体論 (第3回)

3. 最小多項式

今回は体の拡大を調べる上で必要となる最小多項式について解説する. また前回紹介した既約多項式との関係についてもみる.

定義 3-1
L/K を体の拡大, $\alpha \in L$ とする. 多項式 $f(x) \in K[x] \setminus \{0\}$ で $f(\alpha) = 0$ を満たすものが存在するとき, α を K **上代数的**と言う.

例えば, $\sqrt{-1}$ は $x^2 + 1 \in \mathbb{Q}[x]$ の根なので $\mathbb{Q}$ 上代数的である.

例題 3-1
$\alpha = \sqrt{2} + \sqrt{3}$ は $\mathbb{Q}$ 上代数的であることを示せ.

[証明]
$\alpha^2 = 5 + 2\sqrt{6}$ より $\alpha^4 - 10\alpha^2 + 1 = 0$. 従って, α は $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ の根より $\mathbb{Q}$ 上代数的である.

$\square$

[補足] 体 K の元 a は $x - a \in K[x]$ の根なので K 上代数的である.

問題 3-1

(1) $\alpha = \sqrt{\sqrt{2} + 1}$ が $\mathbb{Q}$ 上代数的であることを示せ.

(2) $\theta = \frac{2\pi}{5}$ とおくとき, $\cos\theta$ は $\mathbb{Q}$ 上代数的であることを示せ.

定理 3-1

L/K を体の拡大, $\alpha \in L$ を K 上代数的とする. $f(x)$ は α を根に持つ $K[x] \setminus \{0\}$ において最小次数の多項式とする.

(1) $f(x)$ は K 上既約である.

(2) $g(x) \in K[x]$ に対して次の同値が成り立つ.

$$g(\alpha) = 0 \iff f(x) \mid g(x).$$

(3) $h(x)$ も α を根に持つ $K[x] \setminus \{0\}$ において最小次数の多項式とする. このとき, $h(x) = cf(x)$ $(c \in K)$ と表せる.

[証明]

(1) $f(x)$ は K 上可約と仮定する. このとき,

$$f(x) = g_1(x)g_2(x), \quad \deg g_1 \geq 1, \quad \deg g_2 \geq 1$$

を満たす $g_1(x), g_2(x) \in K[x]$ が取れる. ここで,

$$0 = f(\alpha) = g_1(\alpha)g_2(\alpha)$$

より, $g_1(\alpha) = 0$ または $g_2(\alpha) = 0$. しかし, $\deg g_1 < \deg f$, $\deg g_2 < \deg f$ なので, $f(x)$ の最小性に矛盾. 従って, $f(x)$ は K 上既約である.

(2) $\Longleftarrow$ は明らか. $\Longrightarrow$ を示す. まず,

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

となる $q(x), r(x) \in K[x]$ を取る. ここで,

$$0 = g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

従って, $f(x)$ の最小性より $r(x) = 0$ を得る. よって $f(x) \mid g(x)$ である.

(3) $h(\alpha) = 0$ より $h(x) = g(x)f(x)$ となる $g(x) \in K[x]$ が存在する. 一方, $f(x)$ と $h(x)$ の最小性から $\deg f = \deg h$ が従う. よって $\deg g = 0$. 従って $g(x) = c$ $(c \in K)$ と表せる.

□

定義 3-2

L/K を体の拡大, $\alpha \in L$ を K 上代数的とする. $f(x)$ を α を根に持つ $K[x] \setminus \{0\}$ の最小次数のモニック多項式とする. このような $f(x)$ を **α の K 上の最小多項式**と言う.

[補足] 定理 3-1 (3) より最小多項式は一意的に存在することが分かる.

例 3-1
x^2+1 は $\sqrt{-1}$ の $\mathbb{Q}$ 上の最小多項式である.

[証明]
x^2+1 は $\sqrt{-1}$ を根に持つモニック多項式である. 一方, $\sqrt{-1}$ は $\mathbb{Q}$ 上の 1 次多項式の根にはなり得ないので, $\sqrt{-1}$ の $\mathbb{Q}$ 上の最小多項式は 2 次以上である. 従って, x^2+1 が $\sqrt{-1}$ の $\mathbb{Q}$ 上の最小多項式となる.

$\square$

次に最小多項式と既約多項式の関係をみる.

定理 3-2
L/K を体の拡大とし, モニック多項式 $f(x)\in K[x]$ は $\alpha\in L$ を根に持つとする. このとき, 次の二つは同値である.

(i) $f(x)$ は α の K 上の最小多項式.

(ii) $f(x)$ は K 上既約.

[証明]
(i)⇒(ii) は定理 3-1 (1) から従う.
(ii)⇒(i) を示す. $g(x)$ を α の K 上の最小多項式とする. $f(\alpha)=0$ より, 定理 3-1(2) から

$$f(x)=q(x)g(x) \quad (g(x)\in K[x])$$

と表せる. $\deg g\geq 1$ であり, $f(x)$ は K 上既約であるから $q(x)=c \ (c\in K)$ とかける. $f(x)$, $g(x)$ は共にモニックより $c=1$. 従って, $f(x)=g(x)$ を得る.

$\square$

例題 3-2

(1) $\alpha=\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式を求めよ.

(2) $\alpha=\sqrt[3]{2}$ のとき, $\alpha^2+\alpha$ が無理数であることを示せ.

[解答]
(1) $f(x)=x^3-2\in\mathbb{Q}[x]$ とする. $f(x)$ はモニック多項式で, $f(\alpha)=0$ を満たす. また, $f(x)$ は $p=2$ でアイゼンシュタインの定理の条件を満たすので $\mathbb{Q}$ 上既約である. 従って, 定理 3-2 から, $f(x)$ は α の $\mathbb{Q}$ 上の最小多項式である.

(2) $\alpha^2+\alpha\in\mathbb{Q}$ と仮定する. $\alpha^2+\alpha=c$ $(c\in\mathbb{Q})$ とし,

$$g(x)=x^2+x-c\in\mathbb{Q}[x]$$

と置けば, $g(\alpha) = 0$. これは α の $\mathbb{Q}$ 上の最小多項式が $x^3 - 2$ であることに反する. 従って $\alpha^2 + \alpha$ は無理数である.

$\square$

問題 3-2 $f(x) = x^3 + 2x + 1$ とし, α を $f(x)$ の実数根とする.

(1) $f(x)$ が α の $\mathbb{Q}$ 上の最小多項式であることを示せ.

(2) $\frac{1}{\alpha}$ の $\mathbb{Q}$ 上の最小多項式を求めよ.

問題 3-3 素数 p に対して, $\alpha = e^{\frac{2\pi i}{p}}$ の $\mathbb{Q}$ 上の最小多項式を求めよ.