最小多項式に関するまとめ

定理 体 K とその拡大体 L と $\alpha\in L$ と K 係数の 0 でない多項式 $F(x)\in K[x]$ で α を根に持つもの ($x=\alpha$ とすると 0 になるもの) について，以下の条件は互いに同値である.

(1) $F(x)$ は α の K 上での最小多項式である.
(F(x) は α を根に持つ 0 でない K 係数多項式の中で次数が最小のものである.)

(2) $F(x)$ は K 上既約である.

(3) 自然な環の準同型写像 $\overline{\varphi}: K[x]/(F(x))\to K(\alpha)$, $\overline{f(x)}\mapsto f(\alpha)$ は同型写像になる.

(4) $[K(\alpha):K]=\deg F(x)$.

以下の証明も大事だが，
以上の同値性は空気のごとく使われることに注意せよ!

証明

(1) ⇒ (2) の対偶　$F(x)$ は体 K 上既約でないと仮定する. そのとき，ある 1 次以上の $G(x), H(x)\in K[x]$ が存在して，$F(x)=G(x)H(x)$. このとき，$G(x), H(x)$ の次数は 1 次以上でかつ $F(x)$ の次数より真に小さくなる. $F(x)$ は α を根に持つので，$0=F(\alpha)=G(\alpha)H(\alpha)$. ゆえに $G(\alpha)=0$ または $H(\alpha)=0$.
ゆえに $F(x)$ は α の K 上での最小多項式ではない.

以下の設定をこの証明中で自由に使う.

環の準同型写像 $\varphi: K[x] \to K(\alpha)$ を $\varphi(f(x)) = f(\alpha)$ $(f(x) \in K[x])$ と定める.

$\mathrm{Ker}\,\varphi = \{f(x) \in K[x] \mid f(\alpha) = 0\}$ は $K[x]$ のイデアルになる.

$K[x]$ は PID なので $\mathrm{Ker}\,\varphi = (F_\alpha(x))$, $F_\alpha(x) \in K[x]$ と書ける. ←($F_\alpha(x)$ と $F(x)$ を区別せよ.)

$0 \neq F(x) \in \mathrm{Ker}\,\varphi$ なので $\mathrm{Ker}\,\varphi \neq \{0\}$ かつ $F_\alpha(x) \neq 0$.

$F_\alpha(x)$ は α の K 上での最小多項式になる (最小多項式の存在).

(証明 $0 \neq f(x) \in K[x]$ かつ $f(\alpha) = 0$ のとき, $f(x) \in \mathrm{Ker}\,\varphi = (F_\alpha(x))$ なので $f(x) = F_\alpha(x)\,g(x)$, $g(x) \in K[x]$ と書け, $g(x) \neq 0$ でなければいけない. $\deg f(x) \geqq \deg F_\alpha(x)$. ゆえに, そのような $f(x)$ の中で $F_\alpha(x)$ の次数は最小になっている.)

$F(x) \in \mathrm{Ker}\,\varphi = (F_\alpha(x))$ より, ある 0 でない $G(x) \in K[x]$ が存在して, $F(x) = F_\alpha(x)\,G(x)$.

(2) $\Rightarrow$ (1) の対偶　$F(x)$ は α の K 上での最小多項式ではないと仮定する.

そのとき $\deg F(x) > \deg F_\alpha(x)$ なので, 上の $F(x) = F_\alpha(x)\,G(x)$ より, $F(x)$ は K 上既約でないことがわかる.

以上によって, (1) $\Leftrightarrow$ (2) が示された.

(1) $\Rightarrow$ (3)　$F(x)$ は α の K 上での最小多項式であると仮定する.

そのとき, $\deg F(x) = \deg F_\alpha(x)$ なので, 上の $F(x) = F_\alpha(x) G(x)$ おいて, $G(x) \in K^\times$ となる. ゆえに, $(F(x)) = (F_\alpha(x)) = \mathrm{Ker}\,\varphi$ となる.

したがって環の準同型定理によって, 次の環の同型写像が得られる:

$\overline{\varphi} : K[x]/(F(x)) \xrightarrow{\sim} \mathrm{Im}\,\varphi$, $\overline{\varphi}(\overline{f(x)}) = f(\alpha)$.

(1) と (2) の同値性より, $F(x)$ は K 上既約になるので, PID に関する一般論より, $\mathrm{Ker}\,\varphi = (F(x))$ は $K[x]$ の極大イデアルになる.

(PID では既約元 a で生成される単項イデアルは極大イデアルになる.)

ゆえに, $K[x]/(F(x))$ は体になり, $\mathrm{Im}\,\varphi$ は K と α を含む L の部分体になることがわかる.

K と α を含む L の部分体は任意の $f(x) \in K[x]$ に対する $f(\alpha)$ も含むので, $\mathrm{Im}\,\varphi$ を含む.

$K(\alpha)$ は K と α を含む L の部分体の中で最小のもので, K と α を含む L の部分体 $\mathrm{Im}\,\varphi$ が $K(\alpha)$ に含まれていることになる. ゆえに, $\mathrm{Im}\,\varphi = K(\alpha)$.

これで, $\overline{\varphi} : K[x]/(F(x)) \xrightarrow{\sim} K(\alpha)$, $\overline{f(x)} \mapsto f(\alpha)$ という同型が得られた.

$(3) \Rightarrow (4)$ 同型 $K[x]/(F(x)) \cong K(\alpha)$, $\overline{f(x)} \leftrightarrow f(\alpha)$ が成立しているとき,

$$[K(\alpha):K] = \dim_K K(\alpha) = \dim_K K[x]/(F(x)) = \deg F(x).$$

$(4) \Rightarrow (1)$ α の K 上での最小多項式 $F_\alpha(x)$ について, $(1) \Rightarrow (3)$ の証明より,
同型 $K[x]/(F_\alpha(x)) \cong K(\alpha)$, $\overline{f(x)} \leftrightarrow f(\alpha)$ が得られ, $(3) \Rightarrow (4)$ の証明より,
$[K(\alpha):K] = \deg F_\alpha(x)$ が得られる.

$[K(\alpha):K] = \deg F(x)$ と仮定する. このとき, $\deg F(x) = \deg F_\alpha(x)$ なので,
$F(x)$ は α の K 上での最小多項式になる.

q.e.d.

注意 体 K とその拡大体 L と $\alpha \in L$ について, ある 0 でない $F(x) \in K[x]$ で α を根に持つものが存在するとき, α は K 上<u>代数的</u>であるという.
そうでないとき, α は K 上<u>超越的</u>であるという.

$\sqrt{2}$ や $\sqrt{-1}$ は $\mathbb{Q}$ 上代数的で, e や π は $\mathbb{Q}$ 上超越的である. $\square$

$\boxed{\text{使い方}}$ Lは体Kの拡大体であり$\alpha \in L$は体K上代数的な元であるとし，
$F(x)$はαのK上でのモニックな最小多項式であるとする．
MはLの拡大体であるとし，$F(x) = (x-\alpha_1)\cdots(x-\alpha_n)$，$\alpha_1, \dots, \alpha_n \in M$
と仮定する．（$K = \mathbb{Q}$の場合には$M = \mathbb{C}$と取れることが多い．）

このとき，$F(x)$はK上既約であり，$F(\alpha_i) = 0$なので，
$F(x)$は各α_iのK上での最小多項式にもなる．

α_iたちはαの$\underbrace{\text{共役元}}_{\text{K上での}}$

ゆえに，体の同型写像たち

$$\overline{\varphi} : K[x]/(F(x)) \xrightarrow{\sim} K(\alpha), \quad \overline{\varphi}_i : K[x]/(F(x)) \xrightarrow{\sim} K(\alpha_i)$$
$$\overline{f(x)} \longmapsto f(\alpha) \qquad\qquad \overline{f(x)} \longmapsto f(\alpha_i)$$

が得られ，次の体の同型写像を作れる：

$$\overline{\varphi}_i \circ \overline{\varphi}^{-1} : K(\alpha) \xrightarrow{\sim} K(\alpha_i), \quad f(\alpha) \mapsto f(\alpha_i) \quad (f(x) \in K[x]).$$

もしも$K(\alpha_i) = K(\alpha)$ならば，これは$K(\alpha)$の自己同型になる． □

$\boxed{\text{例}}$ $K=\mathbb{Q}$, $\alpha=\sqrt[3]{7}$ の場合. $\omega=e^{2\pi i/3}$ とおく.

α の $\mathbb{Q}$ 上での最小多項式は x^3-7 であり, その根の全体は $\underbrace{\alpha, \omega\alpha, \omega^2\alpha}_{\mathbb{Q}\text{上での}\alpha\text{の共役元}}$.

$\mathbb{Q}(\alpha)$, $\mathbb{Q}(\omega\alpha)$, $\mathbb{Q}(\omega^2\alpha)$ は互いに異なるが, 互いに体として同型になる:

$$\mathbb{Q}(\alpha)\cong\mathbb{Q}(\omega^k\alpha),\quad f(\alpha)\longleftrightarrow f(\omega^k\alpha)\quad (k\in\mathbb{Z},\ f(x)\in K[x]).$$

$\square$

$x^3-7=0$ の解を1つだけ $\mathbb{Q}$ に追加した場合

$\boxed{\text{例}}$ $K=\mathbb{Q}(\omega)$, $\omega=e^{2\pi i/3}$ で $\alpha=\sqrt[3]{7}$ の場合.

α の $K=\mathbb{Q}(\omega)$ 上での最小多項式も x^3-7 になる.

$K(\alpha)=K(\omega^k\alpha)$ $(k\in\mathbb{Z})$ が成立しており, $K(\alpha)$ の自己同型写像

$$\sigma: K(\alpha)\xrightarrow{\sim}K(\omega^k\alpha)=K(\alpha),\quad \sigma(f(\alpha))=f(\omega^k\alpha)\quad (k\in\mathbb{Z},\ f(x)\in K[x])$$

が得られる.

$K(\alpha)=\mathbb{Q}(\omega,\alpha)=\mathbb{Q}(\alpha,\omega\alpha,\omega^2\alpha)$ は $\mathbb{Q}$ に $x^3-7=0$ のすべての解を付け加えてできる体になっている.

$\square$

x^3-7 の解をすべて $\mathbb{Q}$ に追加した場合

$\boxed{\text{注意}}$ 共役元から作られる体の同型は本質的に最小多項式の話になっている. 初学者は最小多項式についてまず理解するとよい.

$\square$