ALGEBRA III*

Hiroshi SUZUKI†
Department of Mathematics
International Christian University

2004 年度版

目 次

*教科書として、永尾汎著「代数学」朝倉書店 を指定。その関係で、証明なども、この教科書に負うところが多い。

†E-mail:hsuzuki@icu.ac.jp

1 体の拡大

定義 1.1 1. 体 K が、体 L の部分環であるとき、K は L の部分体、L は K の拡大体であると言い、$L:K$ と書く。

2. $L:K$ を体の拡大とし、$Y \subset L$ (部分集合) である時、$K \cup Y$ を含む L の部分体で最小のものを、K に Y を添加して得られた体と言い $K(Y)$ で表す。$Y = \{y_1, \ldots, y_n\}$ である時は、$K(Y)$ を $K(y_1, \ldots, y_n)$ とも書く。

3. ある L の元 α によって、$L = K(\alpha)$ と書けるとき、$L:K$ を単純拡大と言う。

例 1.1 $\boldsymbol{Q}(\sqrt{2}):\boldsymbol{Q}$、$\boldsymbol{Q}(\sqrt{2},\sqrt{3}):\boldsymbol{Q}$ は、ともに単純拡大である。後者は、明らかではないが、$\boldsymbol{Q}(\sqrt{2},\sqrt{3}) = \boldsymbol{Q}(\sqrt{2}+\sqrt{3})$ が得られるので、このことから分かる。Exercise 1.3 参照。

定義 1.2 $L:K$ を体の拡大とし、$\alpha \in L$ とする。

1. 零でない多項式 $p(x) \in K[x]$ で、$p(\alpha) = 0$ となるものがあるとき、α を K 上代数的な元と呼び、そうでないとき、すなわち、$1, \alpha, \ldots, \alpha^n, \ldots$ が K 上で一次独立の時、 α を K 上超越的な元と呼ぶ。

2. $\alpha \in L$ が K 上代数的であるとき、$m(\alpha) = 0$ となる零でない多項式 $m(x) \in K[x]$ で、次数最小、monic (最高次の係数が 1) なものを、α の最小多項式と呼ぶ。

命題 1.1 $L:K$ を体の拡大とし、α を K 上代数的な L の元、$m(x) \in K[x]$ を α の最小多項式とする。このとき、次が成立する。

(1) $m(x)$ は、既約。

(2) $f(x) \in K[x]$ が、 $f(\alpha) = 0$ を満たせば、$m(x)$ は、$f(x)$ を割り切る。特に、最小多項式はただ一つであり、さらに、$f(x) \in K[x]$ が、既約な *monic* な多項式で、$f(\alpha) = 0$ ならば、$f(x) = m(x)$ すなわち、$f(x)$ は、最小多項式である。

(3) $K(\alpha) \simeq K[x]/(m(x))$。

(4) $K(\alpha) = K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \mid a_i \in K\}$ であり、$1, \alpha, \ldots, \alpha^{d-1}$ は、K 上 一次独立である。ただし、$\deg m(x) = d$ とする。

証明 (1) $m(x) = m_1(x)m_2(x)$、$\deg m_1(x)$, $\deg m_2(x) < d$ とすると、$0 = m(\alpha) = m_1(\alpha)m_2(\alpha)$ すなわち、$m_1(\alpha) = 0$ または、$m_2(\alpha) = 0$ を得る。しかし、これは、$m(x)$ が、$m(\alpha) = 0$ となる、零でない最小次数の多項式であることに反する。

(2), (3), (4) $\phi : K[x] \to L$ を $f(x)$ の x に α を代入する写像とすると、これは、$\mathrm{Im}\phi = K[\alpha]$ となる環準同型写像である。零写像ではないから、$\mathrm{Ker}\phi$ は、$0 \neq m(x)$ を含む、全体でも零でもないイデアルである。$K[x]$ は、単項イデアル整域であるから、$\mathrm{Ker}\phi = (p(x))$

となる monic な多項式がある。$m(x) \in (p(x))$ かつ、(1) より、$m(x)$ が既約であることより、$p(x) = m(x)$ を得る。命題 II.4.4 より、$(p(x))$ は、極大イデアル、すなわち、$K[\alpha] \simeq K[x]/(p(x))$ は、体である。従って、$K(\alpha)$ が、K と α を含む、最小の部分体であることより、$K[\alpha] = K(\alpha)$ を得る。一方、$m(x)$ は、$m(\alpha) = 0$ となる多項式の中で、次数が最小であったから、$1, \alpha, \ldots, \alpha^{d-1}$ は、K 上 一次独立である。さらに、$f(x) \in K[x]$ とし、

$$f(x) = q(x)m(x) + r(x),\ \deg r(x) < d = \deg m(x),\ q(x),\ r(x) \in K[x]$$

とすると、$f(\alpha) = r(\alpha)$。これより、

$$K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \mid a_0, \ldots, a_{d-1} \in K\}$$

も得る。 ■

命題 1.2 *K を体、$m(x)$ を K 上既約な monic な多項式とする。このとき、拡大 $K(\alpha) : K$ で、α の最小多項式が $m(x)$ となるものがある。*

証明 $\pi : K \longrightarrow K[x] \longrightarrow K[x]/(m(x))$ を自然な写像とすると、π は単射。$\pi(K)$ を K と同一視すると、$K \subset K[x]/(m(x)) = L$ は、体である。$\alpha = x + (m(x))$ とする。明らかに、L において、$m(\alpha) = m(x) + (m(x)) = (m(x)) = 0$ だから、$m(x)$ は、命題 1.1 より、α の最小多項式となる。 ■

定義 1.3 *$i : R_1 \longrightarrow R_2$ を環準同型とする。このとき、R_1、R_2 を係数とする多項式環の間の写像 $\hat{i} : R_1[x] \longrightarrow R_2[x]$ を次のように定義する。*

$$a_0 + a_1x + \cdots + a_sx^s \mapsto i(a_0) + i(a_1)x + \cdots + i(a_s)x^s.$$

すると、$\hat{i}$ は、環準同型写像である。さらに、i が同型写像なら、$\hat{i}$ も 同型写像である。

次の定理は、この講義のあらゆる場面で、鍵となるものである。

定理 1.3 *$i : K \to L$ を体同型、$K(\alpha) : K$、$L(\beta) : L$ を体の拡大とし、α を K 上代数的、β を L 上代数的とする。$m(x)$ が K 上 α の最小多項式とする。もし、$\hat{i}(m(x))$ が L 上 β の最小多項式ならば、体同型 $j : K(\alpha) \longrightarrow L(\beta)$ で、$j_{|K} = i$、$j(\alpha) = \beta$ となるものが存在する。*

証明 $d = \deg m(x) = \deg(\hat{i}(m(x))) = d$ とする。

$$\pi : K[x] \xrightarrow{\hat{i}} L[x] \longrightarrow L[x]/((\hat{i}(m(x))) \simeq L[\beta] = L(\beta)$$

とすると、明らかに、$(m(x)) \subset \mathrm{Ker}\pi$。逆に、$f \in \mathrm{Ker}\pi$ とすると、$\hat{i}(f(x)) \in (\hat{i}(m(x)))$ を得る。$\hat{i}$ は、同型写像だから、$f(x) \in (m(x))$ を得る。これより、

$$K(\alpha) \simeq K[\alpha] \simeq K[x]/(m(x)) \simeq \mathrm{Im}\,\pi = L[x]/(\hat{i}(m(x)) \simeq L[\beta] = L(\beta)$$

となる。この同型対応が、定理の主張を満たすことは、明らか。 ■

上の定理は、$K[\alpha]$ の元、$a_0+a_1\alpha+\cdots+a_{d-1}\alpha^{d-1}$ を自然に $i(a_0)+i(a_1)\alpha+\cdots+i(a_{d-1})\alpha^{d-1}$ に対応する対応が、同型写像であることを示している。このようにしてみると、全単射は、明らかであるが、積が保たれることを示す必要がある。

例 **1.2** 1 の原始 3 乗根、すなわち、x^2+x+1 の根を ω とすると、$\boldsymbol{Q}$ 上の既約多項式 x^3-2 の根は、$\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ である。上の定理により、$\boldsymbol{Q}(\sqrt[3]{2})$ から、$\boldsymbol{Q}(\sqrt[3]{2}\omega)$ への同型写像で、$\sqrt[3]{2}$ を $\sqrt[3]{2}\omega$ に移すものが存在することが分かる。このように、定理 1.3 は、ある条件を満たす同型写像の存在を示すときに有効である。

2 拡大の次数と作図問題

定義 **2.1** $L:K$ を体の拡大とする。演算を次のように定義する。

$$(\lambda,u)\mapsto \lambda u\ (\lambda\in K,\ u\in L),\ (u,v)\mapsto u+v\ (u,v\in L).$$

すると、L は、K 上のベクトル空間になる。このときの次元 $\dim_K L$ を体の拡大 $L:K$ の次数と呼び、$[L:K]$ と書く。

定理 **2.1** $M:L$、$L:K$ を体の拡大とする。このとき、次が成立する。

$$[M:K]=[M:L][L:K].$$

証明

- $\{x_i \mid i\in I\}$ を L の K 上の基底。
- $\{y_j \mid j\in J\}$ を M の L 上の基底。

このとき、$\{x_iy_j \mid i\in I,\ j\in J\}$ が M の K 上の基底であることを示せば良い。

(一次独立なこと) $k_{ij}\in K$ $(i\in I,\ j\in J)$ とし

$$0=\sum_{i\in I,\ j\in J}k_{ij}x_iy_j=\sum_{j\in J}\left(\sum_{i\in I}k_{ij}x_i\right)y_j$$

が成立しているとする。$\sum_{i\in I}k_{ij}x_i\in L$ であることを考えると、$\{y_j \mid i\in J\}$ が L 上の一次独立であることから、$\sum_{i\in I}k_{ij}x_i=0$ が全ての、$j\in J$ について、成立することが分かる。同様にして、$\{x_i \mid i\in I\}$ が K 上の一次独立であることから、$k_{ij}=0$ が全ての、$i\in I$、$j\in J$ について、成立することが分かる。従って、一次独立である。

(生成すること) $x\in M$ とする。$\{y_j \mid i\in J\}$ が M の L 上の基底であることから、$l_j\in L$ $(j\in J)$ で、$x=\sum_{j\in J}l_jy_j$ を満たすものが存在する。また、$\{x_i \mid i\in I\}$ が L の K

上の基底であることから、各 $j \in J$ について、$k_{ij} \in K$ $(i \in I)$ で、$l_j = \sum_{i \in I} k_{ij} x_i$ を満たすものが存在する。これを代入すると、

$$x = \sum_{j \in J} l_j y_j = \sum_{i \in I,\, j \in J} k_{ij} x_i y_j$$

従って、M の元は、$\{x_i y_j \mid i \in I,\, j \in J\}$ の K 係数の一次結合で書けることが分かる。■

注　上の定理は、集合の濃度の演算を用いれば、無限の場合も成立する。

命題 **2.2** $K(\alpha) : K$ を単純拡大とする。このとき、次が成立する。

(1) α が K 上超越的ならば、$[K(\alpha) : K] = \infty$。

(2) α が K 上代数的で、$m(x)$ をその最小多項式とする。すると、$[K(\alpha) : K] = \deg m$。

証明　命題 1.1 より明らか。■

定義 **2.2** $L : K$ を体の拡大とする。$[L : K] < \infty$ のとき、$L : K$ を有限次拡大であるという。また、L の各元が K 上代数的であるとき、代数拡大と呼ぶ。

命題 **2.3** $L : K$ を体の拡大とする。このとき、$[L : K] < \infty$ であることと、K 上代数的な元、$\alpha_1, \ldots, \alpha_t \in L$ で $L = K(\alpha_1, \ldots, \alpha_t)$ となるものがあることとは、同値である。さらにこのとき、$L : K$ は、代数拡大である。

証明　$K(\alpha_1, \ldots, \alpha_i) = K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)$ だから、$\alpha_1, \ldots, \alpha_t$ が 代数的ならば、

$$[K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})] \leq [K(\alpha_i) : K] < \infty.$$

帰納法により、定理 2.1 を適用する事により、$[L : K] < \infty$。

逆に、$[L : K] = n < \infty$ とする。$\alpha_1, \ldots, \alpha_t$ を K 上の基底とすると、$L = K(\alpha_1, \ldots, \alpha_t)$。従って、$L : K$ が代数的であることを示せばよい。$\alpha \in L$ とすると、仮定より $n+1$ 個の元, $1, \alpha, \alpha^2, \ldots, \alpha^n$ は、一次独立ではあり得ない。従って、α は、零ではない n 次以下の多項式の根である。■

以下作図問題について考える。

与えられた点集合 $\boldsymbol{R}^2 \supset P$ から、定規によっては、P の 2 点を通る直線を引く。コンパスによっては、P の 2 点間の距離に等しい半径の円を P の点を中心に描くものとする。$\boldsymbol{R}^2 \supset P_0$ を点の集合とする。P_0 からはじめて、上の操作を続けて行って得られる点の集合 P を P_0 から作図可能という。

- $P = P_0 \cup \{r_1, r_2, \ldots, r_n\},\ r_i = (x_i, y_i)\ (i = 1, \ldots, n),$
- $P_0 = \{p_1, p_2, \ldots, p_s\},\ p_j = (x'_j, y'_j)\ (j = 1, \ldots, s),$

- $K_0 = \boldsymbol{Q}(x'_1, \ldots, x'_s, y'_1, \ldots, y'_s)$, $K_i = K_{i-1}(x_i, y_i)$, $(i = 1, \ldots, n)$

とする。

命題 2.4 $[K_{i-1}(x_i) : K_{i-1}] \leq 2$ かつ、$[K_{i-1}(y_i) : K_{i-1}] \leq 2$ $(i = 1, \ldots, n)$。

証明　新しい点が作図されるのは、直線と直線の交点、直線と円の交点、円と円の交点である。いずれの場合も、2次または、1次の方程式の根として、得られるので、x_i、y_i の、K_{i-1} 上の最小多項式の次数は、1または、2である。 ■

定理 2.5 点 $r = (x, y)$ が、P_0 から作図可能ならば、$[K_0(x) : K_0]$、$[K_0(y) : K_0]$ は、ともに2べきである。

証明　$[K_i : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}]$ だから、命題 2.4 より、$[K_i : K_{i-1}]$ は、$1, 2, 4$ のいずれかとなる。従って、帰納法により、$[K_n : K_0]$ も2べきとなる。$x \in K_n$ とすると、$[K_n : K_0] = [K_n : K_0(x)][K_0(x) : K_0]$ より、$[K_0(x) : K_0]$ が2べきであることを得る。$[K_0(y) : K_0]$ についても同様。 ■

例 2.1　1. $(\sqrt[3]{2}, 0)$ は、$(0, 0)$、$(1, 0)$ から作図できない。この場合は、$K_0 = \boldsymbol{Q}$ となり、$[\boldsymbol{Q}(\sqrt[3]{2}) : \boldsymbol{Q}] = 3$ であることから、不可能であることが導ける。これは、立体倍積問題と呼ばれる問題である。

2. $\pi/3$ は、3等分出来ない。$\theta = \pi/3$ とすると、

$$1/2 = \cos \pi/3 = \cos 3\theta = 4\cos^3 \theta - 3\cos \theta$$

だから、$\cos\theta$ は、$\boldsymbol{Q}$ 上3次の既約多項式の根である。従って、$[\boldsymbol{Q}(\cos\theta) : \boldsymbol{Q}] = 3$ となり、作図が不可能であることが得られる。

3　自己同型、不変体、分解体

定義 3.1 $L : K$ を体の拡大とする。

1. L の自己同型（環としての全単射）σ が、K-自己同型であるとは、$\sigma(k) = k$ がすべての $k \in K$ について、成り立つことである。

2. L の K-自己同型全体を、拡大 $L : K$ のガロア群 (Galois Group) といい、$\Gamma(L : K)$ とかく。$\Gamma(L : K)$ は、写像の合成に関して、群になる。

定義 3.2 $L : K$ を体の拡大、$G = \Gamma(L : K)$ を拡大 $L : K$ のガロア群とする。

1. $K \subset M \subset L$ なる体 M を中間体 (intermidiate field) と言う。

2. M が拡大 $L : K$ の中間体のとき、$M^* = \Gamma(L : M)$ とする。$M^* \leq K^* = G$ である。

3. $H \leq G$ のとき、$H^+ = \{a \in L \mid \sigma(a) = a \text{ for all } \sigma \in H\}$ は、拡大 $L : K$ の中間体である。これを、H の不変体という。

これによって、体の拡大 $L : K$ の中間体全体と、$G = \Gamma(L : K)$ の部分群全体との間に $*$ と $+$ により対応が定義できる。Galois は、拡大 $L : K$ がある性質（正規性・分離性）を満たすとき、この対応は、包含関係を逆にする全単射であることを示した。

例 **3.1** $\Gamma(\boldsymbol{C} : \boldsymbol{R}) = \{1 = id_{\boldsymbol{C}}, \sigma\}$、$\sigma(\alpha) = \bar{\alpha}$ 複素共役。
$\tau \in \Gamma(\boldsymbol{C} : \boldsymbol{R})$ とする。$\boldsymbol{C} = \boldsymbol{R}(i) = \{a + bi \mid a, b \in \boldsymbol{R}\}$ であることに注意すると、σ は、$\boldsymbol{R}$ の元を変えないから、

$$\tau(a + bi) = \tau(a) + \tau(b)\tau(i) = a + b\tau(i)$$

よって、$\tau(i)$ だけによって、τ は、決定される。また、

$$\tau(i)^2 = \tau(i^2) = \tau(-1) = -1$$

であるから、$\tau(i) = \pm i$。これより、$\tau \in \{id_{\boldsymbol{C}},\ \sigma\}$ を得る。i を $-i$ に移す自己同型が実際存在することは、直接的にも計算で証明できるが、定理 1.3 も有効である。

例 **3.2** $\Gamma(\boldsymbol{Q}(\sqrt[3]{2}) : \boldsymbol{Q}) = 1$
$c = \sqrt[3]{2}$ とおく。$\tau \in \Gamma(\boldsymbol{Q}(\sqrt[3]{2}) : \boldsymbol{Q})$ とすると、

$$\tau(c)^3 = \tau(c^3) = \tau(2) = 2.$$

従って、$\tau(c) \in \{c, c\omega, c\omega^2\}$、$\omega = (-1 + \sqrt{-3})/2$ (1 の原始 3 乗根) であるが、$\tau(c) \in \boldsymbol{Q}(\sqrt[3]{2}) \subset \boldsymbol{R}$ であるから、$\tau(c) = c$ となる。$\boldsymbol{Q}(\sqrt[3]{2})$ は、$\boldsymbol{Q}$ と、$\sqrt[3]{2}$ で生成された体であるから、$\tau(c) = c$ ならば、τ は、恒等写像となる。

ガロアの定理の成り立つ条件は、体の拡大 $L : K$ のガロア群が、十分たくさん元を持っているすなわち、拡大の次数と同じだけ L の K-自己同型を持つということである。上の例では、拡大 $\boldsymbol{C} : \boldsymbol{R}$ は、その条件を満たすが、$\boldsymbol{Q}(\sqrt[3]{2}) : \boldsymbol{Q}$ は、その条件を持たしていない。上の考察から、それは、単純拡大の場合、その生成元の最小多項式の根を全て含むかどうかが関係していることが分かる。このことをふまえ、以下、分解体を定義し、これについて考える。

定義 **3.3** K を体、$f(t) \in K[t]$ を多項式とする。

1. $f(t)$ が K 上で分解 (split) しているとは、K の元 $k, \alpha_1, \ldots, \alpha_n$ が存在して、$f(t) = k(t - \alpha_1) \cdots (t - \alpha_n)$ と書けること、すなわち、$f(t)$ が K の中で、一次因子に分解していることを言う。

2. 体 Σ が、f に対する K の分解体であるとは、以下の条件を満たすことである。

(a) f は、Σ で分解している。

(b) $K \subset \Sigma' \subset \Sigma$ で f が体 Σ' で分解していれば、$\Sigma' = \Sigma$。

すなわち、Σ は、f が分解する極小の体ということである。上の 2 番目の条件は、次の条件にも置き換えることが出来る。

(c) $\Sigma = K(\alpha_1, \ldots, \alpha_n)$、$\alpha_1, \ldots, \alpha_n$ は、f の Σ における根。

定理 3.1 K を体 $f(t) \in K[t]$ とする。このとき、K 上 f の分解体が存在する。

証明　$\deg f$ に関する帰納法で証明する。f が K で分解していれば、$\Sigma = K$ にすればよい。特に、$\deg f = 1$ のときは、分解体は存在する。

$\deg f > 1$ かつ、f は、K で分解していないとする。このときは、f の既約因子 f_1 で、$\deg f_1 > 1$ なるものがある。f_1 は、monic として良い。命題 1.2 より、K の拡大 $K(\alpha) : K$ で、α の最小多項式が f_1 となるものがある。$f \in K(\alpha)[t]$ で $f = (t - \alpha)g$、$g \in K(\alpha)[t]$、$\deg g = \deg f - 1$ と書ける。帰納法の仮定より、$K \subset K(\alpha) \subset \Sigma$ となる拡大体で Σ は、$K(\alpha)$ 上 g の分解体となるものがある。$\alpha_1, \ldots, \alpha_n$ を g の Σ 内の根とすると、

$$\Sigma = K(\alpha)(\alpha_1, \ldots, \alpha_n) = K(\alpha, \alpha_1, \ldots, \alpha_n)$$

だから、Σ は、K 上 f の分解体である。 ■

命題 3.2 $i : K \to K'$ を 体同型、$f \in K[t]$、Σ を K 上 f の分解体とする。また、L を $\hat{i}(f)$ が L で分解するような K' の拡大体とする。このとき、単射準同型 $j : \Sigma \to L$ で $j_{|K} = i$ すなわち、K 上では、i となっているものが存在する。

証明　$\deg f$ に関する帰納法で示す。$f(t) = k(t - \alpha_1) \cdots (t - \alpha_n)$ と $\Sigma[t]$ の中で、分解できているとする。m を K 上での α_1 の最小多項式とし、

$$f = mh = (t - \alpha_1)g, \ \text{ in } \Sigma[t]$$

とする。$\hat{i}(f) = \hat{i}(m)\hat{i}(h)$ と書け、$\hat{i}$ が同型写像であることより、$\hat{i}(m)$ は、K' 上既約である。L 上で、

$$\hat{i}(m) = (t - \beta_1) \cdots (t - \beta_r), \ \beta_1, \ldots, \beta_r \in L$$

と分解できているとする。定理 1.3 より、同型写像 $j_1 : K(\alpha_1) \to K(\beta_1)$ で、$j_{1|K} = i$、$j_1(\alpha_1) = \beta_1$ となっているものが存在する。Σ は、多項式 g に対する $K(\alpha_1)$ 上の分解体だから帰納法の仮定により、同型写像 $j : \Sigma \to L$ で、$j_{|K(\alpha_1)} = j_1$ となるものがある。明らかに、$j_{|K} = j_{1|K} = i$ だから、命題が証明された。 ■

定理 3.3 $i : K \to K'$ を体同型、$f \in K[t]$ とする。T を f の K 上の分解体、T' を $\hat{i}(f)$ の K' 上の分解体とする。このとき、同型写像 $j : T \to T'$ で、$j_{|K} = i$ となるものが存在する。

証明　命題 3.2 より、単射準同型写像 $j : T \to T'$ で $j_{|K} = i$ となるものが存在する。$\hat{i}(f)$ は、$j(T)$ で分解するから、分解体の極小性より、$j(T) = T'$ を得る。従って、j は、同型写像である。 ■

例 **3.3** $f(t) = (t^3 + 1)(t^2 - 3)$ とすると、この多項式の $\boldsymbol{C}$ 内の根は、

$$-1,\ \frac{1+\sqrt{3}i}{2},\ \frac{1-\sqrt{3}i}{2},\ \sqrt{3},\ -\sqrt{3}$$

だから、分解体は、

$$\boldsymbol{Q}(-1, \frac{1+\sqrt{3}i}{2}, \frac{1-\sqrt{3}i}{2}, \sqrt{3}, -\sqrt{3}) = \boldsymbol{Q}(\sqrt{3}, i)$$

である。

練習問題 **3.1** $L : K$ を有限次拡大とする。この時、$\Gamma(L : K)$ の位数は有限であることを示せ。さらに、一般に、$N : K$ を体の拡大とすると、L から N の中への K-単射準同型の数は有限である。

4　正規性と分離性

定義 **4.1** 体の拡大 $L : K$ が正規であるとは、L において、少なくとも一つの根を持つ K 上の既約多項式 f は、全て、L において分解している時を言う。

例 **4.1** 2 次の拡大は、常に、正規拡大である。なぜなら、$L : K$ が 2 次の拡大とすると、K 上既約で、L に根を持つ多項式は、次数が高々 2 で、根と係数の関係から、片方が、L に含まれれば、他方も含まれるからである。特に、$\boldsymbol{C} : \boldsymbol{R}$ は、正規拡大である。

例 **4.2** 「代数学の基本定理」によってすべての $\boldsymbol{C}$ 上の多項式は、$\boldsymbol{C}$ において、分解する。このことにより、K を $\boldsymbol{C}$ の部分体とすると、$\boldsymbol{C} : K$ は、常に、正規拡大である。

注　「代数学の基本定理」は、名前とは異なり、証明には、$\boldsymbol{C}$ の解析的な性質を用いる。いくつかの、証明が知られている。もっとも、代数的な証明としては、$\boldsymbol{R}$ 上の奇数次の多項式は、必ず、実数解を持つことを用い、Sylow の定理から示す方法も知られている。

例 **4.3** 体の拡大 $\boldsymbol{Q}(\sqrt[3]{2}) : \boldsymbol{Q}$ は、正規ではない。$t^3 - 2$ は、この拡大の中に、一つは根を持つが、分解しているわけではない。$\boldsymbol{Q}(\sqrt[3]{2}, \omega)$、$\omega = (-1 + \sqrt{-3})/2$ ならば、$t^3 - 2$ は、分解している。定義からは直接これが、正規かどうか分からないが、下の定理から分かるように、ある多項式の分解体は、正規拡大であることが分かる。

定理 **4.1** 体の拡大 $L : K$ が有限かつ正規であるという事と、L が、K 上ある多項式の分解体であることとは、同値である。

証明　$L:K$ は、有限かつ正規拡大とする。すると、命題 2.3 より、L の元 $\alpha_1, \alpha_2, \ldots, \alpha_n$ で、$L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ となるものがある。$m_i\ i = 1, 2, \ldots, n$ を、α_i の K 上の最小多項式、$f = m_1 m_2 \cdots m_n$ とすると、$L:K$ が、正規であることより f は、L で分解、よって、L は、K 上 f の分解体である。

逆に L を K 上 g の分解体 $\alpha_1, \alpha_2, \cdots, \alpha_n$ をその根とする。$\alpha_1, \alpha_2, \cdots, \alpha_n$ は、K 上代数的だから、命題 2.3 より、$L = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$ は、K 上有限である。f を L に根を持つ K 上の既約多項式とする。$\theta_1 \in L$、$f(\theta_1) = 0$ とする。M を $L \subset M$ なる、fg の分解体とする。$\theta_2 \in M$、$f(\theta_2) = 0$ とし、以下、$\theta_2 \in L$ を示す。$i = 1, 2$ としたとき、

$$L(\theta_i) = K(\alpha_1, \alpha_2, \cdots, \alpha_n)(\theta_i) = K(\theta_i)(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

だから、$L(\theta_i)$ は、$K(\theta_i)$ 上 g の分解体である。一方 定理 1.3 により、$K(\theta_1)$ から、$K(\theta_2)$ への同型写像 σ で、$\sigma_{|K} = id_K$ となるものがある。また、定理 3.3 により、$L(\theta_1)$ から、$L(\theta_2)$ への同型写像 $\tilde{\sigma}$ で、$\tilde{\sigma}_{|K(\theta_1)} = id_{K(\theta_1)}$ となるものがある。これにより、

$$[L(\theta_1) : K(\theta_1)] = [L(\theta_2) : K(\theta_2)],\ [K(\theta_1) : K] = [K(\theta_2) : K].$$

$\theta_1 \in L$ だから、

$$\begin{aligned} [L:K] &= [L(\theta_1) : K] = [L(\theta_1) : K(\theta_1)][K(\theta_1) : K] \\ &= [L(\theta_2) : K(\theta_2)][K(\theta_2) : K] = [L(\theta_2) : K] \\ &= [L(\theta_2) : L][L : K] \end{aligned}$$

従って、$L(\theta_2) = L$。これより、$\theta_2 \in L$。従って、$L:K$ は、正規拡大である。 ■

定義 4.2 f を体 K 上の既約多項式とする。

1. f が、f の分解体において、重根を持たないとき、f を分離的または、分離多項式と言う。(分解体は、同型であるから、この定義は、分解体の取り方によらない。)
2. f が、分離的ではないとき、f を非分離的と言う。

定義 4.3 K を体とし、$f(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t]$ とする。このとき、

$$Df = a_1 + 2a_2 t + \cdots + n a_n t^{n-1}$$

を f の形式的微分という。

形式的微分に関しては、次が成り立つ。

$$D(f+g) = Df + Dg,\ D(fg) = Df \cdot g + f \cdot Dg,\ D(\lambda g) = \lambda Dg.$$

命題 4.2 K を体、$0 \neq f \in K[t]$ とする。f が、分解体において、多重根を持つと言うことと、$K[t]$ において、$(f, Df) \neq 1$ と言うこととは、同値である。

証明　f の分解体 Σ 上で、$f(t)=(t-\alpha)2g(t)$、$\alpha\in\Sigma$ とする。$Df=(t-\alpha)((t-\alpha)Dg+2g)$ より、$\Sigma[t]$ で、$(f,Df)\neq 1$ である。α の K 上の最小多項式を、m とすると、命題 1.1 より、m は、f、Df を割り切る。従って、$K[t]$ で、$(f,Df)\neq 1$ である。

f が、多重根を持たないとする。$\deg f$ による帰納法で、$\Sigma[t]$ で、$(f,Df)\neq 1$ を言う。$\deg f=1$ の時は、$Df\in K-\{0\}$ より、明らか。

$\deg f\geq 2$ のとき、$f=(t-\alpha)g$、かつ、f は、重根を持たないから、g は、$t-\alpha$ では割り切れない。従って、$Df=(t-\alpha)Dg+g$。帰納法の仮定から $(g,Dg)=1$。Σ は、f の分解体だから、f の既約因子は、すべて、1 次。$t-\beta$ を　g の因子とすると、$\alpha\neq\beta$ より、$t-\beta$ は、Df を割り切れず、$\Sigma[t]$ で、$(f,Df)=1$。特に、$K[t]$ でも、$(f,Df)\neq 1$ が得られる。 ■

命題 **4.3**　(1) $\mathrm{char}K=0$ ならば、K 上の任意の既約多項式は、K 上分離的である。

(2) $\mathrm{char}K=p>0$ ならば、K 上の既約多項式 f が非分離的だと言うことと、$f(t)\in K[t^p]$ となっていることとは、同値。すなわち、$f(t)$ は、以下のように書ける。

$$f(t)=a_0+a_1t^p+\cdots+a_rt^{rp},\ a_i\in K,\ i=0,1,\ldots,r.$$

証明　f を K 上既約かつ、非分離な多項式とする。すると、命題 4.2 より、$(f,Df)\neq 1$ である。ここで、f は、既約であり、Df は、f よりも次数が低いから、$Df=0$ でなければならない。一方、$f(t)=c_0+c_1t+\cdots+c_nt^n$ とすると、$Df(t)=c_1+2c_2t+\cdots+nc_nt^{n-1}$ だから、$ic_i=0$ が、各 i について成り立たなければならない。すなわち、$c_i\neq 0$ ならば、$i=0$ が、K の中で、成り立たなければならない。これは、標数 が正であり、かつ $p\mid i$ を意味する。従って、$f(t)\in K[t^p]$ を得る。 ■

定義 **4.4**　$L:K$ を体の拡大とする。

1. $f\in K[t]$ のすべての既約因子が、K 上分離的であるとき、f は、K 上分離的であると言う。

2. $\alpha\in L$ が、K 上代数的であって、かつ α の最小多項式が K 上分離的であるとき α は、K 上分離的であると言う。

3. L の元がすべて、K 上分離的であるとき、$L:K$ を分離拡大という。

命題 **4.4**　$L:K$ を分離的な体の拡大とし、M をその中間体とする。このとき、$L:M$、$M:K$ は、共に分離的である。

証明　$M:K$ が分離的であるのは、定義より明らか。$\alpha\in L$、m_M を α の M 上の最小多項式、m_K を K 上の最小多項式とすると、m_M は m_K を割り切る。仮定より、m_K は、その分解体において重根を持たないから、m_M もそうであり、α は、M 上分離的でもある。 ■

5　次数と位数

命題 5.1 K、L を体とするとき、K から L への相異なる単射準同型 $\lambda_1, \ldots, \lambda_n$ は、L 上で一次独立である。すなわち、$a_1, \ldots, a_n \in L$ に対して、

$$a_1\lambda_1(x) + \cdots + a_n\lambda_n(x) = 0 \ \ for\ all\ x \in K \Rightarrow a_1 = \cdots = a_n = 0.$$

証明　n に関する帰納法で示す。$n = 1$ の時、$a_1\lambda_1(x) = 0$ が、すべての $x \in K$ について成立すると、$\lambda_1(1) = 1 \neq 0$ だから、$a_1 = 0$ を得る。

$n - 1$ の時には成立するとする。$a_1, \ldots, a_n \in L$ に対して、

$$a_1\lambda_1(x) + \cdots + a_n\lambda_n(x) = 0 \tag{1}$$

がすべての $x \in K$ について成立するとする。$a_1 = 0$ ならば、$n - 1$ 個の場合に帰着出来るから、$a_1 \neq 0$ とする。$\lambda_1 \neq \lambda_n$ だから、K の元 y で、$\lambda_1(y) \neq \lambda_n(y)$ となるものがある。式 (1) の x に xy を代入したものと、式 (1) に、$\lambda_n(y)$ をかけたものを考える。

$$a_1\lambda_1(y)\lambda_1(x) + \cdots + a_n\lambda_n(y)\lambda_n(x) = 0 \tag{2}$$
$$a_1\lambda_n(y)\lambda_1(x) + \cdots + a_n\lambda_n(y)\lambda_n(x) = 0 \tag{3}$$

式 (2) から、式 (3) を引いたものを考えると、

$$a_1(\lambda_1(y) - \lambda_n(y))\lambda_1(x) + \cdots + a_{n-1}(\lambda_{n-1}(y) - \lambda_n(y))\lambda_{n-1}(x) = 0 \tag{4}$$

帰納法の仮定より、すべての係数が 0 になる。特に、$a_1(\lambda_1(y) - \lambda_n(y)) = 0$。仮定より、$a_1 \neq 0$、$\lambda_1(y) \neq \lambda_n(y)$。これは、矛盾である。 ■

以下、連立一次斉次方程式の定理を利用する。

命題 5.2 次の連立一次方程式は、$n > m$ のとき、すべては、零でない解を持つ。

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

定理 5.3 K を 体とし、G を $\mathrm{Aut}K$ の有限部分群とする。K_0 を G の不変体、

$$K_0 = \{k \in K \mid \sigma(k) = k, \ \ for\ every\ \sigma \in G\}$$

とすると、$[K : K_0] = |G|$。

証明　$G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$、$|G| = n$、$[K : K_0] = m$ とする。

Step 1. $m < n$ とする。$\{x_1, \ldots, x_m\}$ を K_0 上の K の基底とする。次の連立一次方程式を考える。

$$\begin{cases} \sigma_1(x_1)y_1 + \cdots + \sigma_n(x_1)y_n = 0 \\ \sigma_1(x_2)y_1 + \cdots + \sigma_n(x_2)y_n = 0 \\ \cdots\cdots \\ \sigma_1(x_m)y_1 + \cdots + \sigma_n(x_m)y_n = 0 \end{cases}$$

命題 5.2 により、仮定 $m < n$ から、すべては 0 でない $y_1, \ldots, y_n \in K$ で、この方程式の解となっているものがある。$a \in K$ とすると、$\{x_1, \ldots, x_m\}$ は、K_0 上 K の基底だから、$\alpha_1, \ldots, \alpha_m \in K_0$ で、

$$a = \alpha_1 x_1 + \cdots + \alpha_m x_m = \sum_{i=1}^{m} \alpha_i x_i$$

となるものがある。すると、

$$\begin{aligned} & y_1\sigma_1(a) + \cdots + y_n\sigma_n(a) \\ = \;& y_1\sigma_1(\sum_{i=1}^{m} \alpha_i x_i) + \cdots + y_n\sigma_n(\sum_{i=1}^{m} \alpha_i x_i) \\ = \;& y_1 \left(\sum_{i=1}^{m} \sigma_1(\alpha_i)\sigma_1(x_i) \right) + \cdots + y_n \left(\sum_{i=1}^{m} \sigma_n(\alpha_i)\sigma_n(x_i) \right) \\ = \;& y_1 \left(\sum_{i=1}^{m} \alpha_i\sigma_1(x_i) \right) + \cdots + y_n \left(\sum_{i=1}^{m} \alpha_i\sigma_n(x_i) \right) \\ = \;& \sum_{i=1}^{m} \alpha_i(\sigma_1(x_i)y_1 + \cdots + \sigma_n(x_i)y_n) \\ = \;& 0 \end{aligned}$$

a は、K の任意の元だったから、命題 5.1 より、$y_1 = \cdots = y_n = 0$ を得る。これは、$y_1, \ldots, y_n$ の取り方に反する。

Step 2. $m > n$ とする。すると、K_0 上一次独立な K の元 $x_1, \ldots, x_{n+1}$ がとれる。そこで、以下の連立一次方程式を考える。

$$\begin{cases} \sigma_1(x_1)y_1 + \cdots + \sigma_1(x_{n+1})y_{n+1} = 0 \\ \sigma_2(x_1)y_1 + \cdots + \sigma_2(x_{n+1})y_{n+1} = 0 \\ \cdots\cdots \\ \sigma_n(x_1)y_1 + \cdots + \sigma_n(x_{n+1})y_{n+1} = 0 \end{cases}$$

命題 5.2 により、すべては 0 でない $y_1, \ldots, y_{n+1} \in K$ で、この方程式の解となっているものがある。この様な解のうち、0 でないものが最小になるように、$y_1, \ldots, y_{n+1}$ を選び、x_i の順序を入れ替え、$y_1, \ldots, y_r \neq 0$、$y_{r+1} = \cdots = y_{n+1} = 0$ とする。従って、各 $j = 1, \ldots, n$ に対して、

$$\sigma_j(x_1)y_1 + \cdots + \sigma_j(x_r)y_r = 0 \tag{5}$$

この式に、$\sigma \in G$ を作用させる。すると、

$$\sigma\sigma_j(x_1)\sigma(y_1) + \cdots + \sigma\sigma_j(x_r)\sigma(y_r) = 0 \tag{6}$$

が、すべての $j = 1, \ldots, n$ に対して、成立する。

$$\{\sigma_1, \ldots, \sigma_n\} = \{\sigma\sigma_1, \ldots, \sigma\sigma_n\}$$

であることを考えると、すべての $j = 1, \ldots, n$ に対して次の式が成立することが分かる。

$$\sigma_j(x_1)\sigma(y_1) + \cdots + \sigma_j(x_r)\sigma(y_r) = 0 \tag{7}$$

ここで、式 (5) に $\sigma(y_1)$ をかけたものから、式 (6) に、y_1 をかけたものをひくと、

$$\begin{array}{rrcl} & \sigma_j(x_1)y_1\sigma(y_1) + \cdots + \sigma_j(x_r)y_r\sigma(y_1) & = & 0 \\ -) & \sigma_j(x_1)\sigma(y_1)y_1 + \cdots + \sigma_j(x_r)\sigma(y_r)y_1 & = & 0 \\ \hline & \sigma_j(x_2)(y_2\sigma(y_1) - \sigma(y_2)y_1) + \cdots + \sigma_j(x_r)(y_r\sigma(y_1) - \sigma(y_r)y_1) & = & 0 \end{array}$$

$y_1, \ldots, y_r$ は、上の方程式を満たすすべては零でない解のうちで、0 でないものの数が最少のものだったから、

$$y_i\sigma(y_1) - y_1\sigma(y_i) = 0,\ i = 2, \ldots, r$$

が成り立つ。この式は、$y_i y_1^{-1} = \sigma(y_i y_1^{-1})$ を意味し、$\sigma \in G$ は、任意だったから $y_i y_1^{-1} \in K_0$ を得る。従って、$y_i = z_i y_1$ を満たす $z_i \in K_0$ が各 $i = 2, \ldots, r$ について存在する。式 (5) で、$j = 1$ とすると、$\sigma_1 = 1$ だったことに注意して、

$$\begin{aligned} 0 &= x_1y_1 + x_2y_2 + \cdots + x_ry_r \\ &= x_1y_1 + x_2z_2y_1 + \cdots + x_rz_ry_1 \\ &= (x_1 + x_2z_2 + \cdots + x_rz_r)y_1 \end{aligned}$$

$y_1 \neq 0$ だから、$x_1 + x_2z_2 + \cdots + x_rz_r = 0$ を得る。しかし、$z_i \in K_0$、$i = 2, \ldots, r$ だったから、これは、$x_1, \ldots, x_r$ が K_0 上一次独立とした仮定に矛盾する。

Step 1、Step 2 より、$|G| = n = m = [K : K_0]$ を得る。 ■

系 5.4 $L : K$ を体の有限次拡大とする。$H \leq G = \Gamma(L : K)$ とすると、次の等式が成り立つ。

$$[L : K] = |H| \cdot [H^+ : K].$$

証明　定理 5.3 を適用すると、$[L : H^+] = |H|$ だから、

$$[L : K] = [L : H^+][H^+ : K] = |H| \cdot [H^+ : K]$$

を得る。 ■

定理 5.5 $L:K$ を体の有限正規拡大とし、M を その中間体とする。$\tau : M \to L$ が、K-単射準同型ならば、L の K-自己同型 $\sigma : L \to L$ で、$\sigma_{|M} = \tau$ となっているものが存在する。特に、$p(t) \in K[t]$ を既約な多項式とし、α, β をその根とすると、L の K-自己同型で、$\sigma(\alpha) = \beta$ となっているものが存在する。

証明　定理 4.1 より、L を K 上 $f(t) \in K[t]$ の分解体として良い。すると、L は、M 上 f の分解体と見ることが出来るが、$\tau(M)$ 上 f の分解体と見ることも出来る。従って、定理 3.3 を適用することによって、前半が得られる。後半は、定理 1.3 によって、まず、$K(\alpha)$ から、$K(\beta)$ の同型写像で、α を β に移すものを作れば、後は、前半部分の適用により、結果を得る。 ■

6　ガロアの定理

$L:K$ を体の有限次拡大、$G = \Gamma(L:K)$ とする。$\mathcal{F}$ で、中間体全体を表し、$\mathcal{G}$ で、G の部分群全体を表すとする。

$M \in \mathcal{F}$、$H \in \mathcal{G}$ とする。

$$\begin{aligned} *: M \to M^* &= \{\sigma \in G \mid \sigma(m) = m, \ \text{for all } m \in M\} = \Gamma(L:M) \\ +: H \to H^+ &= \{a \in L \mid \sigma(a) = a, \ \text{for all } \sigma \in H\} \end{aligned}$$

定理 6.1（ガロアの基本定理）$L:K$ を有限分離正規拡大、$[L:K] = n$、$G = \Gamma(L:K)$、$M \in \mathcal{F}$ とする。このとき、次が成立する。

(1) $|G| = n$。

(2) $*$ と、$+$ は、互いに逆写像で、包含関係を逆転させ、$\mathcal{F}$ と、$\mathcal{G}$ の間の一対一対応を与える。

(3) $[L:M] = |M^*|$、$[M:K] = |G|/|M^*|$。

(4) $M:K$ が正規拡大 $\Leftrightarrow M^* \lhd G$。

(5) $M:K$ が正規拡大 $\Rightarrow \Gamma(M:K) \simeq G/M^*$。

有限正規分離拡大のことを有限次ガロア拡大ともいう。この節の目標は、上の定理を証明することである。

定義 6.1 $L:K$ を代数拡大、N が、$L:K$ の正規閉包であるとは、N が、L の拡大体で、次の条件を満たすものである時を言う。

1. $N:K$ は、正規拡大。
2. $L \subset M \subset N$ で、$M:K$ が正規ならば、$N = M$。

すなわち、正規閉包は、L を含む K の正規拡大の中で、最小のもの。

定理 6.2 $L:K$ が有限拡大ならば、$L:K$ の正規閉包 N で、$N:K$ が有限拡大となるものがある。$M:K$ も、正規閉包ならば、$N:K$ と同型である。

証明　（存在）$L=K(\alpha_1,\ldots,\alpha_r)$、$m_i$ を α_i の K 上の最小多項式とする。$f=m_1\cdots m_r$ とする。N を f の K 上の分解体とすれば、α_i は、m_i の根だから、$L=K(\alpha_1,\ldots,\alpha_r)\subset N$ かつ、(1)、(2) を満たすのは、明らか。

（一意性）上の f について、M も、f の K 上の分解体となる。よって、定理 3.3 より、同型。 ■

補題 6.3 $K\subset L\subset N\subset M$ を、体の拡大で、$[L:K]<\infty$、かつ N は、$L:K$ の正規閉包とする。$\tau:L\to M$ を K-単射準同型とすると、$\tau(L)\subset N$ である。

証明　$\alpha\in L$ とし、m を α の K 上の最小多項式とする。このとき、τ が、K の元を動かさないことより、

$$0=m(\alpha)=\tau(m(\alpha))=m(\tau(\alpha)).$$

従って、$\tau(\alpha)$ は、m の根である。N は、K 上正規であるから、m は、N で分解する。従って、$\tau(\alpha)\in N$。α は、任意だったから、$\tau(L)\subset N$。 ■

定理 6.4 $L:K$ を有限拡大とすると、次は同値。

(1) $L:K$ は、正規拡大。

(2) L を含む K の正規拡大 M で次を満たすものがある。

$$\Gamma(L:K)=\{\sigma:L\to M\mid \sigma \text{ は、} K\text{-単射準同型}\}$$

(3) L を含む K の任意の正規拡大 M は、次を満たす。

$$\Gamma(L:K)=\{\sigma:L\to M\mid \sigma \text{ は、} K\text{-単射準同型}\}$$

証明　(1) $\Rightarrow$ (3)　補題 6.3 を $L=N$ として、適用する。$\sigma:L\to M$ を K-単射準同型とすると、$\sigma(L)\subset L$ で、σ は、K-線形だったから、$[L:K]=[\sigma(L):K]$、従って、$L=\sigma(L)$ すなわち、$\sigma\in\Gamma(L:K)$ を得る。

(3) $\Rightarrow$ (2)　M を、拡大 $L:K$ の正規閉包とすれば、明らか。

(2) $\Rightarrow$ (1)　f を $\alpha\in L$ を根にもつ、K-上の既約多項式とする。すると、f は、M で分解する。$f(\beta)=0$ とすると、定理 5.5 によって、$\sigma\in\Gamma(M:K)$ で、$\sigma(\alpha)=\beta$ となるものが存在する。仮定より $\beta=\sigma(\alpha)\in\sigma(L)=\sigma_{|L}(L)=L$ だから、f は、L で分解していることになり、$L:K$ は、正規拡大である。 ■

定理 6.5 $K\subset L\subset M$ を体の拡大の列とし、$M:K$ は、有限正規拡大とする。$[L:K]=n$ ならば、L から、M の中への K-単射準同型の数は、n 以下であり、それが、丁度 n となるのは、$L:K$ が分離拡大の時、しかもその時に限る。

証明　$[L:K]$ に関する帰納法で証明する。$[L:K]=1$ の時は、$L=K$ だから、明らか。

$[L:K]=n>1$ とし、$\alpha\in L\setminus K$、m を、α の最小多項式とする。($L:K$ が非分離の時は、α として、非分離な元を取っておく。) $\alpha=\alpha_1,\dots,\alpha_s$ を m の相異なる根とする。従って、仮定より、$L:K$ が、分離的 ということと、$s=[K(\alpha):K]$ が、同値という状況が成り立っている。定理 5.5 によって、$\sigma_1,\dots,\sigma_s\in\Gamma(M:K)$ で、$\sigma_i(\alpha)=\alpha_i$ となるものが存在する。一方

$$r=[L:K(\alpha)]=n/[K(\alpha):K]<n$$

だから、帰納法の仮定により、

$$t=|\{K(\alpha)\text{-単射準同型 } L\to M\}|\le r$$

で、等号が成立するのは、$L:K(\alpha)$ が分離拡大の時、またその時に限る。ここで、$\rho_1,\dots,\rho_t$ を 相異なる $L\to M$ なる $K(\alpha)$-単射準同型とし、$\phi_{ij}=\sigma_i\rho_j$ とする。ϕ_{ij} は、$L\to M$ の K-単射準同型である。まず、$\phi_{ij}=\phi_{i'j'}$ とすると、

$$\alpha_i=\sigma_i(\alpha)=\sigma_i\rho_j(\alpha)=\phi_{ij}(\alpha)=\phi_{i'j'}(\alpha)=\sigma_{i'}\rho_{j'}(\alpha)=\sigma_{i'}(\alpha)=\alpha_{i'}$$

だから、$i=i'$。各 σ_i は同型だから、$\sigma_i\rho_j=\sigma_i\rho_{j'}$ ならば、$\rho_j=\rho_{j'}$ を得る。さらに、ϕ を $L\to M$ なる、K-単射準同型とすると、$\phi(\alpha)$ も、m の根だから、$\phi(\alpha)=\alpha_i$ となる i が存在する。すると、$\sigma_i^{-1}\phi$ は、$L\to M$ なる、K-単射準同型で、$\sigma_i^{-1}\phi(\alpha)=\alpha$ だから、$K(\alpha)$-準同型。従って、$\sigma_i^{-1}\phi=\rho_j$ となる、j が存在する。これによって、

$$st=|\{K\text{-単射準同型 } L\to M\}|\le[L:K(\alpha)][K(\alpha):K]=n$$

で、等号成立は、$s=r$ のときに限る。従って、主張を得る。 ■

定理 6.6 $L:K$ を有限拡大とする。このとき、$L:K$ が正規かつ分離拡大ということと、K が、$\Gamma(L:K)$ の不変体であることとは、同値である。

証明　$L:K$ が正規かつ分離拡大であるとする。定理 5.5、6.5 によって、$|\Gamma(L:K)|=[L:K]$。しかし、不変体 K_0 は、K を含み、かつ、定理 5.3 によって、$[L:K_0]=|\Gamma(L:K)|$ だったから、$K=K_0$ を得る。

逆に、M を $L:K$ の正規閉包とすると、

$$[L:K]=|\Gamma(L:K)|\le|\{K\text{-単射準同型 } L\to M\}|$$

で、等号が成立するのは、定理 6.5 によって、分離的の時で、かつ、定理 6.4 より、それは、正規の時である。 ■

定理 6.1 の証明 (1) 定理 6.6 により、$G^+=K$。定理 5.3 により、$|G|=[L:G^+]=[L:K]=n$。

(2)(3) $H\le(H^+)^*$。しかし、$|(H^+)^*|=|\Gamma(L:H^+)|=|H|$。よって、$H=(H^+)^*$ また、$M\subset(M^*)^+$。$[L:M]=[L:(M^*)^+]=|M^*|$

(4)(5) Excercise。

これより、定理 6.1 の証明を得る。 ■

7　べき根による解の存在

定義 7.1 体の拡大 $L:K$ がべき根による拡大であるとは、$L=K(\alpha_1,\ldots,\alpha_m)$ であり、各 $i=1,2,\ldots,m$ について、$\alpha_i^{n(i)}\in K(\alpha_1,\ldots,\alpha_{i-1})$ となる自然数 $n(i)$ があることである。

補題 7.1 $L:K$ を有限拡大とする。M を $L:K$ の正規閉包とする。すると、K を含む M の部分体 $L_1,\ldots,L_s$ で、$M=L_1\cdots L_s$、$L_i:K\simeq L:K$ となっているものが存在する。

証明　命題 2.3 により、$L=K(\alpha_1,\ldots,\alpha_r)$、$\alpha_i$ は、K 上代数的と書ける。m_i を α_i の K 上の最小多項式とし、$f=m_1\cdots m_s$ とする。M は、K 上 f の分解体 β_{ij} を m_i の根とする。定理 5.5 より、$\sigma_{ij}(\alpha_i)=\beta_{ij}$、$L_{ij}=\sigma_{ij}(L)\ni\beta_{ij}$。すると、拡大 $L_{ij}:K$ と、$L:K$ かつ、

$$M\supset\prod_{i,j}L_{ij}\supset K(\beta_{ij},i,j)=M$$

これより、求める分解が得られた。 ■

補題 7.2 $L:K$ べき根による拡大。M を $L:K$ の正規閉包とする。このとき、$M:K$ もべき根による拡大である。

証明　$L:K$ が有限であることは、べき根による拡大の定義より明らか。補題 7.1 により、$M=L_1\cdots L_s$、$L_i:K\simeq L:K$、$L_i:K$ は、べき根による拡大となるものがある。ここで、$R_i=L_1\cdots L_i$ とする。$R_i:K$ をべき根による拡大とする。$R_i=K(\alpha_1,\ldots,\alpha_m)$ をべき根列、また、$L_{i+1}=K(\beta_1,\ldots,\beta_n)$ とし、$\beta_1,\ldots,\beta_n$ をべき根列とする。このとき、べき根列の定義より、$\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n$ は、べき根列である。従って、$R_{i+1}:K$ は、べき根による拡大となり、帰納法により、$M:K$ もべき根による拡大となる。 ■

補題 7.3 K を標数 0 の体、L を t^p-1 の K 上の分解体、p を素数とする。このとき、$\Gamma(L:K)$ は、アーベル群である。

証明　まず、t^p-1 の微分は、pt^{p-1} だから、t^p-1 は、重根を持たない。$\alpha,\beta\in L$ を根とすると、$\alpha^p=\beta^p=1$。従って、$(\alpha\beta)^p=1$、$(\alpha^{-1})^p=(\alpha^p)^{-1}$ が成り立つから、根全体は、位数 p の群を成す。p は、素数だから、巡回群となる。ϵ をその生成元とする。$L=K(1,\epsilon,\ldots,\epsilon^{p-1})=K(\epsilon)$ だから、$\Gamma(L:K)$ の元は、ϵ への作用で決まる。$\sigma,\tau\in\Gamma(L:K)$ とすると、$\sigma(\epsilon)$、$\tau(\epsilon)$ は、共に、t^p-1 の根だから、$\sigma(\epsilon)=\epsilon^i$、$\tau(\epsilon)=\epsilon^j$ と書ける。従って、

$$\sigma\tau(\epsilon)=\sigma(\epsilon^j)=\sigma(\epsilon)^j=\epsilon^{ij}=\tau(\epsilon)^i=\tau(\epsilon^i)=\tau\sigma(\epsilon)$$

だから、$\sigma\tau=\tau\sigma$ を得るから、$\Gamma(L:K)$ は、アーベル群である。 ■

補題 7.4 K を標数 0 の体で、t^n-1 は、K で、分解しているとする。$a\in K$ とし、L を t^n-a の K 上の分解体とすると、$\Gamma(L:K)$ は、アーベル群である。

証明　t^n-1 は、重根を持たない。$\epsilon_1,\ldots,\epsilon_n$ をその根とする。t^n-a の一つの根を α とする。すると、$\alpha\epsilon_1,\ldots,\alpha\epsilon_n$ がその根である。かつ、$L=K(\alpha\epsilon_1,\ldots,\alpha\epsilon_n)=K(\alpha)$。$\sigma,\tau\in\Gamma(L:K)$ とすると、$\sigma(\alpha)=\alpha\epsilon_i$、$\tau(\alpha)=\alpha\epsilon_j$ となる、i,j が存在する。従って、以下が成り立つ。

$$\sigma\tau(\alpha)=\sigma(\alpha\epsilon_j)=\sigma(\alpha)\sigma(\epsilon_j)=\alpha\epsilon_i\epsilon_j=\tau(\alpha)\tau(\epsilon_i)=\tau(\alpha\epsilon_i)=\tau\sigma(\alpha)$$

これより、$\sigma\tau=\tau\sigma$、従って、$\Gamma(L:K)$ は、アーベル群である。 ■

定義 7.2 群 G が可解 (solvable) であるとは、G の部分群の列 $G_1,\ldots,G_{n-1}$ で、以下の条件を満たすものが存在することである。

$$1=G_0\lhd G_1\lhd\cdots\lhd G_{n-1}\lhd G_n=G,\ G_{i+1}/G_i \text{ は、アーベル群},\ i=0,1,\ldots,n-1.$$

定理 7.5 G を群。$H\leq G$、$N\lhd G$ とする。このとき以下が成り立つ。

(1) G が可解ならば、H も可解。

(2) G が可解であることと、N と、G/N が共に可解であることとは、同値である。

注

1. アーベル群は、可解。
2. A_5 の正規部分群は、1 と A_5 のみで、かつ、A_5 は、アーベル群ではない。よって、A_5 は、可解ではない。定理 7.5 により、A_5 と同型な部分群を含む群 A_n、S_n $n\geq 5$ は、可解群ではない。

定義 7.3 $f\in K[t]$、Σ を K 上 f の分解体とする。$\Gamma(\Sigma:K)$ を f の K 上のガロア群という。

注　定義 7.3 の記号のもとで、X を根全体とすると、$\phi:\Gamma(\Sigma:K)\to S^X$ を自然な写像とすると、これは、単射である。

定義 7.4 K を標数 0 の体、$f\in K[t]$、Σ を K 上 f の分解体とする。このとき、f がべき根で解けるとは、Σ の拡大体 M で、$M:K$ がべき根による拡大となるものがある時を言う。

8　ガロア群の可解性

本節の目標は、次の定理を証明することである。

定理 8.1 K を標数 0 の体とする。$f \in K[t]$、Σ を K 上 f の分解体とする。このとき次は、同値である。

(i) f は、べき根で解ける。

(ii) f の K 上のガロア群は、可解。

定理 8.2 K を標数 0 の体とし、$K \subset L \subset M$ とする。$M : K$ がべき根による拡大ならば、$\Gamma(L : K)$ は、可解群である。

証明　*Step 1.*　$\Gamma(L : K)$ の不変体は、K としてよい。特に、$L : K$ を正規拡大としてよい。

(証) K_0 を不変体とする。明らかに、$\Gamma(L : K) = \Gamma(L : K_0)$ から、$K \subset K_0 \subset L \subset M$ で $M : K_0$ は、べき根による拡大だったから、$M : K_0$ をべき根による拡大として、$\Gamma(L : K)$ が可解であることを示せばよい。すなわち、$K = K_0$ として良い。このときは、定理 6.6 により、$L : K$ は、正規拡大である。

Step 2.　$L : M$ としてよい。

(証) N を $M : K$ の正規閉包とする。補題 7.2 より、$N : K$ はべき根による拡大。定理 6.1 より、$\Gamma(L : K) \simeq \Gamma(M : K)/L^*$. ここで、定理 7.5 より、$\Gamma(M : K)$ が可解ならば、$\Gamma(L : K)$ も可解となるから、$L = M$ の場合に示せばよい。(K が、$\Gamma(M : K)$ の不変体であることも注意。)

Step 3.　$L = K(\alpha_1, \ldots, \alpha_n)$、$\alpha_i^{n(i)} \in K(\alpha_1, \ldots, \alpha_{i-1})$、$n(i)$ は素数、とできる。

Step 4.　n に関する帰納法。$n(1) = p$ とする。M_0 を $t^p - 1$ の L 上の分解体、$M_0 = L(\epsilon)$、$\epsilon^p = 1 \neq \epsilon$、$M_1 = K(\epsilon)$。$L$ を K 上 f の分解体とすると、M_0 は、K 上 $f \cdot (t^p - 1)$ の分解体だから K 上正規で、定理 6.1 により、

$$\Gamma(L : K) \simeq \Gamma(M_0 : K)/L^*.$$

よって $\Gamma(M_0 : K)$ が可解であることを示せば 定理 7.5 (2) より、$\Gamma(L : K)$ も可解であることが得られる。

$M_1 = K(\epsilon)$ だから、補題 7.3 より、$\Gamma(M_1 : K)$ は、アーベル群である。従って、再び、定理 6.1 と、定理 7.5 (2) を適用することにより、

$$\Gamma(M_0 : K) \rhd \Gamma(M_0 : M_1),\ \Gamma(M_0 : K)/\Gamma(M_0 : M_1) \simeq \Gamma(M_1 : K)$$

より、$\Gamma(M_0 : M_1)$ が可解であることを示せば良い。

$M_0 = M_1(\alpha_1, \ldots, \alpha_n)$、$H = M_1(\alpha_1)^*$ とする。$t^p - 1$ は、M_1 で分解しているから、$M_1(\alpha_1)$ は、$t^p - \alpha_1^p$ の M_1 上の分解体。よって、$M_1(\alpha) : M_1$ は、正規拡大。$\Gamma(M_1(\alpha_1) : M_1)$ は、アーベル群だから、

$$\Gamma(M_1(\alpha_1) : M_1) \simeq \Gamma(M_0 : M_1)/\Gamma(M_0 : M_1(\alpha_1))$$

もアーベル群。帰納法の仮定から $\Gamma(M_0 : M_1(\alpha_1))$ は、可解だから $\Gamma(M_0 : M_1)$ は、可解である。 ■

定義 8.1 $L : K$ を有限ガロア拡大。$G = \Gamma(L : K)$ とする。$a \in L$ に対して、

$$N_{L/K}(a) = N(a) = \prod_{\tau \in G} \tau(a)$$

を a のノルムという。$\sigma \in G$ だから、

$$\sigma(N(a)) = \prod_{\tau \in G} \sigma\tau(a) = \prod_{\tau' \in G} \tau'(a) = N(a)$$

これは、$N(a) \in K$ を意味する。

定理 8.3 $L : K$ を有限ガロア拡大、$\Gamma(L : K) =< \tau >= G$ 巡回群、$a \in L$ とする。このとき、$N(a) = 1$ となることと、L のある元 $b \neq 0$ について、$a = b/\tau(b)$ となることとは同値。

証明 $a = b/\tau(b)$、$b \neq 0$ とする。$|G| = n$ とすると、$\tau^n = 1$ だから、

$$N(a) = a\tau(a) \cdots \tau^{n-1}(a) = \frac{b}{\tau(b)} \frac{\tau(b)}{\tau^2(b)} \cdots \frac{\tau^{n-1}(b)}{\tau^n(b)} = 1$$

逆に $N(a) = 1$ とする。$a \neq 0$ かつ、$1 = \tau^0, \tau^1, \ldots, \tau^{n-1}$ は、命題 5.1 によって、L 上一次独立だから次の式を満たす $c \in L$ がある。

$$a\tau^0(c) + a\tau(a)\tau^1(c) + \cdots + (a\tau(a) \cdots \tau^{n-1}(a))\tau^{n-1}(c) \neq 0$$

この左辺を b と置くと、

$$\begin{aligned} \tau(b) &= \tau(a)\tau(c) + \tau(a)\tau^2(a)\tau^2(c) + \cdots + (\tau(a)\tau^2(a) \cdots \tau^{n-1}(a)a)c \\ &= \frac{1}{a}(a\tau(a)\tau(c) + a\tau(a)\tau^2(a)\tau^2(c) + \cdots + (a\tau(a) \cdots \tau^{n-1}(a))\tau^{n-1}(c) + ac) \\ &= \frac{b}{a} \end{aligned}$$

■

定理 8.4 $L : K$ を有限ガロア拡大、$\Gamma(L : K) = G < \tau >\simeq \boldsymbol{Z}/p\boldsymbol{Z}$、$p$ を素数とする。K の標数は、0 または、p と素とする。$t^p - 1$ が K 上で、分解しているとする。すると、L の元 α と、K の元 a で、$L = K(\alpha)$ となるものが存在する。ここで、α は、$t^p - a$ の根である。

証明 $\epsilon^p = 1 \neq \epsilon$ とする。$\tau^i(\epsilon) = \epsilon$ より、$N(\epsilon) = \epsilon \cdots \epsilon = 1$. 従って、定理 8.3 によって、$L$ の元 α で、$\epsilon = \alpha/\tau(\alpha)$ となるものが存在する。よって、$\alpha^p = \tau(\alpha^p)$。従って、$a = \alpha^p \in K$ となる。$\tau(\alpha) = \epsilon^{-1}\alpha, \epsilon^{-2}\alpha, \ldots$ は、すべて異なる。従って、$K(\alpha)$ は、$t^p - a$ の K 上の分解体で、$\Gamma(K(\alpha) : K)| \geq p$ より、$K(\alpha) = L$。 ■

定理 8.5 K を標数 0 の体。$\Gamma(L:K)=G$ を可解、$L:K$ を正規拡大とする。このとき、L の拡大 R で、$R:K$ がべき根による拡大となるものが存在する。

証明　G に関する帰納法で示す。$|G|=1$ の時は明らか。H を極大な真の正規部分群とする。G/H は素数 p を位数とする巡回群となる。N を t^p-1 の L 上の分解体とすると、$N:K$ は正規かつ、$\Gamma(N:K)$ 可解となる。M を K 及び t^p-1 の根により生成された N の部分体、 $K(\epsilon)$ とする。$\phi:\Gamma(N:M)\to\Gamma(L:K)$ は、$N=L(\epsilon)$ だから単射。$|\Gamma(N:M)|<|\Gamma(L:K)|$ なら、帰納法の仮定により、この場合は成立する。$K\subset K(\epsilon)=M\subset N\subset R$。同型とすると、$\Gamma(N:M)$ の指数 p の正規部分群を H_1 とすると、$[H_1^+:M]=p$。よって、これは、べき根による拡大。

$$K\subset K(\epsilon)=M\subset H_1^+\subset N$$

従って、この場合も帰納法の仮定により定理が成り立つ。 ■