f(x) = 0$ をゼロ多項式という．$f_{n-1} = 1$ のとき，$f(x)$ をモニック多項式という．x の最高次数 $n-1$ を多項式 $f(x)$ の次数といい，$\deg f(x)$ で表す．ゼロ多項式 $f(x) = 0$ の次数は，形式的に $-\infty$ とする．また，$\mathcal{F}$ 上のすべての多項式の集合を $\mathcal{F}[x]$ で表す．

$\forall f(x), g(x) \in \mathcal{F}[x]$ に対し，多項式の加法と乗法をそれぞれ,

$$f(x) + g(x) = \sum_{i=0}^{\deg f(x)} (f_i + g_i)x^i \tag{3・14}$$

$$f(x) \cdot g(x) = \sum_{i=0}^{\deg f(x)} \sum_{j=0}^{\deg g(x)} (f_i \cdot g_j)x^{i+j} \tag{3・15}$$

で定義する．ただし，$\deg f(x) \geq \deg g(x)$，$f_i + g_i$ と $f_i \cdot g_j$ はそれぞれ $\mathcal{F}$ 上の加法と乗法である．$\mathcal{F}[x]$ は，上記で定義される加法と乗法に関して環をなす．$\mathcal{F}[x]$ を多項式環という．

$\forall m(x), f(x), g(x) \in \mathcal{F}[x]$ に対し，$f(x)m(x) = g(x)$[*]のとき $f(x)$ が $g(x)$ を割り切る．これを $f(x)|g(x)$ と表す．このとき，$g(x)$ は $f(x)$ の倍数，$f(x)$ は $g(x)$ の因数という．次数が 1 次以上の多項式 $p(x)$ が $\beta p(x)$ か $\beta \in \mathcal{F}$ によってのみ割り切られるとき，多項式 $p(x)$ を既約多項式といい，モニック既約多項式を素多項式という．$f(x)$ と $g(x)$ の両方を割り切る最大次数のモニック多項式を最大公約多項式といい，$\gcd(f(x), g(x))$ で表す．特に，$\gcd(f(x), g(x)) = 1$ のとき，$f(x)$ と $g(x)$ は互いに素であるという．

(1) 整除法

多項式環では，除法が成り立たないので消約と余りをともなう演算を考える．すなわち，$\forall f(x), g(x) \in \mathcal{F}[x]$ に対し,

$$g(x) = f(x)q(x) + r(x) \tag{3・16}$$

$$-\infty \leq \deg r(x) < \deg f(x) \tag{3・17}$$

となる $\exists q(x), r(x) \in \mathcal{F}$ が一意に定まる．ここで，$q(x)$ を商，$r(x)$ を剰余という．

以下に合同演算を定義する上で，商より剰余の方が重要な意味をもつ．

(2) 合同演算

$\forall f(x), g(x), m(x) \in \mathcal{F}[x]$ に対し，$m(x)|(f(x) - g(x))$ であるとき，そしてそのときに限って，$m(x)$ を法として $f(x)$ と $g(x)$ は合同であるという．これを $f(x) \equiv g(x) \pmod{m(x)}$ で表す．これは差 $f(x) - g(x)$ が，$m(x)$ の倍数のすべてを表す集合の中に存在することを意味しており，$\mathcal{F}[x]$ のすべての多項式 $f(x)$ を $m(x)$ で割れば一意に剰余が得られる事実に基づく．

(3) 因数分解の一意性

ある体 $\mathcal{F}$ 上の非ゼロ多項式 $f(x)$ は，その体 $\mathcal{F}$ 上の有限個の素多項式と，その体 $\mathcal{F}$ のあ

[*] 乗法の記号 "·" を省略して記述する．

る定数 β の積に一意に分解される．すなわち，

$f(x)$ は有限個の素多項式と $\exists\beta \in \mathcal{F}$ の積として表される．

m 個の素多項式 $p_1(x), p_2(x), \ldots, p_m(x)$ と n 個の素数 $q_1(x), q_2(x), \ldots, q_n(x)$ について，$p_1(x)p_2(x)\cdots p_m(x) = q_1(x)q_2(x)\cdots q_n(x)$ ならば，$m = n$ であって，しかも $p_1(x)p_2(x)\cdots p_m(x)$ の順序を適当に入れ換えれば，$q_1(x)q_2(x)\cdots q_n(x)$ に完全に一致する．

(4) ユークリッド互除法

多項式環におけるモニック多項式 $f(x)$, $g(x)$ の最大公約多項式を求めるアルゴリズム，ユークリッド互除法を以下に示す．

$\forall f(x), g(x) \in \mathcal{F}[x], \deg f(x) \geq \deg g(x)$ とし，$f_0(x) = f(x)$, $f_1(x) = g(x)$ とおく．そして自然数 $n \geq 1$ に対し，$\deg f_n(x) > -\infty$ である限り，$f_{n+1}(x)$ を，

$$f_{n-1}(x) = f_n(x)q_n(x) + f_{n+1}(x) \tag{3･18}$$

$$-\infty \leq \deg f_{n+1}(x) < \deg f_n(x) \tag{3･19}$$

によって定義する．このとき，ある自然数 $N \geq 1$ に対し，$f_{N+1}(x) = 0$ であり，

$$f_N(x) = \gcd(f(x), g(x)) \tag{3･20}$$

である．

さらに，ユークリッド互除法を施すことにより，

$$\gcd(f(x), g(x)) = f(x)X(x) + g(x)Y(x) \tag{3･21}$$

と表される $\exists X(x), Y(x) \in \mathcal{F}[x]$ の多項式の組の一つを求めることができる．

3-2-4 多項式環とガロア体

体 $\mathcal{F}$ 上のモニック多項式 $m(x)$, $\forall f(x), g(x) \in \mathcal{F}[x]$ とする．

$$f(x) + g(x) \equiv h(x) \pmod{m(x)} \tag{3･22}$$

$$f(x) \cdot g(x) \equiv k(x) \pmod{m(x)} \tag{3･23}$$

で定義される加法と乗法をもつ集合 $\{f(x) | -\infty \leq \deg f(x) < \deg m(x), f(x) \in \mathcal{F}[x]\}$ を剰余類環または商環といい，$\mathcal{F}_{m(x)}[x]$ で表す．

$p(x)$ が素多項式のとき，そしてそのときに限って，剰余類環 $\mathcal{F}_{p(x)}[x]$ は体をなす．そして $\mathcal{F}$ がガロア体のとき，$\mathcal{F}_{p(x)}[x]$ もガロア体である．

3-2-5 原始元

$\exists\alpha \in GF(q)$ に対して，$GF(q)$ のすべての非ゼロ元を α のべき乗で表現できるとき，α を $GF(q)$ の原始元という．$GF(q') \subset GF(q)$ とする．$GF(q)$ の原始元 α を根としてもつ $GF(q')$ 上の素多項式 $p(x)$ を原始多項式という．すなわち，$p(\alpha) = 0$ である．原始元の定義より，任

意のガロア体 $GF(q)$ の非ゼロ元の集合 $GF(q)-\{0\}$ は巡回乗法群をなすことは明らかである．従って，$GF(q)-\{0\}$ は，位数 $q-1$ の元を必ずもつ．この元が $GF(q)$ の原始元である．任意のガロア体 $GF(q)$ は原始元を必ずもつ．

3-2-6 ガロア体の構造

$GF(q)$ の部分体の中で最小の位数 p をもつ部分体を $GF(p)$ とする．p を $GF(q)$ の標数という．任意のガロア体 $GF(q)$ の標数 p は素数である．

$GF(p)\subset GF(q)$ とする．$\forall\beta\in GF(q)$ に対し，$m(\beta)=0$ となる $GF(p)$ 上の最小次数の多項式 $m(x)$ を β の最小多項式という．β の $GF(p)$ 上の最小多項式 $m(x)$ は一意に存在する．さらに β が $GF(p)$ 上のある多項式 $f(x)$ の根であるとき，$m(x)|f(x)$ である．ここで，$m(x)$ は $GF(p)$ 上で既約である．$f(x)$ を $GF(p)$ 上の多項式とする．$f(x)$ を 1 次式の多項式の積でのみ表現可能な拡大体 $GF(q)$ が存在する．このとき，拡大体 $GF(q)$ を $f(x)$ の分解体という．

ある自然数 m に対して $q=p^m$ とし，$GF(p)$ 上の多項式,

$$f(x)=x^{p^m}-x \tag{3･24}$$

を考える．これは，$\forall\beta_i\in GF(q), i=1,2,\ldots,q$ とすれば，1 次の多項式の積,

$$f(x)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_q) \tag{3･25}$$

と表すことが可能である．すなわち，$GF(q)$ は $f(x)$ の分解体である．この分解体の位数は，$q=p^m$ である．従って，p^m 個の元をもつガロア体 $GF(p^m)$ が存在する．上述の $GF(q)$ の最小の部分体 $GF(p)$ についての議論を $GF(q)$ の任意の部分体 $GF(q')$ について行えば，任意のガロア体 $GF(q)$ 上の次数 m の素多項式が少なくとも一つは存在し，同時に原始多項式が少なくとも一つは存在することを示すことができる．

■参考文献

1) 平澤茂一, 西島利尚, “符号理論入門,” 培風館, 1999.
2) 高木貞治, “初等整数論講義,” 共立出版, 1931.

■12 群 - 1 編 - 3 章

3-3 ガロア体の表現

（執筆者：西島利尚）[2008 年 12 月 受領]

3-3-1 べき表現・多項式表現・ベクトル表現

本節は，計算機によるガロア体の表現に限定して述べる．すなわち，標数 2 のガロア体について述べる．一般に，標数 p のガロア体についても同様である．$GF(2)$ 上の m 次の原始多項式 $p(x)$ の根を $\alpha \in GF(2^m)$ とする．$GF(2^m)$ の非ゼロ元は，すべて原始元 α のべき乗で表現できる．すなわち，

$$\{\alpha^0 = 1, \alpha^1, \alpha^2, \ldots, \alpha^{2^m-2}\} \tag{3･26}$$

で表される．これは明らかに巡回乗法群である．この巡回乗法群に加法の単位元 0 を加えた集合がガロア体 $GF(2^m)$ である．すなわち，

$$GF(2^m) = \{0, 1, \alpha^1, \alpha^2, \ldots, \alpha^{2^m-2}\} \tag{3･27}$$

で表される．これをガロア体 $GF(2^m)$ のべき表現という．

また，$GF(2^m)$ は $p(x)$ を法とする多項式の剰余類環であるから，$GF(2^m)$ の元は次数が，$\deg p(x)$ 次未満の $GF(2)$ 上のすべての多項式で表される．すなわち，

$$a(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0 \in GF(2^m) \tag{3･28}$$

と表される．ただし，$\forall a_i \in GF(2) = \{0, 1\}$，$i = 0, 1, \ldots, m-1$ である．これをガロア体 $GF(2^m)$ の多項式表現という．

多項式表現において，$a(x)$ の係数のみを書き出した，

$$\boldsymbol{a} = (a_{m-1}, a_{m-2}, \ldots, a_1, a_0) \in GF(2^m) \tag{3･29}$$

をガロア体 $GF(2^m)$ のベクトル表現という．

ガロア体のべき表現は乗法を実行するのに適した表現で，ベクトル表現あるいは多項式表現は加法を実行するのに適した表現である．すなわち，乗法は，

$$\alpha^i \cdot \alpha^j = \alpha^{i+j} \pmod{2^m-1} \tag{3･30}$$

を実行すればよく，加法は，

$$\boldsymbol{a} + \boldsymbol{b} = (a_{m-1} + b_{m-1}, a_{m-2} + b_{m-2}, \ldots, a_1 + b_1, a_0 + b_0) \tag{3･31}$$

あるいは，

$$a(x) + b(x) = (a_{m-1} + b_{m-1})x^{m-1} + (a_{m-2} + b_{m-2})x^{m-2} + \cdots + (a_1 + b_1)x + (a_0 + b_0) \tag{3･32}$$

を実行すればよい．

$GF(2)$ 上の原始多項式 $p(x) = x^4 + x + 1$，$p(\alpha) = 0$ の原始元 $\alpha \in GF(2^4)$ を用いて，$GF(2^4)$

表 3･1　$GF(2^4)$ の元の表現

べき表現	多項式表現	ベクトル表現
0	0	0000
$\alpha^0 = 1$	1	0001
α	x	0010
α^2	x^2	0100
α^3	x^3	1000
α^4	$x+1$	0011
α^5	x^2+x	0110
α^6	x^3+x^2	1100
α^7	x^3+x+1	1011
α^8	x^2+1	0101
α^9	x^3+x	1010
α^{10}	x^2+x+1	0111
α^{11}	x^3+x^2+x	1110
α^{12}	x^3+x^2+x+1	1111
α^{13}	x^3+x^2+1	1101
α^{14}	x^3+1	1001

のすべての元を α のべき表現，多項式表現，そしてベクトル表現の具体例を表 3･1 に示す．

3-3-2 基底

n 次元線形空間 $\mathcal{V}$ において，$\{e_1, e_2, \ldots, e_n\}$，$\exists e_i \in \mathcal{V}$，$i = 1, 2, \ldots, n$，が 1 次独立で，しかもこれらが $\mathcal{V}$ を生成するならば，$\{e_1, e_2, \ldots, e_n\}$ は，$\mathcal{V}$ の基底である．

以下に $GF(2^m)$ を表現するための基本的な基底を示す．

(1) 多項式基底

$GF(2)$ 上の素多項式 $p(x)$ の根を α とする．すなわち，$p(\alpha) = 0$ とする．このとき $GF(2^m)$ の多項式表現において $x = \alpha$ とすれば，$GF(2^m)$ の任意の元 β は，$\alpha^0 = 1$，α，α^2，…，α^{m-1} の線形結合で表される．すなわち，

$$\beta = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots + a_1\alpha + a_0 \in GF(2^m) \tag{3･33}$$

と表される．このとき $\{\alpha^{m-1}, \alpha^{m-2}, \ldots, \alpha^0\}$ を多項式基底という．

(2) 正規基底

$GF(2)$ 上の原始多項式 $p(x)$ の根を α とする．すなわち，$p(\alpha) = 0$ とする．このとき，原始多項式 $p(x)$ の根のすべての集合は $\{\alpha^{2^{m-1}}, \alpha^{2^{m-2}}, \ldots, \alpha^2, \alpha\}$ で表される．この集合は原始多項式 $p(x)$ の選び方によって，1 次独立となる場合とそうでない場合がある．1 次独立となる場合を正規基底という．正規基底となる根をもつ原始多項式は，$GF(2)$ 上で任意の次数に対し，少なくとも一つは存在する．

■参考文献

1)　平澤茂一, 西島利尚, “符号理論入門,” 培風館, 1999.
2)　今井秀樹, “符号理論,” コロナ社, 1990.