5　線型空間

抽象的ベクトル空間 (線型空間) に関しては線形解析で扱ったと思うが，その定義は係数体が一般の体の場合も同じ定義を採用できる。

定義 5.1 K を体とする。空でない集合 V に和 (足し算) とスカラー倍が定義されていて，次の (1)–(8) の性質を満足する時 V を K 上の**ベクトル空間** (*vector space*) といい V の各元を**ベクトル** (*vector*) と呼ぶ。$\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ を V の元とし α, β を K の元とする時

(1) $(\boldsymbol{u}+\boldsymbol{v})+\boldsymbol{w} = \boldsymbol{u}+(\boldsymbol{v}+\boldsymbol{w})$　(結合法則)

(2) $\boldsymbol{u}+\boldsymbol{v} = \boldsymbol{v}+\boldsymbol{u}$　(交換法則)

(3) 特別な元 $\boldsymbol{o}$ (零ベクトル又は零元と呼ばれる) が存在して任意のベクトルに対し $\boldsymbol{v}+\boldsymbol{o} = \boldsymbol{v}$ となる。

(4) 任意のベクトル $\boldsymbol{v}$ に対しあるベクトル $\boldsymbol{v}'$ が存在して ($\boldsymbol{v}$ の逆元という) $\boldsymbol{v}+\boldsymbol{v}' = \boldsymbol{o}$ となる (普通 $\boldsymbol{v}' = -\boldsymbol{v}$ と表す)。

(5) $\alpha(\boldsymbol{u}+\boldsymbol{v}) = \alpha\boldsymbol{u}+\alpha\boldsymbol{v}$　(分配法則)

(6) $(\alpha+\beta)\boldsymbol{v} = \alpha\boldsymbol{v}+\beta\boldsymbol{v}$　(分配法則)

(7) $(\alpha\beta)\boldsymbol{v} = \alpha(\beta\boldsymbol{v})$

(8) $1\boldsymbol{v} = \boldsymbol{v}$

体 L が体 K の拡大体であるとき，和は L の和，K の元との積をスカラー倍と見なすと，定義 5.1 の (1)–(8) をみたすので，L はベクトル空間をなす。L が K 上のベクトル空間として n 次元のとき，この n を拡大 L/K の拡大次数といい $[L:K]$ と書く。

$K = \boldsymbol{Q}$,$L = \boldsymbol{Q}(\sqrt{2})$ のとき，L を K 上のベクトル空間と見なすと，$1, \sqrt{2}$ が基底をなす事が分かる。よって $[\boldsymbol{Q}(\sqrt{2}) : \boldsymbol{Q}] = 2$ である。

$K = \boldsymbol{Q}$,$L = \boldsymbol{Q}(\sqrt[3]{2})$ のとき，L を K 上のベクトル空間と見なすと，$1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ が基底をなす事が分かる。よって $[\boldsymbol{Q}(\sqrt[3]{2}) : \boldsymbol{Q}] = 3$ である。

命題 5.2 L を K の拡大体とする。α の K 上の次数を n とすると，$[K(\alpha) : K] = n$ が成立する。

証明　$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ が基底をなす事が証明できる。

6　有限体

以下 F を有限体とする。

命題 6.1 $K \subset L$ を有限体とする。$[L:K] = n$ とすると $\#(L) = \#(K)^n$ である。

命題 6.2 F の標数は 0 ではない。

証明 $\underbrace{1+\cdots+1}_{k} = \varphi(k)$ と置く。F は有限集合なので，十分大きい n について，$\varphi(1), \varphi(2), \ldots, \varphi(n)$ がすべて異なることはない。よって $n > m$ となるある n と m に対し $\varphi(n) = \varphi(m)$ が成立する。$\underbrace{1+\cdots+1}_{n} = \underbrace{1+\cdots+1}_{m}$ より，$\underbrace{1+\cdots+1}_{n-m} = 0$ が得られ，標数が 0 でない事が分かる。 ∎

命題 4.4 より有限体 F の標数 p は素数である。$F_p = \{0, 1, 1+1, \ldots, \underbrace{1+\cdots+1}_{p-1}\}$ とおくと，F_p は体となるので，F は F_p の拡大体になっている (勿論 $F = F_p$ の場合も含む)。F は有限集合なので，F_p 上のベクトル空間と見たとき有限次元である。この次元を n とする。F の基底 $\alpha_1, \ldots, \alpha_n$ を 1 つ決めると F の任意の元 $a \in F$ は $a = a_1\alpha_1 + \cdots + a_n\alpha_n$ と表す事ができる。即ち F は $\underbrace{F_p \times \cdots \times F_p}_{n}$ と同一視できるので，$\#(F) = p^n$ である。ただし $\#(F)$ は集合 F の元の個数を表す。以上により次が示された。

定理 6.3 F を有限体とすると，ある素数 p と自然数 n が存在して $\#(F) = p^n$ である。

要素の個数が q 個である体を q 元体と呼び F_q と表す事にする。2 元体・3 元体・4 元体・5 元体は存在するが 6 元体は存在しない事が分かる。

次に 2^n 元体を具体的に見ていこう。最初は 2 元体。これは $F_2 = \boldsymbol{Z}_2 = \{0, 1\}$ でありすでに学んでいる。

次は 4 元体。標数は 2 なので，$1 + 1 = 0$ となっている。$F_2 = \{0, 1\} \subset F_4$ とみなす事ができる。$\alpha \in F_4 - \{0, 1\}$ なる元を取ってくると $1, \alpha$ は F_2 上のベクトル空間としての F_4 の基底になっている。α^2 は F_4 の元なので $\alpha^2 = a\alpha + b$ $(a, b \in F_2)$ と書く事ができる。$a = 1$ かつ $b = 1$ の場合以外は $\alpha \in F_2$ となるので $\alpha^2 = \alpha + 1$，これを移項して $\alpha^2 + \alpha + 1 = 0$ を得る。α は F_2 上の既約多項式 $X^2 + X + 1$ の解である。

即ち F_2 の唯一の既約 2 次多項式 $X^2 + X + 1$ の解 α を 1 つとってきたとき，$F_4 = F_2(\alpha)$ となっている。$F_4 = \{0, 1, \alpha, \alpha+1\}$ であるが，0 は既約多項式 X の解，1 は既約多項式 $X + 1$ の解，$\alpha, \alpha + 1$ は既約多項式 $X^2 + X + 1$ の解になっている。

4 元体の data 及びその和と積を計算機にインプリメントする事を考える。$F_2 = \{0, 1\}$ は 1bit data として与えられていると考える。bit data として bit 和を $\bigoplus$ bit 積を $\bigodot$ で表す。F_4 の元は $a\alpha + b$ の形をしている。計算機上では通常は 2 進数で ab と表現する。即ち data の集合としては通常 $D = \{00, 01, 10, 11\}$ をとる。$ab, cd \in D$ に対し和 $+$ は $ab + cd = (a \bigoplus c)(b \bigoplus d)$ となる。積は F_4 では $(a\alpha+b)(c\alpha+d) = ac\alpha^2+(ad+bc)\alpha+bd = ac(\alpha+1)+(ad+bc)\alpha+bd = (ac+ad+bc)\alpha+(ac+bd)$ と表されるので $ab \cdot cd = ((a \bigodot c) \bigoplus (a \bigodot d) \bigoplus (b \bigodot c))\,((a \bigodot c) \bigoplus (b \bigodot d))$ となる。

次に 8 元体 F_8 を考える。F_2 上の 3 次の既約多項式は $X^3 + X^2 + 1$ と $X^3 + X + 1$ の 2 つであったが，それとどう関係するのであろう。4 元体の場合と同様に $F_2 = \{0, 1\} \subset F_8$ とみることができる。$\alpha \in F_8 - \{0, 1\}$ とするとなる元を取ってくる。$1, \alpha, \alpha^2$ が F_2 上のベクトル空間としての F_8 の基底になっている事を示したい。もしそうでないとすると，$F_2[X]$ のある 2 次多項式 $f(X)$ が存在して $f(\alpha) = 0$ となっている。このとき $f(X) = X^2 + X + 1$ となり，$F_2(\alpha) \subset F_8$ は 4 元体となる。$[F_8 : F_2(\alpha)] = n$ とすると，命題 6.1 より $8 = 4^n$ となるがこれは矛盾。

α^3 は基底 $1, \alpha, \alpha^2$ の線型結合で書けるので，ある 3 次式 $f(X)$ に対し $f(\alpha) = 0$ である。$f(X)$ が既約でなければ α は 2 次または 1 次の多項式の解になるがこれは矛盾，よって $f(X)$ は既約である。F_2 上の 3 次の既約多項式は $g(X) = X^3 + X + 1$ または $h(X) = X^3 + X^2 + 1$ の 2 つである。$g(X + 1) = h(X)$ なので，$h(\alpha) = 0$ のときは $g(\alpha + 1) = h(\alpha) = 0$ となる。このとき α を $\alpha + 1$ に置き換えて議論をすればよいので，$g(\alpha) = 0$，即ち $f(X) = g(X)$ として話を進める。$F_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$ となっていて，$\alpha, \alpha^2, \alpha^2 + \alpha$ は $g(X) = 0$ の解であり，$\alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha + 1$ は $h(X) = 0$ の解である。

別の言い方をすると，$g(X) = 0$ の 3 つの解 α, β, γ，$h(X) = 0$ の 3 つの解 $\delta, \varepsilon, \zeta$ とすると，$F_8 = \{0, 1, \alpha, \beta, \gamma, \delta, \varepsilon, \zeta\}$ である。

演習問題 6.1　8 元体 F_8 の data 及びその和と積を 4 元体の場合と同様に計算機にインプリメントせよ。

更にしつこく 16 元体を考える。既約 4 次多項式は $f(X) = X^4 + X + 1$, $g(X) = X^4 + X^3 + 1$, $h(X) = X^4 + X^3 + X^2 + X + 1$ の 3 つである。$\alpha \in F_{16} - F_2$ をとってくる。α が既約 2 次方程式の解になる事もあるが，それは後で扱う事にして，ここではそうなっていないとする。α は 3 つの既約方程式のどれかの解になっている。ここでは $f(X) = 0$ の解であるとして議論しよう。計算を実行すると $f(X) = 0$ の解は α, $\alpha + 1$, α^2, $\alpha^2 + 1$，$g(X) = 0$ の解は $\alpha^3 + 1$, $\alpha^3 + \alpha$, $\alpha^3 + \alpha^2 + 1$, $\alpha^3 + \alpha^2 + \alpha$，$h(X) = 0$ の解は α^3, $\alpha^3 + \alpha + 1$, $\alpha^3 + \alpha^2$, $\alpha^3 + \alpha^2 + \alpha + 1$ が分かる。残りの 2 つ $\alpha^2 + \alpha$ と $\alpha^2 + \alpha + 1$ は 2 次方程式 $X^2 + X + 1 = 0$ の解である事が分かる。

α が既約 2 次方程式の解の場合を扱おう。前の α と混乱しないようにその元を β と書き直そう。即ち β は $X^2 + X + 1$ の解とする。$F_2(\beta)$ は 4 元体になるのでこれを F_4 と書く。F_4 上の 2 次既約多項式は $X^2 + X + \beta$, $X^2 + X + \beta + 1$, $X^2 + \beta X + 1$, $X^2 + \beta X + \beta$, $X^2 + (\beta + 1)X + 1$, $X^2 + (\beta + 1)X + \beta + 1$ の 6 個である。

$F_{16} - F_4$ から元 α をとってくる。$1, \alpha$ は F_4 上のベクトル空間としての F_{16} の基底になる。よって α は上の 1 つの 2 次式からできる方程式の解になっている。今 $X^2 + X + \beta$ の解と仮定する。よって F_{16} の元は x, y を F_4 の元とするとき，$x + y\alpha$ と書ける。たとえば $x = \beta + 1$, $y = \beta$ のとき，$x + y\alpha = (\beta + 1) + \beta\alpha = \alpha^2 + \alpha + 1 + (\alpha^2 + \alpha)\alpha = \alpha^3 + \alpha + 1$ となっている。

次に 3^n 元体を見よう。$n = 1$ のときは $F_3 = \boldsymbol{Z}_3$ である。F_3 上の既約 1 次多項式は X, $X + 1$, $X + 2$ の 3 つである。既約 2 次多項式は $f(X) = X^2 + 1$, $g(X) = X^2 + X + 2$, $h(X) = X^2 + 2X + 2$ の 3 つである。$f(X) = 0$ の解を α とすると，$f(X) = 0$ の解は $\alpha, 2\alpha$, $g(X) = 0$ の解は $\alpha+1, 2\alpha+1$ $h(X) = 0$ の解は $\alpha + 2, 2\alpha + 2$ である。$F_9 = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$ となっている。

既約な 3 次式は $a(X) = X^3 + 2X + 1$, $b(X) = X^3 + 2X^2 + 1$, $c(X) = X^3 + X^2 + 2$, $d(X) = X^3 + 2X + 2$, $e(X) = X^3 + 2X^2 + X + 1$, $f(X) = X^3 + X^2 + X + 2$, $g(X) = X^3 + X^2 + 2X + 1$, $h(X) = X^3 + 2X^2 + 2X + 2$ である。$a(X) = 0$ の解を α とすると，$a(X) = 0$ の解は α,$\alpha+1$,$\alpha+2$, $b(X) = 0$ の解は $2\alpha^2 + 1$,$2\alpha^2 + 2\alpha$,$2\alpha^2 + \alpha$, $c(X) = 0$ の解は $\alpha^2 + 2$,$\alpha^2 + \alpha$,$\alpha^2 + 2\alpha$, $d(X) = 0$ の解は 2α,$2\alpha + 1$,$2\alpha + 2$, $e(X) = 0$ の解は $2\alpha^2$,$2\alpha^2 + 2\alpha + 2$,$2\alpha^2 + \alpha + 2$, $f(X) = 0$ の解は α^2,$\alpha^2 + \alpha + 1$,$\alpha^2 + 2\alpha + 1$, $g(X) = 0$ の解は $\alpha^2 + 1$,$\alpha^2 + \alpha + 2$,$\alpha^2 + 2\alpha + 2$, $h(X) = 0$ の解は $2\alpha^2 + 2$,$2\alpha^2 + 2\alpha + 1$,$2\alpha^2 + \alpha + 1$ である。