体論 (第4回)

4. 拡大次数

体の拡大 L/K が与えられると, L には次で K 上のベクトル空間の構造が入る.

(i) 足し算: $L \times L \to L$ $((x, y) \longmapsto x + y)$,

(ii) スカラー倍 : $K \times L \longrightarrow L$ $((a, x) \longmapsto ax)$.

ただし, 上の $x + y$ や ax は体 L の足し算と掛け算で考える.

定義 4-1 (拡大次数)

体の拡大 L/K に対して,

$$[L : K] := \dim_K L \qquad (L \text{ の } K \text{ 上のベクトル空間としての次元})$$

を L/K **の拡大次数**と言う. $[L : K] < \infty$ のとき, L/K は**有限次拡大**といい, そうでないとき, L/K を**無限次拡大**という. また $[L : K] = n$ のとき, L/K を n **次拡大**と呼ぶ.

[補足] $K \subseteq L$ であるから,

$$[L : K] = 1 \Longleftrightarrow L = K$$

が成り立つ.

ベクトル空間の次元の復習も兼ねて, 次の例題を考える.

例題 4-1

$\{1 + i, 1 - i\}$ は $\mathbb{C}/\mathbb{R}$ の基底である. 特に

$$[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}} \mathbb{C} = 2.$$

※ 体の拡大 L/K に対して, L/K の基底とは, L の K 上ベクトル空間としての基底のことである.

[**証明**]

(1 次独立であること) $a, b \in \mathbb{R}$ が

$$a(1+i) + b(1-i) = 0$$

を満たすとする. このとき,

$$(a+b) + i(a-b) = 0$$

より, $a+b = a-b = 0$. よって $a = b = 0$. 従って, $1+i, 1-i$ は $\mathbb{R}$ 上 1 次独立である.

($\mathbb{C}$ を生成すること) $z \in \mathbb{C}$ を取る. $z = a + bi$ $(a, b \in \mathbb{R})$ と表し, 次のように変形する.

$$z = a + bi = \frac{a+b}{2}(1+i) + \frac{a-b}{2}(1-i).$$

従って, z は $1+i, 1-i$ の $\mathbb{R}$ 上の 1 次結合で表せる.

□

問題 4-1 $\alpha = \sqrt{-2}$, $\beta = 1 + \alpha$ とし, また

$$M = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$$

と置く. このとき, $\{\beta, \beta^2\}$ は M の $\mathbb{Q}$ 上の基底であることを示せ.

定理 4-1

L/K を体の拡大, $\alpha \in L$ は K 上代数的とする. $f(x)$ を α の K 上の最小多項式とし, $n = \deg f$ とする. さらに,

$$M := K[\alpha] = \{g(\alpha) \mid g(x) \in K[x]\}$$

と置く. このとき, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ は M の K 上の基底となる.

※ M は L の部分ベクトル空間になっていることは容易に分かる.

[**証明**]

(1 次独立であること) $a_0, \ldots, a_{n-1} \in K$ として $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$ とする. 多項式 $g(x)$ を

$$g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in K[x]$$

で定めると,

$$g(\alpha) = 0, \quad \deg g < n = \deg f$$

が成り立つ. $f(x)$ は α の K 上の最小多項式なので $g(x)=0$ でなければならない. よって

$$a_0 = a_1 = \cdots = a_{n-1} = 0$$

となり, $1, \alpha, \ldots, \alpha^{n-1}$ は K 上 1 次独立である.

(M を生成すること) $z \in M$ とし, $z = g(\alpha)$ となる $g(x) \in K[x]$ を取る. 割り算の原理から

$$g(x) = q(x)f(x) + r(x), \quad \deg r < n$$

を満たす $q(x), r(x) \in K[x]$ が取れる. このとき,

$$r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \quad (a_i \in K)$$

と表すと,

$$z = g(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}.$$

よって, z は $1, \alpha, \ldots, \alpha^{n-1}$ の K 上の 1 次結合で表せる.

□

定理 4-2

定理 4-1 の状況を考える. このとき, M は体である. 特に $M = K(\alpha)$ であり,

$$[K(\alpha) : K] = \deg f.$$

[証明]

環準同型

$$\Phi : K[x] \longrightarrow L \quad (g(x) \longmapsto g(\alpha))$$

を考える. このとき,

$$\mathrm{Im}(\Phi) = \{g(\alpha) \mid g(x) \in K[x]\} = M.$$

また, 定理 3-1 (2) から,

$$\begin{aligned} \ker(\Phi) &= \{g(x) \in K[x] \mid g(\alpha) = 0\} \\ &= \{h(x)f(x) \mid h(x) \in K[x]\} \\ &= (f(x)). \end{aligned}$$

よって, 準同型定理から

$$K[x]/(f(x)) = K[x]/\ker(\Phi) \simeq \mathrm{Im}(\Phi) = M.$$

また $(f(x))$ は $K[x]$ の極大イデアルであることが確かめられる (問題 4-2). よって, M は体である.

次に後半の主張についてみる. M の定義より $M \subseteq K(\alpha)$. 逆に, M は K と α を含む体なので, $K(\alpha)$ の最小性から $K(\alpha) \subseteq M$ も言える. よって $M = K(\alpha)$. また定理 4-1 より,

$$[K(\alpha) : K] = \dim_K K(\alpha) = \dim_K M = \deg f.$$

□

[**補足**] 上の証明から次の同型が成り立つ.

$$K[x]/(f(x)) \simeq K[\alpha] = K(\alpha) \quad \left(\overline{g(x)} \longmapsto g(\alpha) \right).$$

問題 4-2 $f(x) \in K[x]$ を体 K 上の既約モニック多項式とする. $K[x]$ が PID であることを利用して, $(f(x))$ が $K[x]$ の極大イデアルであることを示せ.

例題 4-2

$\alpha = \sqrt[3]{2}$ とする.

(1) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ を求めよ.

(2) α^2 の $\mathbb{Q}$ 上の最小多項式を求めよ.

(解答)

(1) $f(x) = x^3 - 2$ は α の $\mathbb{Q}$ 上の最小多項式である (例題 3-2 を参照). 定理 4-2 より

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 3.$$

(2) $g(x) = x^3 - 4$ と置くと, $g(\alpha^2) = 0$ である. また

$$\alpha^2 \in \mathbb{Q}(\alpha), \qquad \alpha = \frac{1}{2}(\alpha^2)^2 \in \mathbb{Q}(\alpha^2)$$

より $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$ が分かる. 従って

$$[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

よって, α^2 の $\mathbb{Q}$ 上の最小多項式の次数は 3 である. 従って, $g(x)$ は α^2 の $\mathbb{Q}$ 上の最小多項式である.

□

問題 4-3 $\alpha = \sqrt{2+\sqrt{2}}$ と置く.

(1) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ を求めよ.

(2) $\{1, 1+\alpha, 1+\alpha+\alpha^2, 1+\alpha+\alpha^2+\alpha^3\}$ は $\mathbb{Q}(\alpha)/\mathbb{Q}$ の基底であることを示せ.