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 係数のモニックな多項式 $F(x) \in K[x]$ 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 を根に持つモニックな 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 $(2) \Rightarrow (1)$, $(1) \Rightarrow (2)$（対偶）, $(1) \Rightarrow (3) \Rightarrow (4)$, $(4) \Rightarrow (1)$

$(1) \Rightarrow (2)$ 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次以上のモニックな $G(x), H(x) \in K[x]$ 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 $F_\alpha(x) \neq 0$. $F_\alpha(x)$ はモニックにとれる.

$F_\alpha(x)$ 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) ⇒ (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.
$F(x)$ も $F_\alpha(x)$ もモニックなので $F(x) = F_\alpha(x)$ となる. 特に, $(F(x)) = (F_\alpha(x)) = \operatorname{Ker}\varphi$ 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:

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

(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, $\operatorname{Ker}\varphi = (F(x))$ 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, $\operatorname{Im}\varphi$ は K と α を含む L の部分体になることがわかる.
したがって, $K(\alpha) \subset \operatorname{Im}\varphi$.

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 $\operatorname{Im}\varphi$ 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 $\operatorname{Im}\varphi$ が $K(\alpha)$ に含まれていることになる. したがって, $\operatorname{Im}\varphi \subset K(\alpha)$.

ゆえに, $\operatorname{Im}\varphi = K(\alpha)$.

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) ⇒ (4)　同型 $K[x]/(F(x)) \cong K(\alpha)$, $\overline{f(x)} \longleftrightarrow f(\alpha)$ 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) ⇒ (1)　α の K 上での最小多項式 $F_\alpha(x)$ について, (1) ⇒ (3) の証明より,

同型 $K[x]/(F_\alpha(x)) \cong K(\alpha)$, $\overline{f(x)} \longleftrightarrow f(\alpha)$ が得られ, (3) ⇒ (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 上代数的であるという.

そうでないとき, α は K 上超越的であるという.

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

$\boxed{\text{使い方}}$ 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

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

が得られ，次の体の同型写像を作れる:

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

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

$\boxed{例}$ $K=\mathbb{Q}$, $\alpha=\sqrt[3]{7}$ 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:

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

□

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

$\boxed{例}$ $K=\mathbb{Q}(\omega)$, $\omega=e^{2\pi i/3}$ 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.

□

x^3-7 の解をすべて $\mathbb{Q}$ に追加した場合

$\boxed{注意}$ 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.

□

定義 体Kの中で正の整数個の1の和 $1+1+\cdots+1$ が決して0にならないとき、Kの**標数は0**であるという。

正の整数Nで体Kの中でのN個の1の和が0になるものが存在するとき、Kは**正標数**であるといい、そのようなNの最小値をKの**標数**と呼ぶ。 □

メインの問題は次ページの問題です。

問題5-1 Kは標数0の体であるとし、Lはその任意の拡大体であるとする。K上の既約多項式がLの中に重根を持たないことを示せ。 □

問題5-2 正標数の体の標数が常に素数になることを示せ。 □

素数 p に対して、$\mathbb{F}_p = \mathbb{Z}/(p)$ とおく。

$\mathbb{F}_p$ は位数 p（元の個数が p）の体になり、$\mathbb{F}_p$ の標数も p になる。

注 用語的には 有理式 = 有理函数

体Kに対して、$K(x) = \left\{ \dfrac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in K[x],\ g(x) \neq 0 \right\}$ をK上の（1変数）**有理函数体**と呼ぶ。

x は文字

問題5-3 p は素数であるとし、$L = \mathbb{F}_p(t) =$（1変数 t の $\mathbb{F}_p$ 上の有理函数体）とおく。Lの部分体KとK上の既約多項式 $F(x) \in K[x]$ の組 $(K, F(x))$ でF(x)がLの中に重根を**持つ**ものの1つを具体的に構成せよ。 □

$\boxed{\mathbb{C}\text{の部分体の単拡大定理}}$ K は $\mathbb{C}$ の部分体であるとし, $\alpha_1, \dots, \alpha_r \in \mathbb{C}$ は K 上代数的であると仮定する. このとき, ある $\theta \in \mathbb{C}$ が存在して, $K(\alpha_1, \dots, \alpha_r) = K(\theta)$. □

この定理の証明 (講義でやったはず) を読んで以下の問いに答えよ. もしくは教科書を見よ.

$\boxed{\text{問題 5-4}}$ $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}(\theta)$ をみたす $\theta \in \mathbb{C}$ を具体的に与え, 実際にその等号が成立することを証明せよ. □

$\boxed{\text{問題 5-5}}$ 上の定理の $r = 2$ の場合の証明を書け. すなわち, 次を示せ:

K は $\mathbb{C}$ の部分体であるとし, $\alpha, \beta \in \mathbb{C}$ は K 上代数的であると仮定する.
このとき, ある $\theta \in \mathbb{C}$ が存在して, $K(\alpha, \beta) = K(\theta)$. □

$\boxed{\text{注意}}$ 上の定理は問題 5-5 の結果を使うと, 以下をみたす $\theta_1, \dots, \theta_{n-1} \in \mathbb{C}$ が次々に得られることからしたがう:

$K(\alpha_1, \alpha_2) = K(\theta_1)$, $K(\alpha_1, \alpha_2, \alpha_3) = K(\theta_1, \alpha_3) = K(\theta_2)$, $K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = K(\theta_2, \alpha_4) = K(\theta_3)$, …,
$K(\alpha_1, \dots, \alpha_{n-1}, \alpha_n) = K(\theta_{n-2}, \alpha_n) = K(\theta_{n-1})$. □