体論から Galois 理論へ

2025 年 11 月 5 日

目次

1 K 代数

1.1 K 代数

Def 1.1

k を可換環とする．

(1) 環 A と $s_A : k \to A$ を環準同型の組 (A, s_A) を k **代数** (k**-algebra**)[†1] という．このとき，s_A を (A, s_A) の**構造射** (**structural morphism**)[†2] という．

(2) $(A, s_A), (B, s_B)$ を k 代数とする．環準同型 $\varphi : A \to B$ が $\varphi \circ s_A = s_B$ を充たすとき，φ を k **準同型** (k**-homomorphism**) という．(A, s_A) から (B, s_B) への k 準同型の全体を $\mathrm{Hom}_k^{\mathrm{al}}(A, B)$ で表す．

$$\begin{tikzcd} A \arrow[rr, "\varphi"] & \arrow[d, phantom, "\circlearrowleft"] & B \\ & k \arrow[ul, "s_A"] \arrow[ur, "s_B"'] & \end{tikzcd}$$

(3) k 準同型が同型であれば k **同型** (k**-isomorphism**) という．k 代数 A の k 自己同型の全体は合成に関して群となる．これを A の k **自己同型群** (k**-automorphism group**) といい，$\mathrm{Aut}_k^{\mathrm{al}} A$ で表す．

(4) k 準同型 $\varphi : A \to B$ が単射であれば A を $\varphi(A)$ を同一視して，$A \subset B$ と考えられる．このとき A を B の**部分 k 代数** (**sub-k-algebra**) という．

Example 1.1. $\varphi : \mathbb{Z} \to \mathbb{Z}/(n), m \to m + (n)$ によって $\mathbb{Z}/(n)$ は $\mathbb{Z}$ 代数と見做せる．

Prop 1.1

(A, s_A) を k 代数とする．作用 $k \times A \to A$ を

$$a \cdot x := s_A(a)x \ (a \in k, x \in A)$$

で定めると，A は k 加群と見做せる．

Proof. 簡単に check できる． ■

[†1] 構造射 s_A を省略して k 代数 A とかくことが多い．

[†2] 構造射には単射性を課す場合もある．単射の時は $k \subset A$ と見做せる．

Prop 1.2

$(A, s_A), (B, s_B)$ を k 代数とする．$\varphi : A \to B$ を環準同型とする．このとき，

$$\varphi \text{ が } k \text{ 準同型} \Leftrightarrow \ k \text{ 加群の準同型（} k \text{ 線型写像）}$$

Proof. $(\Rightarrow)$ 準同型なので和を保つことは明らか．$a \in k, x \in A$ に対し，

$$\varphi(a \cdot x) = \varphi(s_A(a)x) = \varphi(s_A(a))\varphi(x) \overset{\downarrow}{=} s_B(a)\varphi(x) = a \cdot \varphi(x)$$

$(\Leftarrow)$ $a \in k$ に対し，

$$\varphi \circ s_A(a) = \varphi(s_A(a)1) = \varphi(a \cdot 1) \overset{\downarrow}{=} a \cdot \varphi(1) = a \cdot 1 = s_B(a)$$

それぞれ $\downarrow$ の位置で条件を使用した． ■

1.2　体準同型

Def 1.2

K を零環でない環とする．$K^\times = \{0\}$ のとき，K を**斜体** (**skew field**) または**可除環** (**division ring**) という．特に K が可換環なら**体** (**field**) という．体の間の環準同型を**体準同型** (**field homomorphism**) という．

Example 1.2. 体でない斜体の例としては **Hamilton の四元数** (**Hamiltonian quaternion**) の全体 $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ が知られる．

Prop 1.3

可換環 A に対し次は同値．

(1) A は体である．
(2) A のイデアルは全て trivial.

Proof. (1) $\Rightarrow$ (2) $I \subset A$ をイデアルとする．$x \in I \setminus \{0\}$ が取れるなら，$\exists y \in A, xy = 1 \in A$ より $I = A$. よって A のイデアルは $\{0\}$ または A のみ.
(2) $\Rightarrow$ (1) $x \in A \setminus \{0\}$ に対し，$(x) = A$ である．よって $1 \in (x)$ であるから，$\exists y \in A, xy = 1$. 従って A は体. ■

Cor 1.1

体準同型は埋込，つまり単射である．

Proof. $\varphi : K_1 \to K_2$ を体準同型とする．このとき $\operatorname{Ker}\varphi$ は K_1 のイデアルであるが，体のイデアルは trivial である．$\varphi(1) = 1$ より，$\operatorname{Ker}\varphi \neq A$. よって $\operatorname{Ker}\varphi = \{0\}$ で φ は単射. ■

Def 1.3 (1) 体 L の部分環 K が体であるとき，K は L の**部分体** (**subfield**)，L は K の**拡大体** (**extension field**) といい，この関係を L/K で表し体拡大という．

(2) $L/M, M/K$ が体拡大であるとき，M は L/K の**中間体** (**intermediate field**) といい，$L/M/K$ で表す．

Remark 1.1. L/K が体拡大のとき L は包含写像 $K \hookrightarrow L$ を構造射として K 代数と見做せる．よって **Prop 1.1** により，L は K 線型空間と見做せる．

以降は言及せずとも，この構造射により K 代数，K 線型空間と見做すことにする．

Remark 1.2. L_1, L_2 が体 K の拡大体であるとき，K 代数と見做せる．このとき，体準同型 $\varphi : L_1 \to L_2$ が K 準同型であるとは，$\varphi|_K = \mathrm{id}_K$ ということであるが，**Prop 1.2** によりこれは K 線型空間 L_1, L_2 間の K 線型写像であることと同値である．

$$\begin{tikzcd}
L_1 \arrow[rr, "\varphi"] & & L_2 \\
& K \arrow[ul, "\iota_1"] \arrow[ur, "\iota_2"'] \arrow[u, phantom, "\circlearrowright"] &
\end{tikzcd}$$

つまり，K 準同型は体準同型かつ K 線型な写像である．

よって L_1 から L_2 の K 準同型の全体は，

$$\begin{aligned}
\mathrm{Hom}_K^{\mathrm{al}}(L_1, L_2) &= \{\varphi \in \mathrm{Hom}^{\mathrm{al}}(L_1, L_2) : \varphi|_K = \mathrm{id}_K\} \\
&= \mathrm{Hom}^{\mathrm{al}}(L_1, L_2) \cap \mathrm{Hom}_K(L_1, L_2)
\end{aligned}$$

L/K を体拡大とするとき，L 上の K 自己同型群は，

$$\begin{aligned}
\mathrm{Aut}_K^{\mathrm{al}} L &= \{\varphi \in \mathrm{Aut}^{\mathrm{al}}(L) : \varphi|_K = \mathrm{id}_K\} \\
&= \mathrm{Aut}^{\mathrm{al}}(L) \cap \mathrm{Aut}_K(L)
\end{aligned}$$

但し，
$$\left|\begin{array}{l}
\mathrm{Hom}^{\mathrm{al}}(L_1, L_2) \text{ は } L_1 \text{ から } L_2 \text{ への体準同型全体} \\
\mathrm{Hom}_K(L_1, L_2) \text{ は } L_1 \text{ から } L_2 \text{ への } K \text{ 線型写像全体} \\
\mathrm{Aut}^{\mathrm{al}}(L) \text{ は体としての } L \text{ 上自己同型群} \\
\mathrm{Aut}_K(L) \text{ は } K \text{ 線型空間としての } L \text{ 上自己同型群}
\end{array}\right.$$
とした．[†3]

Example 1.3. 複素共軛 $\rho : \mathbb{C} \to \mathbb{C}, z \mapsto \overline{z}$ は $\mathbb{C}$ 上の $\mathbb{R}$ 自己同型．

Example 1.4. $\varphi : \mathbb{C} \to \mathbb{C}, a + b\sqrt{-1} \mapsto a + 2b\sqrt{-1}$ $(a, b \in \mathbb{R})$ とすると，

$$\varphi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C}) \text{ and } \varphi \notin \mathrm{Hom}^{\mathrm{al}}(\mathbb{C}, \mathbb{C})$$

なので，$\varphi \notin \mathrm{Hom}_{\mathbb{R}}^{\mathrm{al}}(\mathbb{C}, \mathbb{C})$

[†3] 群としての L 上自己同型群を $\mathrm{Aut}(L)$, 集合としての L 自己同型群（L 上の対称群）を $\mathfrak{S}(L)$ と表すことにする．

2 体拡大

2.1 標数と素体

$\mathbb{P} \subset \mathbb{Z}$ を素数の全体とする．

Prop 2.1

K を体とする．環準同型 $\varphi : \mathbb{Z} \to K, n \mapsto n \cdot 1$ [†4]に対し，イデアル $\operatorname{Ker}\varphi$ は $\operatorname{Ker}\varphi = (p)$ $(p \in \mathbb{P} \cup \{0\})$ とかける．

Proof. $\operatorname{Im}\varphi$ は K の部分環なので整域であり，また $\mathbb{Z}/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$ である．よって $\operatorname{Ker}\varphi$ は素イデアルであるから，$\operatorname{Ker}\varphi = (0)$ また $\exists p \in \mathbb{P}, \operatorname{Ker}\varphi = (p)$. ■

$$
\begin{tikzcd}
\mathbb{Z} \arrow[r, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & \operatorname{Im}\varphi \subset K \\
\mathbb{Z}/\operatorname{Ker}\varphi \arrow[ur, dashed, "\simeq"'] &
\end{tikzcd}
$$

Def 2.1

Prop 2.1 の $p \in \mathbb{P} \cup \{0\}$ を体 K の**標数** (**characteristic**) といい，$\operatorname{ch} K$ とかく．

Example 2.1. (1) $\varphi : \mathbb{Z} \to \mathbb{Q}$ は単射なので，$\operatorname{ch}\mathbb{Q} = 0$.

(2) $\mathbb{F}_p := \mathbb{Z}/(p)$ $(p \in \mathbb{P})$ とすると，$\operatorname{ch}\mathbb{F}_p = p$.

Def 2.2

真の部分体を持たない体を**素体** (**prime field**) という．

Remark 2.1. 素体は $\mathbb{Q}$ または $\mathbb{F}_p$ しかない．

Prop 2.2

任意の体は 1 つの素体を包む．特に標数 0 の体は $\mathbb{Q}$ を，正標数 p の体は $\mathbb{F}_p$ を包む．

Proof. $\operatorname{ch} K = 0$ のとき **Prop 2.1** から $\mathbb{Z} \subset K$ である．$\mathbb{Z} \setminus \{0\} \subset K^\times$ なので $\mathbb{Q} \subset K$ である．また $\operatorname{ch} K = p > 0$ のとき **Prop 2.1** から $\mathbb{Z}/(p) \subset K$ であるがこれは体である． ■

[†4] $n \cdot 1 := \underbrace{1 + \cdots + 1}_{n}$

Remark 2.2. 体 L_1, L_2 が共通の素体 K を包むとき，$\mathrm{Hom}_K^{\mathrm{al}}(L_1, L_2) = \mathrm{Hom}^{\mathrm{al}}(L_1, L_2)$.

Prop 2.3

$\mathrm{ch}\, K = p > 0, n \in \mathbb{Z}_{>0}, q = p^n$ のとき，

$$\mathrm{Frob}_q : K \to K, x \mapsto x^q$$

は体準同型．これを **Frobenius 準同型** (**Frobenius homomorphism**) という．

Proof. (1) $x, y \in K$ に対し, $\mathrm{Frob}_q(x+y) = \mathrm{Frob}_q(x) + \mathrm{Frob}_q(y)$ を示す. $(x+y)^q = x^q + y^q$ を n に関する帰納法により示す．まず $n = 1$ のとき，

$$(x+y)^p = x^p + y^p + \sum_{j=1}^{n-1} \binom{p}{j} x^j y^{p-j}$$

ここで,

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} = \frac{p(p-1)\cdots(p-j+1)}{j!}$$

$0 < j < p$ のとき，$j!$ は p で割れないので $p \mid \binom{p}{j}$．よって，$(x+y)^p = x^p + y^p$.

$n(\geq 1)$ 未満での成立を仮定するとき，

$$(x+y)^q = (x+y)^{p \cdot p^{n-1}} = (x^p + y^p)^{p^{n-1}} = x^{p \cdot p^{n-1}} + y^{p \cdot p^{n-1}} = x^q + y^q$$

(2) $x, y \in K$ に対し，$\mathrm{Frob}_q(xy) = (xy)^q = x^q y^q = \mathrm{Frob}_q(x)\,\mathrm{Frob}_q(y)$.

(3) $\mathrm{Frob}_q(1) = 1$ は明白.

■

Cor 2.1

$f(T) \in \mathbb{F}_p[T]$ に対し，$f(T^p) = f(T)^p$.

Proof. $f(T) = a_0 + a_1 T + \cdots + a_n T^n \in \mathbb{F}_p[T]$ とする．Fermat の小定理から $\forall j$，$a_j^p = a_j$ なので，**Prop 2.3** を用いて，

$$f(T)^p = a_0^p + a_1^p T^p + \cdots + a_n^p T^{np} = a_0 + a_1 T^p + \cdots + a_n T^{np} = f(T^p)$$

■

Def 2.3

L/K を体拡大，$S \subset L$ を部分集合とする．K の拡大体であって S を包む最小のものを K に S を**添加した体** (**field obtained by adjoining** S) または K 上 S で**生成される体** (**field generated by** S) といい，$K(S)$ で表す．特に $S = \{s_1, \cdots, s_n\}$ のと

き，$K(S)$ を $K(s_1, \cdots, s_n)$ で表す．有限集合で K 上生成される体を K **上有限生成な体** (**finitely generated over** K) という．

Remark 2.3. $K(S)$ は次で与えられる．

$$K(S) = \left\{ \frac{f(s_1, \cdots, s_n)}{g(t_1, \cdots, t_n)} \mid \frac{f(T_1, \cdots, T_n)}{g(T_1, \cdots, T_n)} \in K(T_1, \cdots, T_n), s_i, t_i \in S, n \in \mathbb{N} \right\}$$

Remark 2.4. S_1, S_2 に対し $K(S_1 \cup S_2) = K(S_1)(S_2)$

Def 2.4
M_1, M_2 は体 L の部分体であるとき，$M_1 \cup M_2$ を包む最小の L の部分体を M_1, M_2 の**合成体** (**composite**) といい，$M_1 M_2$ で表す．

Remark 2.5. $M_1 M_2 = M_1(M_2) = M_2(M_1)$ である．

2.2 拡大次数

Def 2.5
L/K を体拡大とすると，L は K 線型空間と見做せる．この空間の次元 $\dim_K L$ を**拡大次数** (**extension degree**) といい，$[L : K]$ と表す．$[L : K] < \infty$ であるとき L/K は**有限次拡大** (**finite extension**)，$[L : K] = \infty$ であるとき**無限次拡大** (**infinite extension**) という．$[L : K] = d$ のとき，L/K は d **次拡大** (**dgree** d **extension**) という，

Example 2.2. (1)$[\mathbb{C} : \mathbb{R}] = 2$ (2)$[\mathbb{R} : \mathbb{Q}] = \aleph_1$

Prop 2.4 (有限次拡大の推移律)
$L/M/K$ を体拡大とする．このとき，$[L : K] = [L : M][M : K]$ である．特に，

$$L/M, M/K \text{ が有限次拡大} \Leftrightarrow L/K \text{ も有限次拡大}$$

$$\begin{tikzcd}
L \arrow[d, no head] \\
M \arrow[d, no head] \arrow[u, bend right, "\mathrm{fin}"'] \\
K \arrow[u, bend right, "\mathrm{fin}"'] \arrow[uu, bend left, "\mathrm{fin}"]
\end{tikzcd}$$

Proof. $\mathcal{A} = \{\alpha_\lambda\}_\lambda \subset L$ を L の M 上の基底，$\mathcal{B} = \{\beta_\mu\}_\mu \subset M$ を M の K 上の基底とする．

このとき $\mathcal{C} := \{\alpha_\lambda \beta_\mu\}_{\lambda,\mu} \subset L$ は L の K 上の基底となっている．よって

$$[L : K] = |\mathcal{C}| = |\mathcal{A}||\mathcal{B}| = [L : M][M : K]$$

■

Def 2.6
$\mathbb{Q}$ の有限次拡大体を**代数体** (**number field**) という．$[K : \mathbb{Q}] = d$ であるとき，K は d **次体** (**number field of degree** d) という．代数体は $\overline{\mathbb{Q}} \subset \mathbb{C}$ の部分体と見做せる．

3　代数拡大

3.1　代数拡大

Def 3.1

L/K を体拡大とする．**代入準同型 (evaluation homomorphism)**

$$\mathrm{ev}_\alpha\colon K[T] \to L,\ f(T) \mapsto f(\alpha)$$

の核

$$\operatorname{Ker} \mathrm{ev}_\alpha = \{f(T) \in K[T] \mid f(\alpha) = 0\}$$

は $K[T]$ のイデアルである．$K[T]$ は PID なので,

$$\exists p(T) \in K[T], \operatorname{Ker} \mathrm{ev}_\alpha = (p(T))$$

(1) $p(T) \neq 0$ のとき，$\alpha \in L$ は K **上代数的 (algebraic over K)** であるという．monic な $p(T)$ は unique であり，この $p(T)$ を α の K 上**最小多項式 (minimal polynomial)** という．

(2) $p(T) = 0$ のとき，$\alpha \in L$ は K **上超越的 (transcendental over K)** であるという．

L の任意の元が K 上代数的であるとき，L/K を**代数拡大 (algebraic extension)** という．そうでないとき，**超越拡大 (transcendental extension)** という．

$$\begin{tikzcd}
K[T] \arrow[r, "\mathrm{ev}_\alpha"] & L \\
\operatorname{Ker} \mathrm{ev}_\alpha = (p(T)) \arrow[u, "\iota"] \arrow[ur, dashed, "0"'] \arrow[u, phantom, shift right=8, "\circlearrowright"]
\end{tikzcd}$$

Remark 3.1. $\alpha \in L$ が K 上代数的 $\Leftrightarrow$ $\exists f(T) \in K[T] \setminus \{0\}, f(\alpha) = 0$

Remark 3.2. $L/M/K$ を体拡大とする．L/K が代数拡大 $\Rightarrow$ L/M も代数拡大

$$\begin{tikzcd}
L \\
M \arrow[u, dash] \arrow[u, bend right, "\mathrm{alg}"'] \\
K \arrow[u, dash] \arrow[uu, bend left=60, "\mathrm{alg}"]
\end{tikzcd}$$

Example 3.1. $\pi \in \mathbb{R}$ は $\mathbb{Q}$ 上超越的（$\because$ **Lindemann の定理**）なので $\mathbb{R}/\mathbb{Q}$ は超越拡大で

ある．

Example 3.2. K を体とすると，$T \in K(T)$ は K 上超越的なので $K(T)/K$ は超越拡大である．

Prop 3.1

L/K を体拡大とし，$\alpha \in L$ は K 上代数的とする．monic 多項式 $p(T) \in K[T] \setminus \{0\}$ について次は同値.

(1) $p(T)$ が α の K 上最小多項式

(2) $p(T)$ は $f(\alpha) = 0$ なる $f(T) \in K[T] \setminus \{0\}$ の中で次数最小のもの

(3) $p(\alpha) = 0$ かつ K 上既約

Proof. (1)⇒(2) まず $p(T) \in \operatorname{Ker} \mathrm{ev}_\alpha$ より $p(\alpha) = 0$．$f(\alpha) = 0, f(T) \in K[T] \setminus \{0\}$ とすると，$f(T) \in \operatorname{Ker} \mathrm{ev}_\alpha = (p(T))$ より

$$\exists q(T) \in K[T], f(T) = p(T)q(T)$$

なので $\deg p(T) \leq \deg f(T)$.
(2)⇒(3) $p(\alpha) = 0$ かつ $p(T) \neq 0$ が K 上既約でないとすると

$$\exists p_1(T), p_2(T) \in K[T] \setminus \{0\}, p(\alpha) = p_1(\alpha)p_2(\alpha) = 0, \deg p_i(T) < \deg p(T)$$

となるが L は整域なので $p_1(\alpha) = 0 \vee p_2(\alpha) = 0$．これは $p(T)$ の次数最小性に矛盾.
(3)⇒(1) $(p(T)) = \operatorname{Ker} \mathrm{ev}_\alpha$ を示す．$p(\alpha) = 0$ から $(p(T)) \subset \operatorname{Ker} \mathrm{ev}_\alpha$ は明白．$K[T]$ は UFD なので $p(T)$ が K 上既約なら素元である．よって $(p(T)) \neq (0)$ は素イデアルであるが $K[T]$ は PID なのでこれは極大イデアルである．$(p(T)) \subset \operatorname{Ker} \mathrm{ev}_\alpha \subsetneq K[T]$ と $(p(T))$ の極大性から $\operatorname{Ker} \mathrm{ev}_\alpha = (p(T))$.

■

Prop 3.2

L/K を体拡大とし，$\alpha \in L$ は K 上代数的であるとする．また $p(T)$ を α の K 上最小多項式とする．このとき，

(1) $K(\alpha) = K[\alpha]$

(2) $K(\alpha)$ の K 上の基底として $\mathcal{B} := \{1, \alpha, \cdots, \alpha^{n-1}\}$ $(n := \deg p(T))$ がとれる．特に $[K(\alpha) : K] = \deg p(T)$

Remark 3.3. $K[\alpha] := \operatorname{Im} \mathrm{ev}_\alpha$（代入準同型 $\mathrm{ev}_\alpha : K[T] \to L$ の像）

Proof. (1) $\supset$ は明白．$K[\alpha] \cong K[T]/\operatorname{Ker} \mathrm{ev}_\alpha$ は整域 L の部分環なので整域である．よって $\operatorname{Ker} \mathrm{ev}_\alpha$ は素イデアルである．また α は K 上代数的なので $\operatorname{Ker} \mathrm{ev}_\alpha \neq (0)$ であり，$K[T]$

は PID であるから $\operatorname{Ker}\mathrm{ev}_\alpha$ は極大イデアルである．従って，$K[\alpha] \cong K[T]/\operatorname{Ker}\mathrm{ev}_\alpha$ は α を含む体である．よって $K(\alpha) \subset K[\alpha]$.

$$\begin{tikzcd}
K[T] \arrow[r, "\mathrm{ev}_\alpha"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & K[\alpha] \subset L \\
K[T]/\operatorname{Ker}\mathrm{ev}_\alpha \arrow[ur, dashed, "\cong"'] &
\end{tikzcd}$$

(2) まず $\mathcal{B}$ が $K(\alpha)$ を生成することを見る．$p(T) = T^n + a_1T^{n-1} + \cdots + a_n$ とする．$m \geq n$ のとき

$$\alpha^m = -(a_1\alpha^{m-1} + \cdots + a_n\alpha^{m-n})$$

とできる．この次数下げを繰り返して，$\alpha^m \in \operatorname{Span}\mathcal{B}$ $(\forall m \in \mathbb{N})$ を得る．よって

$$K(\alpha) = K[\alpha] \subset \operatorname{Span}\mathcal{B}$$

次に線型独立性を見る．$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = 0$ $(c_i \in K)$ と仮定する．このとき

$$f(T) := c_0 + c_1T + c_2T^2 + \cdots + c_{n-1}T^{n-1}$$

と定めると $f(\alpha) = 0$ である．もし $f(T) \neq 0$ なら最小多項式 $p(T)$ の次数最小性に矛盾する．よって $f(T) = 0$，つまり $c_0 = \cdots = c_{n-1} = 0$.

■

Def 3.2

L/K を体拡大とする．$\exists\alpha \in L, L = K(\alpha)$ のとき，L/K は**単拡大** (**simple extension**) であるといい，この α を**生成元** (**generator**) という．

Remark 3.4. **Prop 3.2**(2) により，生成元 α が K 上代数的な単拡大 $K(\alpha)/K$ は有限次拡大である．

Prop 3.3

有限次拡大は代数拡大である．

Proof. L/K を有限次拡大とし，$\alpha \in L$ とする．ある $n \in \mathbb{N}$ が存在して $\{1, \alpha, \cdots, \alpha^n\}$ は線型従属となる．よって非自明な線型関係式 $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$ $(c_i \in K)$ がある．従って α は K 上代数的である． ■

Remark 3.5. 逆は成り立たない．例えば $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \cdots)/\mathbb{Q}$ は代数拡大だが無限次拡大である．

Prop 3.4 (代数拡大の推移律)
L/K を体拡大とする．

$$L/M, M/K \text{ が代数拡大} \Leftrightarrow L/K \text{ も代数拡大}$$

$$\begin{tikzcd}
L \\
M \arrow[u, dash] \arrow[u, bend right, "\mathrm{alg}"'] \\
K \arrow[u, dash] \arrow[u, bend right, "\mathrm{alg}"'] \arrow[uu, bend left, "\mathrm{alg}"]
\end{tikzcd}$$

Proof. $(\Rightarrow)$ $\alpha \in L$ とする．$p(T) = a_0 + \cdots + a_1 T + \cdots + a_{n-1}T^{n-1} + T^n \in M[T]$ を α の M 上の最小多項式とする．

$$M_0 := K,\ M_i := M_{i-1}(a_i)\ (1 \leq i \leq n)$$

で体の拡大列を定める．$a_i \in M$ は K 上代数的なので当然 M_i 上代数的である．よって $\forall i, [M_i : M_{i-1}] < \infty$．従って，

$$[M_n : K] = [M_n : M_{n-1}] \cdots [M_2 : M_1][M_1 : M_0] < \infty$$

また α は M_n 上代数的なので $[M_n(\alpha) : M_n] < \infty$．よって

$$[M_n(\alpha) : K] = [M_n(\alpha) : M_n][M_n : K] < \infty$$

従って $M_n(\alpha)/K$ は有限次拡大なので代数拡大であり，α は K 上代数的.
$(\Leftarrow)$ $\alpha \in L$ は K 上代数的なので当然 M 上代数的でもある．よって L/M は代数拡大．また，$\alpha \in M$ は $\alpha \in L$ でもあるので K 上代数的．よって M/K は代数拡大. ■

Cor 3.1
L/K を体拡大とすると，

$$K^{\mathrm{alg}} := \{\alpha \in K \mid \alpha \text{ is algebraic over K}\}$$

は L/K の中間体である．

Proof. $\alpha, \beta \in K^{\mathrm{alg}}$ とすると $K(\alpha, \beta)/K$ は代数拡大であることを示せば

$$\alpha + \beta, \alpha\beta \in K^{\mathrm{alg}}, \alpha^{-1} \in K^{\mathrm{alg}}\ (\alpha \neq 0)$$

が従い，$L/K^{\mathrm{alg}}/K$ がいえる．$K(\beta)/K$ は代数拡大であるから，β は当然 $K(\alpha)$ 上代数的．$K(\alpha)/K$ と $K(\alpha)(\beta)/K(\alpha)$ が代数拡大であることから $K(\alpha, \beta)/K$ が代数拡大である．$(K(\alpha, \beta) = K(\alpha)(\beta))$ ■

3.2　最小分解体

Def 3.3
K を体，$f(T) \in K[T] \setminus K$ とする．$f(T)$ の根を全て含む K の拡大体を $f(T)$ の**分解体** (**splitting field**) という．$f(T)$ の分解体の中で最小のものを $f(T)$ の**最小分解体** (**smallest splitting field**) という．

Remark 3.6. $f(T) \in K[T]$ の分解体 L とは，$\alpha_1, \cdots, \alpha_n \in L$ が存在して，

$$f(T) = (T - \alpha_1) \cdots (T - \alpha_n)$$

と $f(T)$ を 1 次式の積に分解できるものである．

Example 3.3. $T^4 - 5T^2 + 6 \in \mathbb{Q}[T]$ の最小分解体は $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Thm 3.1 (**Kronecker の定理**)
K を体，$f(T) \in K[T], \deg f(T) > 0$ とすると，$f(T)$ の分解体 L が存在する．

Proof. $n := \deg f(T)$ に関する帰納法による．

$n = 1$ のとき，$L = K$ とすればよい．

$n \geq 2$ とし，n 未満での成立を仮定する．$f(T)$ が可約であるときは n 未満の次数の多項式に分解され，仮定からそれぞれが 1 次式の積に分解できる拡大体があるので $f(T)$ も 1 次式の積に分解できる．

$f(T)$ が既約であるとき，$K[T]$ が PID なので素イデアル $(f(T))$ は極大イデアル．よって $L := K[T]/(f(T))$ は体である．また，$\iota : K \hookrightarrow K[T]$ を包含，$\pi : K[T] \to K[T]/(f(T))$ を射影とすると，$\pi|_K = \pi \circ \iota : K \hookrightarrow L$ は単射である．これを通して L は K の拡大体と見做せる．

$$\begin{tikzcd}
K \arrow[r, "\iota"] \arrow[dr, dashed, "\pi|_K"'] \arrow[dr, phantom, shift left=4ex, "\circlearrowright"] & K[T] \arrow[d, "\pi"] \\
& L = K[T]/(f(T))
\end{tikzcd}$$

$\alpha := \pi(T) \in L$ とすると，$f(\alpha) = 0$ より $f(T) = (T - \alpha)g(T)$ と分解できる．$\deg g = n - 1 < n$ より g に仮定を適用すれば $f(T)$ は 1 次式の積に分解できる． ■

3.3　共軛

Def 3.4
L/K を体拡大，$\alpha \in L$ は K 上代数的とする．α の K 上最小多項式を $p(T)$ とするとき，$p(T)$ の根[†5]を α の K 上**共軛** (**conjugate**) という．

Example 3.4. (1) $1+\sqrt{2} \in \mathbb{C}$ の $\mathbb{Q}$ 上共軛は $1 \pm \sqrt{2}$.
(2) $\sqrt[3]{2} \in \mathbb{C}$ の $\mathbb{Q}$ 上共軛は $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$.
(3) $z \in \mathbb{C}$ の $\mathbb{R}$ 上共軛は z と複素共軛 $\overline{z} = \Re(z) - \Im(z)\sqrt{-1}$.

Prop 3.5
$L/K, F/K$ を代数拡大，$\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, F), \alpha \in L, f(T) \in K[T], f(\alpha) = 0$ とする．このとき $f(\varphi(\alpha)) = 0$．特に $\varphi(\alpha)$ は α の K 上共軛．

Proof. $\varphi|_K = \mathrm{id}_K$ に注意すると，$0 = \varphi(0) = \varphi(f(\alpha)) =$[†6]$\varphi(f)(\varphi(\alpha)) = f(\varphi(\alpha))$ ∎

Prop 3.6
L/K を代数拡大, $\alpha, \beta \in L$ は K 上の共軛とする. このとき, K 同型 $\sigma : K(\alpha) \cong K(\beta)$ で $\sigma(\alpha) = \beta$ なるものが存在する.

Proof. $p(T)$ を α の K 上最小多項式とすると，$K(\alpha) \cong K[T]/(p(T))$ である．ここで

$$\mathrm{ev}_\beta : K[T] \to K[\beta], f(T) \mapsto f(\beta)$$

を考えると，$p(\beta) = 0$ より $p(T) \in \mathrm{Ker}\,\mathrm{ev}_\beta$ である．よって環の準同型定理により，全射 K 準同型 $\varphi : K[T]/(p(T)) \to K[\beta]$ で，$\varphi(T + (p(T))) = \beta$ なるものが存在する．

$$\begin{tikzcd}
K[T] \arrow[r, "\mathrm{ev}_\beta"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & K[\beta] \\
K[T]/(p(T)) \arrow[ur, dashed, "\varphi"'] &
\end{tikzcd}$$

[†5] $p(T)$ の分解体を考えれば全ての根が取れる．
[†6] $f(T) = a_0 + a_1 T + \cdots + a_n T^n \in K_1[T], \varphi \in \mathrm{Hom}^{\mathrm{al}}(K_1, K_2)$ に対し，

$$\varphi(f)(T) := \varphi(a_0) + \varphi(a_1)T + \cdots + \varphi(a_n)T^n \in K_2[T]$$

$K[T]/(p(T))$ は体なので φ は単射であるから，

$$K(\alpha) \cong K[T]/(p(T)) \cong K[\beta] = K(\beta)$$

■

Prop 3.7

L/K を代数拡大とする．

$$\alpha, \beta \in L \text{ は } K \text{ 上共軛} \Leftrightarrow \alpha, \beta \in L \text{ の } K \text{ 上最小多項式は等しい．}$$

Proof. $(\Rightarrow)$ $p(T)$ を α の K 上最小多項式とすると，$p(\beta) = 0$ である．**Prop 3.1**(1)⇒(3) から $p(T)$ は K 上既約なので，再び **Prop 3.1**(3)⇒(1) からは β の K 上最小多項式でもある．
$(\Leftarrow)$ 定義より明白．■

Example 3.5. $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\omega)$

4 代数閉包

Def 4.1
K を体とする．任意の $f(T) \in K[T] \setminus K$ に対し，その任意の根が K に属するとき，K を**代数閉体** (**algebraically closed field**) という．

Remark 4.1. K 代数閉体の代数拡大は自身のみである．

Example 4.1. $\mathbb{C}$ は代数閉体である．（**代数学の基本定理** (**the fundamental theorem of algebra**)）

Def 4.2
Ω/K が代数拡大，Ω が代数閉体であるとき，Ω を K の**代数閉包** (**algebraically closure**) という．

Example 4.2. $\mathbb{C}$ は $\mathbb{R}$ の代数閉包である．しかし $[\mathbb{C} : \mathbb{Q}]$ は代数拡大ではないので $\mathbb{Q}$ の代数閉包ではない．

Prop 4.1
L/K を体拡大，L は代数閉体とすると，

$$K^{\mathrm{alg}} := \{\alpha \in L \mid \alpha \text{ is algebraic over K}\}$$

は K の代数閉包である．

Proof. 体であることは示した．また K^{alg}/K が代数拡大であることは定義から明白．代数閉体であることを示そう．$f(T) \in K^{\mathrm{alg}}[T] \setminus K^{\mathrm{alg}}$ とすると L が代数閉体であることから

$$\exists a \in K^{\mathrm{alg}}, \exists \alpha_i \in L, f(T) = a(T - \alpha_1) \cdots (T - \alpha_n)$$

α_i は $f(T) \in K^{\mathrm{alg}}[T]$ の根であるから，α_i は K^{alg} 上代数的．$K^{\mathrm{alg}}(\alpha_i)/K^{\mathrm{alg}}, K^{\mathrm{alg}}/K$ が代数拡大なので **Prop 3.4** により $K^{\mathrm{alg}}(\alpha_i)/K$ も代数拡大．よって α_i は K 上代数的であるから $\alpha_i \in K^{\mathrm{alg}}$．従って K^{alg} は代数閉体である． ■

$$\begin{tikzcd}
L \arrow[d, dash] \\
K^{\mathrm{alg}}(\alpha_i) \arrow[d, dash] \\
K^{\mathrm{alg}} \arrow[u, bend right, "\mathrm{alg}"'] \arrow[d, dash] \\
K \arrow[u, bend right, "\mathrm{alg}"'] \arrow[uu, bend left, "\mathrm{alg}"]
\end{tikzcd}$$

4.1 代数閉包の存在と一意性

Thm 4.1 (**Steinitz の定理**)
任意の体 K に対し，K の代数閉包 Ω が unique に存在する．[†7]

以降，この定理を前半（存在性）と後半（一意性）に分けて示す．

Thm 4.2
任意の体 K に対し，K の拡大体であって代数閉なものが存在する

Remark 4.2. これが示されれば **Prop 4.1** より，任意の体 K の代数閉包が存在することがいえる．

Proof.

$$\mathscr{P} := \{f(T) \in K[T] \mid f(T) \text{ is irreducible}\}^{\dagger 8}$$

とする．各 $f(T) \in \mathscr{P}$ ごとに変数 T_f を考える．多変数多項式環 $A := K[\{T_f\}_{f\in\mathscr{P}}]$ のイデアル $I := (\{f(T_f)\}_{f\in\mathscr{P}})$ を考えると，$I \subsetneq A$ である．

($\because$) $I = A$ と仮定する．このとき $1 \in I$ より，

$$\exists\{a_j\}_{j=1}^n \subset A, \exists\{f_j(T)\}_{j=1}^n \subset \mathscr{P}, 1 = \sum_{j=1}^n a_j f_j(T_{f_j}) \qquad (*)$$

$\{f_j(T)\}_{j=1}^n \subset K[T]$ の最小分解体 F を取ると，

$$\exists\{\alpha_j\}_{j=1}^n \subset F, \forall j, f_j(\alpha_j) = 0$$

$(*)$ において，$f_j(\alpha_j) = 0$ を代入すると，

$$1 = \sum_{j=1}^n a_j f_j(\alpha_j) = 0$$

A は零環でないのでこれは矛盾．よって $I \subsetneq A$.

$I \subsetneq A$ より $I \subseteq \mathfrak{m} \subsetneq A$ なる極大イデアル $\mathfrak{m}$ が存在する．$L_1 := A/\mathfrak{m}$ とおくとこれは体である．また，$\iota : K \hookrightarrow K[\{T_f\}_{f\in\mathscr{P}}] = A$ を包含，$\pi : A \to A/\mathfrak{m} = L_1$ を射影とすると，$\pi|_K = \pi \circ \iota : K \hookrightarrow L_1$ は単射である．これを通して L_1 は K の拡大体と見做せる．

[†7] この定理は ZF 上では証明できず，選択公理を避けられないことが知られている．

$$\begin{tikzcd} K \arrow[r, "\iota"] \arrow[rd, dashed, "\pi|_K"'] & A = K[\{T_f\}_{f \in \mathscr{P}}] \arrow[d, "\pi"] \\ & L_1 = A/\mathfrak{m} \end{tikzcd}$$

$f(T) \in \mathscr{P}$ とすると，$f(T_f) \in \mathfrak{m}$ なので，

$$f(\pi(T_f)) = f(T_f + \mathfrak{m}) = f(T_f) + \mathfrak{m} = 0 \in L_1$$

なので，$f(T)$ は $\alpha := \pi|_K (T_f) \in L_1$ をもつ．

以上の議論で K を L_1 に置き換えればさらに拡大体 L_2 を得る．同様にこれを繰り返して体の拡大列 $K \subset L_1 \subset L_2 \subset \cdots$ が構成される．そこで

$$\Omega := \bigcup_{n=1}^{\infty} L_n$$

とおくと Ω は体である．

> $(\because)\alpha, \beta \in \Omega$ とすると，充分大きい $N \in \mathbb{N}$ に対し，$\alpha, \beta \in L_N$．当然 L_N は体なので，
>
> $$\alpha + \beta, \alpha\beta \in L_N \subset \Omega,\ \alpha^{-1} \in L_N \subset \Omega\ (\alpha \neq 0)$$

Ω は代数閉であることを示そう．$f(T) = a_0 + a_1 T + \cdots + a_n T^n \in \Omega[T]$ とする．充分大きい $N \in \mathbb{N}$ に対し，$a_0, \cdots, a_n \in L_N$ で $f(T) \in L_N[T]$ である．このとき，

$$\exists \alpha_1 \in L_{N+1}, \exists g_1(T) \in L_{N+1}[T], f(T) = (T - \alpha_1) g_1(T)$$

これを繰り返して，

$$\exists \alpha_1, \cdots, \alpha_n \in L_{N+n} \subset L,\ f(T) = a_n (T - \alpha_1) \cdots (T - \alpha_n)$$

よって，$f(T)$ の根は全て Ω に属するから Ω は代数閉．　■

> **Prop 4.2**
> L/K は体拡大，Ω は K の代数閉包，$\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, \Omega)$ とする．$L(\alpha)/L$ が代数拡大なら φ の $L(\alpha)$ への延長 $\omega \in \mathrm{Hom}_K^{\mathrm{al}}(L(\alpha), \Omega)$ が存在する．

[†8] n 次多項式 $f(T) \in K[T]$ を K^{n+1} の元と見做せば，$\mathscr{P} \subset \bigcup_{n=0}^{\infty} K^{n+1}$ と見做せる．よって $\mathscr{P}$ は集合.

$$
\begin{tikzcd}
 & \Omega \arrow[ddd, dash] \\
L(\alpha) \arrow[ur, dashed, "\omega"] \arrow[d, dash] \arrow[r, phantom, "\circlearrowright"] & \\
L \arrow[uur, "\varphi"'] \arrow[d, dash] & \\
K \arrow[r, "\mathrm{id}_K"] & K
\end{tikzcd}
$$

Proof. $p(T) \in L[T]$ を α の L 上最小多項式とすると，$L(\alpha) \cong L[T]/(p(T))$ である．

$$q(T) := \varphi(p)(T) \in \varphi(L)[T] \subset \Omega[T]$$

とすると，$L \cong \varphi(L)$ なので $q(T)$ は $\varphi(L)$ 上既約である．このとき，

$$L[T]/(p(T)) \xrightarrow{\cong} \varphi(L)[T]/(q(T)),\ f(T) + (p(T)) \mapsto \varphi(f)(T) + (q(T))$$

である．また Ω は代数閉なので $\exists \beta \in \Omega, q(\beta) = 0$ である．$q(T)$ は β の $\varphi(L)$ 上最小多項式であるから，$L(\beta) \cong \varphi(L)[T]/(q(T))$ よって，

$$\widetilde{\varphi} : L(\alpha) \cong L[T]/(p(T)) \cong \varphi(L)[T]/(q(T)) \cong L(\beta)$$

$\widetilde{\varphi}$ は φ の延長になっている．$\omega := \iota_{L(\beta)} \circ \widetilde{\varphi}$ とすればこれが求めるべき延長である．

■

$$
\begin{tikzcd}
 & & \Omega \arrow[d, dash, "\iota_{L(\beta)}"] & \\
L[T]/(p(T)) \arrow[r, "\cong"] & L(\alpha) \arrow[ur, dashed, "\omega"] \arrow[r, "\cong", "\widetilde{\varphi}"'] \arrow[d, dash] & L(\beta) \arrow[d, dash] & \varphi(L)[T]/(q(T)) \arrow[l, "\cong"'] \\
L[T] \arrow[u, "\pi"] & L \arrow[l, "\iota"] \arrow[r, "\cong", "\varphi"'] \arrow[d, dash] & \varphi(L) \arrow[r, "\iota"'] \arrow[d, dash] & \varphi(L)[T] \arrow[u, "\pi"'] \\
 & K \arrow[r, "\mathrm{id}_K"'] & K &
\end{tikzcd}
$$

Thm 4.3

$\Omega_1/L_1/K_1, \Omega_2/L_1/K_1$ を代数拡大，Ω_1, Ω_2 を代数閉体，$\sigma : L_1 \to L_2$ は K 同型とする．このとき，σ の拡張となる K 同型 $\overline{\sigma} : \Omega_1 \to \Omega_2$ が存在する．

$$
\begin{tikzcd}
\Omega_1 \arrow[rr, "\cong", "\overline{\sigma}"'] \arrow[d, dash] & & \Omega_2 \arrow[d, dash] \\
L_1 \arrow[rr, "\cong", "\sigma"'] \arrow[d, dash] \arrow[urr, phantom, "\circlearrowright"] & & L_2 \arrow[d, dash] \\
K \arrow[rr, "\mathrm{id}_K"'] \arrow[urr, phantom, "\circlearrowright"] & & K
\end{tikzcd}
$$

Remark 4.3. この定理が示されれば体 K の代数閉包は同型を除いて unique であることがいえる．これに基づいて K の代数閉包を $\overline{K}$ とかく．

Proof.

$$\mathscr{F} := \{(M, \varphi) \mid \Omega_1/M/L_1, \varphi \in \mathrm{Hom}_K^{\mathrm{al}}(M, \Omega_2), \left.\varphi\right|_{L_1} = \sigma\}$$

とおき，$(M_1, \varphi_1), (M_2, \varphi_2) \in \mathscr{F}$ に対し，

$$(M_1, \varphi_1) \preceq (M_2, \varphi_2) \;:\Leftrightarrow\; M_2/M_1,\ \left.\varphi_2\right|_{M_1} = \varphi_1$$

と定めると，$\preceq$ は $\mathscr{F}$ 上の半順序である．

$$
\begin{tikzcd}
\Omega_1 \arrow[d, dash] & & \Omega_2 \arrow[ddd, dash] \\
M_2 \arrow[urr, "\varphi_2"] \arrow[d, dash] \arrow[r, phantom, "\circlearrowright"] & {} & \\
M_1 \arrow[uurr, "\varphi_1"'] \arrow[d, dash] & & \\
L_1 \arrow[rr, "\sigma"'] & & L_2
\end{tikzcd}
$$

$\mathscr{C} \subset \mathscr{F}$ が全順序部分集合であるとき，$\widehat{M} := \displaystyle\bigcup_{(M,\varphi)\in\mathscr{F}} M$ とおく．$x \in \widehat{M}$ に対し，$x \in M$ なる $(M, \varphi) \in \mathscr{C}$ を選択し，$\widehat{\varphi}(x) := \varphi(x)$ と定める．この $\widehat{\varphi}$ は well-defined である．

> $(\because)$ $x \in M_1, M_2, (M_1, \varphi_1), (M_2, \varphi_2) \in \mathscr{C}$ であったとする．$\mathscr{C}$ は全順序部分集合なので $(M_1, \varphi_1) \preceq (M_2, \varphi_2)$ としても一般性を失わない．このとき，$\left.\varphi_2\right|_{M_1} = \varphi_1$ より $\varphi_1(x) = \varphi_2(x)$.

$(\widehat{M}, \widehat{\varphi})$ は $\mathscr{C}$ の上界である．Zorn の補題により，$\mathscr{F}$ には極大元 $(\Omega, \overline{\sigma})$ が存在する．このとき，$\Omega = \Omega_1$ である．

> $(\because)$ $\Omega \subsetneq \Omega_1$ と仮定する．$\alpha \in \Omega_1 \setminus \Omega$ を取ると，Ω_1/K が代数拡大なので α は Ω 上代数的．よって，**Prop 4.2** より $\overline{\sigma}$ の $\Omega(\alpha)$ への延長 $\widetilde{\overline{\sigma}}$ が存在する．このとき，$(\Omega, \overline{\sigma}) \prec (\Omega(\alpha), \widetilde{\overline{\sigma}})$ であり，$(\Omega, \overline{\sigma})$ の極大性に矛盾する．

よって σ の延長となる $\overline{\sigma} \in \mathrm{Hom}_K^{\mathrm{al}}(\Omega_1, \Omega_2)$ の存在がいえた．さらにこの $\overline{\sigma}$ は K 同型である．

> ($\because$) 単射は明白なので $\overline{\sigma}(\Omega_1) = \Omega_2$ を示す．($\subset$) は明白．$\alpha \in \Omega_2$ とし，α の K 上の最小多項式を $p(T) \in K[T]$ とする．$\overline{\sigma}(\Omega_1) \cong \Omega_1$ は代数閉なので，
>
> $$\exists \beta_1 \cdots, \beta_n \in \overline{\sigma}(\Omega_1),\ p(T) = (T - \beta_1) \cdots (T - \beta_n)$$
>
> $p(\alpha) = 0$ なので
>
> $$\exists i \in \{1, \cdots, n\},\ \alpha = \beta_i \in \overline{\sigma}(\Omega_1)$$
>
> よって $\Omega_2 \subset \overline{\sigma}(\Omega_1)$.

■

Cor 4.1
L/K が代数拡大なら，$\overline{L} = \overline{K}$

Proof. **Thm 4.3** で $L_1 = K, L_2 = L$ とすればよい．■

Def 4.3
$(X, \preceq)$ を半順序集合とする．写像 $\mathrm{cl} : X \to X$ が次の条件を充たすとき，cl を**閉包作用素** (**closure operator**) という．

(1) $\forall x \in X, x \preceq \mathrm{cl}(x)$ (拡大性 extensive)
(2) $\forall x \in X, \mathrm{cl}(x) = \mathrm{cl}(\mathrm{cl}(x))$ (冪等性 idempotemt)
(3) $\forall x, y \in X, x \preceq y \Rightarrow \mathrm{cl}(x) \preceq \mathrm{cl}(y)$ (単調性 isotone)

このとき，$x \in X$ であって $\mathrm{cl}(x) = x$ を充たすものを cl に関する**閉元** (**closed element**) という．

Example 4.3. $(X, \mathcal{O})$ を位相空間，$\mathcal{F}$ をその閉集合系とする．$\mathfrak{P}(X)$ は包含に関して半順序集合である．$\mathrm{cl} : \mathfrak{P}(X) \to \mathfrak{P}(X)$ を，

$$\mathrm{cl}(A) := \bigcap_{A \subset C, C \in \mathcal{F}} C$$

と定めると，cl は閉包作用素になる

Remark 4.4. 同型を同一視した体全体のクラスにおいて，$K_1 \preceq K_2$ を K_2/K_1 が代数拡大であることと定めればこれは半順序である．このクラス上で代数閉包を取る操作は閉包作用素の公理を充たす．

Prop 4.3
L/K を代数拡大，$\alpha \in L$ とする．

$$\beta \in \overline{K} \text{ は } K \text{ 上共軛} \Leftrightarrow \exists \sigma \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}),\ \sigma(\alpha) = \beta$$

Proof. ($\Rightarrow$) **Prop 3.6** から K 同型 $\sigma_0 : K(\alpha) \cong K(\beta)$ で $\sigma_0(\alpha) = \beta$ なるものが存在する．**Prop 4.3** から $\overline{\sigma_0} \in \mathrm{Aut}_K^{\mathrm{al}}(\overline{K})$ に拡張できる．$\sigma := \overline{\sigma_0}|_L$ とすればよい．
($\Leftarrow$) **Prop 3.5** と同じ主張である． ■

5　分離拡大

5.1　分離多項式

Def 5.1

K を体とする．

(1) $\alpha \in \overline{K}$ であり，$f(T) \in \overline{K}[T]$ が $\overline{K}[T]$ 上で $(T-\alpha)^2$ で割り切れるとき，α を $f(T)$ の**重根** (**multiple root**) という．

(2) $f(T) \in K[T]$ が $\overline{K}$ において重根をもたないとき，$f(T)$ は**分離多項式** (**separable polynomial**) という．

Def 5.2

k を可換環とする．1 変数多項式 $f(T) = a_0 + a_1 T + \cdots + a_n T^n \in k[T]$ に対し，

$$\frac{df}{dT}(T) = f'(T) := a_1 + 2a_2 T + \cdots + nT^{n-1} \in k[T]$$

を $f(T)$ の**微分** (**derivation**) という．[†9]また，n 変数多項式

$$f(T_1, \cdots, T_n) = \sum_{i_1, \cdots, i_n} a_{i_1, \cdots, i_n} T_1^{i_1} \cdots T_n^{i_n} \in k[T_1, \cdots, T_n]$$

に対し，

$$g(T_j) := \sum_{i_j} \left(\sum_{\substack{i_1, \cdots, i_{j-1}, \\ i_{j+1} \cdots, i_n}} a_{i_1, \cdots, i_n} T_1^{i_1} \cdots T_{j-1}^{i_{j-1}} T_{j+1}^{i_{j+1}} \cdots T_n^{i_n} \right) T_j^{i_j} \in k[T_1, \cdots, T_{j-1}, T_{j+1}, \cdots, T_n][T_j]$$

を考え，

$$\frac{\partial f}{\partial T_j}(T_1, \cdots, T_n) = \partial_{T_j} f(T_1, \cdots, T_n) := \frac{dg}{dT_j}(T_j) \in k[T_1, \cdots, T_n]$$

と定める．これを $f(T_1, \cdots, T_n)$ の T_j に関する**偏微分** (**pertial derivation**) という．

[†9] 線型性や Leibniz rule，chain rule が当然成り立つ．

Prop 5.1
$f(T) \in K[T], \alpha \in \overline{K}$ とする.

$$\alpha \text{ が } f(T) \text{ の重根} \Leftrightarrow \ f(\alpha) = f'(\alpha) = 0$$

Proof. ($\Rightarrow$) 仮定から $\exists g(T) \in \overline{K}[T], f(T) = (T-\alpha)^2 g(T)$ で,

$$f'(T) = 2(T-\alpha)g(T) + (T-\alpha)^2 g'(T)$$

から $f'(\alpha) = 0$
($\Leftarrow$) 剰余の定理により $\exists g(T) \in \overline{K}[T], \exists p, q \in \overline{K}, f(T) = (T-\alpha)^2 g(T) + pT + q$ であるが,

$$f(T) = 2(T-\alpha)g(T) + (T-\alpha)^2 g'(T) + p$$

仮定から $p\alpha + q = 0, p = 0$ なので $p = q = 0$ を得る. ■

Cor 5.1
$f(T) \in K[T]$ とする．次は同値.

(1) $f(T)$ は分離多項式.
(2) $f(T)$ と $f'(T)$ は $K[T]$ の元として互いに素.

Proof. (1)$\Rightarrow$(2) もし $f(T)$ と $f'(T)$ は $K[T]$ の元として互いに素でなければ,

$$\exists g(T) \in K[T] \setminus K, g(T) | f(T), g(T) | f'(T)$$

$g(\alpha) = 0$ なる $\alpha \in \overline{K}$ に対し，$f(\alpha) = f'(\alpha) = 0$. **Prop 5.1** により α は $f(T)$ の重根．これは矛盾.
(2)$\Rightarrow$(1) $f(T)$ と $f'(T)$ は $K[T]$ の元として互いに素なら,

$$\exists a(T), b(T) \in K[T], a(T)f(T) + b(T)f'(T) = 1$$

もし, $\alpha \in \overline{K}$ が $f(T)$ の重根なら, **Prop 5.1** により, $f'(\alpha) = 0$ だが, $a(v)f(\alpha) + b(\alpha)f'(\alpha) = 0$ となり矛盾. ■

Prop 5.2
$f[T] \in K[T]$ は K 上既約とする.

$$f(T) \text{ が分離多項式} \Leftrightarrow f'(T) \neq 0$$
$$f(T) \text{ が非分離多項式} \Leftrightarrow f'(T) = 0$$

Proof. $f(T)$ が非分離多項式 $\Leftrightarrow$ $f(T) = 0$ を示す.
($\Rightarrow$) 仮定から $f(T)$ と $f'(T)$ は $K[T]$ は互いに素でないので,

$$\exists a(T) \in K[T] \setminus K, \ a(T) \mid f(\alpha), \ a(T) \mid f'(\alpha)$$

ここで $f[T]$ は K 上既約なので，$\exists k \in K$，$f(T) = ka(T)$．よって，$f(T)|f'(T)$．$f'(T) \neq 0$ なら，$\deg f'(T) < \deg f(T)$ となり矛盾．

($\Leftarrow$) $f(T)$ の根 $\alpha \in \overline{K}$ を取ると，$f(\alpha) = f'(\alpha) = 0$ なので，**Prop 5.1** から α は重根． ■

Prop 5.3

$\mathrm{ch}\, K = 0$ なる体 K に対し，既約多項式 $f(T) \in K[T]$ は分離多項式．

Proof. $f(T) = a_0 + a_1 T + \cdots + a_n T^n \in K[T]$ を既約多項式，$\deg f(T) = n$ とすると，$f'(T) = n a_n T^{n-1} + \cdots \neq 0$ なので **Prop 5.2** より $f(T) \in K[T]$ は分離多項式． ■

Example 5.1. $f(T) = T^2 + 1 \in \mathbb{R}[T]$ は $f'(T) = 2T \neq 0$ より分離多項式.

Prop 5.4

K は $\mathrm{ch}\, K = p > 0$ なる体とする．このとき次は同値.

(1) $f(T)$ は非分離多項式

(2) $\exists g(T) \in K[T] : K$上既約分離多項式$, \exists n > 0, f(T) = g(T^{p^n})$

Example 5.2. $f(T) = T^2 + 1 \in \mathbb{F}_2[T]$ は分離多項式ではない．($g(T) = T + 1, n = 1$ とすれば $f(T) = g(T^2)$ である．) 実際,

$$f(T) = T^2 + 1 = T^2 - 2T + 1 = (T - 1)^2$$

なので重根 1 をもつ.

5.2　分離拡大と完全体

Def 5.3

K を体とする.

(1) $\alpha \in \overline{K}$ に対し，α の K 上最小多項式が分離多項式であるとき，α は K 上**分離的** (**separable over** K)，そうでないとき**非分離的** (**inseparable**) であるという.

(2) L/K を代数拡大とする．L の任意の元が K 上分離的であるとき，L/K は**分離拡大** (**separable extension**)，そうでないとき**非分離拡大** (**inseparable extension**) であるという.

Remark 5.1. $L/M/K$ を代数拡大とする．$\alpha \in L$ が K 上分離的なら M 上でも分離的である.

> $(\because)$ α の M 上の最小多項式 $g(T)$ は α の K 上の最小多項式 $f(T)$ を割り切る．よって $f(T)$ が重根を持たないとき，$g(T)$ も重根を持たない．

従って，L/K が分離拡大 $\Rightarrow$ L/M も分離拡大

$$
\begin{tikzcd}
L \arrow[d, dash] \arrow[d, bend left, "\mathrm{sep}"'] \\
M \arrow[d, dash] \\
K \arrow[uu, bend left, "\mathrm{sep}"]
\end{tikzcd}
$$

Example 5.3. (1) $\sqrt[3]{2} \in \overline{\mathbb{Q}}$ は $\mathbb{Q}$ 上分離的．実際，$\mathbb{Q}$ 上の最小多項式 $p(T) = T^3 - 2$ は $p'(T) = 3T^2 \neq 0$ から分離多項式．

(2) $\sqrt[3]{X} \in \overline{\mathbb{F}_3(X)}$ は $\mathbb{F}_3(X)$ 上非分離的．実際，$\mathbb{F}_3(X)$ 上の最小多項式 $p(T) = T^3 - X$ は $p'(T) = 0$ または $p(T) = (T - X)^3$ から非分離多項式．

Prop 5.5

K は $\mathrm{ch}\,K = p > 0$ なる体，L/K を体拡大とする．$\alpha \in L \setminus K$ が，

$$\exists N \geq 0,\ \alpha^{p^{N-1}} \notin K, \alpha^{p^N} \in K$$

を充たすとき, α は K 上非分離的で, α の K 上最小多項式は $T^q - \beta$ $(q := p^N, \beta := \alpha^q)$ である．

Proof. *Proof*(1) of **Prop 2.3** より $T^q - \beta = (T - \alpha)^q$ であるから，α の K 上最小多項式は $p(T) = (T - \alpha)^n$ $(0 < n \leq q)$ とかける．$n < q$ と仮定する．このとき, $n = p^i m, \gcd(m, p) = 1$ とすると,

$$p(T) = (T - \alpha)^{p^i m} = (T^{p^i} - \alpha^{p^i})^m$$

$\alpha^{p^{N-1}} \notin K$ から $\alpha^{p^i} \notin K$ であり $p(T) = T^n - m\alpha^{p^i} T^{p^i(m-1)} + \cdots$ であるが，$m\alpha^{p^i} \notin K$ なので $p(T) \in K[T]$ に矛盾する．よって $p(T) = (T - \alpha)^q = T^q - \beta$（非分離多項式）であり，$\alpha$ は K 上非分離的． ■

Def 5.4

K は $\mathrm{ch}\,K = p > 0$ なる体とするとき,

$$K^{p^{-1}} := \{\alpha \in \overline{K} \mid \alpha^p \in K\}$$

と定める．

Remark 5.2. $K^{p^{-1}}$ は Frobenius 準同型 $\mathrm{Frob}_p : \overline{K} \to \overline{K}$ による部分体 $K \subset \overline{K}$ の逆像なので

$\overline{K}$ の部分体である．また，$K^{p^{-1}}/K$ は明白である．$K^{p^{-1}}$ は K の元の p 乗根全体で K 上生成される体である．

Def 5.5
任意の代数拡大が分離拡大となる体を**完全体** (**perfect field**) という．

Remark 5.3. **Prop 5.3** より標数 0 の体は完全体である．

Prop 5.6
K は $\mathrm{ch}\, K = p > 0$ なる体とする．

$$K \text{ は完全体} \quad \Leftrightarrow \quad K^{p^{-1}} = K$$

Proof. ($\Rightarrow$) $K^{p^{-1}} \supsetneq K$ と仮定すると，$\exists \alpha \in \overline{K} \setminus K, \alpha^p := \beta \in K$．しかし **Prop 5.5** より $T^p - \beta = (T - \alpha)^p$ は K 上既約．これは非分離多項式なので K が完全体であることに矛盾する．よって $K^{p^{-1}} = K$．
($\Leftarrow$) まず仮定より，

$$\forall a \in K, \forall n > 0, \exists b \in K, \ a = b^{p^n}$$

($\because$) $a \in K$ とすると $a \in K^{p^{-1}}$ から $\exists c_1 \in K, a = c_1^p$．また $c_1 \in K^{p^{-1}}$ より $\exists c_2 \in K, c_1 = c_2^p$．よって $a = c_2^{p^2}$．これを繰り返して $b := c_n$ とすればよい．

$f(T) \in K[T]$ は既約とする．ここで $f(T)$ が非分離多項式であると仮定すると，**Prop 5.4** より，

$$\exists g(T) = a_0 + \cdots + a_{m-1}T^{m-1} + T^m \in K[T] : K\text{上既約分離}, \exists n > 0, f(T) = g(T^{p^n})$$

上の議論から $\forall i \in \{0, \cdots, m-1\}, \exists b_i \in K, a_i = b_i^{p^n}$ であるから，

$$\begin{aligned} f(T) &= a_0 + \cdots + a_{m-1}T^{p^n(m-1)} + T^{p^n m} \\ &= b_0^{p^n} + \cdots + b_{m-1}^{p^n} T^{p^n(m-1)} + T^{p^n m} = (b_0 + \cdots + b_{m-1}T^{m-1} + T^m)^{p^n} \end{aligned}$$

となり，$f(T)$ が K 上既約であることに矛盾．よって $f(T)$ は分離多項式である．従って $\overline{K}$ の任意の元は K 上分離的．■

Example 5.4. $\sqrt[p]{T} \in \mathbb{F}_p(T)^{p^{-1}} \setminus \mathbb{F}_p(T)$ より $\mathbb{F}_p(T)$ は完全体でない．

Cor 5.2
有限体は完全体である．

Proof. Frobenius 準同型 $\mathrm{Frob}_p : K \to K, x \mapsto x^p$ は体準同型なので単射である．よって

$$|\mathrm{Frob}_p(K)| = |K|,\ \mathrm{Frob}_p(K) \subset K$$

であり $|K| < \infty$ なので $\mathrm{Frob}_p(K) = K$．つまり Frob_p は全射．よって $K^{p^{-1}} = K$ であるから **Prop 5.6** により K は完全体． ■

Def 5.6
K は $\mathrm{ch}\, K = p > 0$ なる体，L/K を体拡大とする．

$$\forall \alpha \in L, \exists n \geq 0, \alpha^{p^n} \in K$$

を充たすとき，L/K を**純非分離拡大** (**purely inseparable extension**) という．また K/K も純非分離拡大であるとする．[†10]

Prop 5.7
L/K は体拡大，$\mathrm{ch}\, K = p > 0$ とする．次は同値．

(1) L/K は純非分離拡大
(2) 任意の $\alpha \in L \setminus K$ は K 上分離的

Proof. (1) ⇒ (2) **Prop 5.5** より従う．
(2) ⇒ (1) $\alpha \in L \setminus K, p(T)$ を α の K 上最小多項式とする．$p(T)$ は非分離多項式なので，

$$\exists g(T) \in K[T] : K\text{上既約分離}, \exists n > 0, p(T) = g(T^{p^n})$$

$\alpha^{p^n} \in L$ は $g(T)$ の根なので，$\deg g(T) > 1$ と仮定すると $L \setminus K$ が K 上分離的な元を含み (2) に矛盾．よって $\deg g(T) = 1$ で $\exists \beta \in K, g(T) = T - \beta$ とすると，$\alpha^{p^n} = \beta \in K$． ■

5.3　分離次数

Def 5.7
L/K を有限次拡大とする．$[L : K]_{\mathrm{sep}} := |\mathrm{Hom}^{\mathrm{al}}_K(L, \overline{K})|$ を**分離次数** (**separable degree**) という. また, $[L : K]_{\mathrm{ins}} := \dfrac{[L : K]}{[L : K]_{\mathrm{sep}}}$ を**非分離次数** (**inseparable degree**) という. [†11]

Remark 5.4. 分離次数 $[L : K]_{\mathrm{sep}}$ は以下の可換図式における φ の本数.

[†10] K/K は分離拡大なので純非分離拡大は非分離拡大とは限らない.
[†11] 包含 $\iota : L \hookrightarrow \overline{K}$ は K 準同型なので $[L : K]_{\mathrm{sep}} \geq 1$ であり，$[L : K]_{\mathrm{ins}}$ は定義される.

$$\begin{tikzcd} L \arrow[r, "\varphi"] & \overline{K} \\ K \arrow[u, "\iota_{K,L}"] \arrow[ur, "\iota_{K,\overline{K}}"'] \arrow[u, phantom, "\circlearrowleft", shift left=6] \end{tikzcd}$$

以降この分離次数について考察しよう．

Prop 5.8

$K(\alpha)/K$ が代数拡大のとき，

$$[K(\alpha) : K]_{\mathrm{sep}} \leq [K(\alpha) : K]$$

さらに，

$$\alpha \text{ が } K \text{ 上分離的} \Leftrightarrow [K(\alpha) : K]_{\mathrm{sep}} = [K(\alpha) : K]$$
$$\alpha \text{ が } K \text{ 上非分離的} \Leftrightarrow [K(\alpha) : K]_{\mathrm{sep}} < [K(\alpha) : K]$$

Proof. $p(T) \in K[T]$ を α の K 上最小多項式とし，$n := \deg p(T)$ とする．

$$p(T) = (T - \alpha_1) \cdots (T - \alpha_n) \ (\alpha_i \in \overline{K})$$

とする．**Prop 4.3** より，各 $i \in \{1, \cdots, n\}$ に対し，$\varphi_i \in \mathrm{Hom}^{\mathrm{al}}_K(K(\alpha), \overline{K})$ を $\varphi_i(\alpha) = \alpha_i$ を充たすものとして定義できる．

一方 $\varphi \in \mathrm{Hom}^{\mathrm{al}}_K(K(\alpha), \overline{K})$ に対し，

$$p(\varphi(\alpha)) = \varphi(p)(\varphi(\alpha)) = \varphi(p(\alpha)) = \varphi(0) = 0$$

より $\exists i \in \{1, \cdots, n\}, \varphi = \varphi_i$ である．従って $\mathrm{Hom}^{\mathrm{al}}_K(K(\alpha), \overline{K}) = \{\varphi_1, \cdots, \varphi_n\}$．

$$\therefore |\mathrm{Hom}^{\mathrm{al}}_K(K(\alpha), \overline{K})| \leq n = \deg p(T) = [K(\alpha) : K]$$

さらに，

$$\begin{aligned} \alpha \text{ が } K \text{ 上分離的} &\Leftrightarrow p(T) \text{ は分離多項式} \\ &\Leftrightarrow \alpha_1, \cdots, \alpha_n \text{ は相異なる．} \\ &\Leftrightarrow \varphi_1, \cdots, \varphi_n \text{ は相異なる．} \\ &\Leftrightarrow |\mathrm{Hom}^{\mathrm{al}}_K(K(\alpha), \overline{K})| = n = [K(\alpha) : K] \end{aligned}$$

また，α が分離的であることと，α が非分離的であることは排反かつ全ての場合を尽くすので，

$$\alpha \text{ が } K \text{ 上非分離的} \Leftrightarrow \ [K(\alpha) : K]_{\mathrm{sep}} < [K(\alpha) : K]$$

もいえる． ■

Remark 5.5. この証明から $[K(\alpha):K]_{\mathrm{sep}}$ は α の K 上共軛の個数であることがわかる. 分離拡大では α の最小多項式において共軛はダブりなくカウントされ $[K(\alpha):K]_{\mathrm{sep}} = [K(\alpha):K]$ となる.

Prop 5.9
有限次拡大 $L/M/K$ に対し,

$$[L:K]_{\mathrm{sep}} = [L:M]_{\mathrm{sep}}[M:K]_{\mathrm{sep}}, \quad [L:K]_{\mathrm{ins}} = [L:M]_{\mathrm{ins}}[M:K]_{\mathrm{ins}}$$

Proof. **Thm 4.3** から, $\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(M,\overline{K})$ に対し, 拡張となる K 同型

$$\overline{\varphi} : \overline{M} \xrightarrow{\cong} \overline{K}$$

が存在する. ここで M/K は代数拡大であるから $\overline{M} = \overline{K}$ なので, $\overline{\varphi} \in \mathrm{Aut}_K^{\mathrm{al}}\overline{K}$ である. 各 $\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(M,\overline{K})$ に対し $\overline{\varphi}$ を 1 つ選択しておき, 写像 Φ を次で定める.

$$\begin{aligned}\Phi : \mathrm{Hom}_K^{\mathrm{al}}(M,\overline{K}) \times \mathrm{Hom}_M^{\mathrm{al}}(L,\overline{K}) &\to \mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K}) \\ (\varphi,\psi) &\mapsto \overline{\varphi}\circ\psi\end{aligned}$$

このとき, Φ は全単射となる. 実際,

$$\begin{aligned}\Psi : \mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K}) &\to \mathrm{Hom}_K^{\mathrm{al}}(M,\overline{K}) \times \mathrm{Hom}_M^{\mathrm{al}}(L,\overline{K}) \\ \varphi &\mapsto (\varphi|_M, (\overline{\varphi|_M})^{-1}\circ\varphi)\end{aligned}$$

とすると, $\Phi = \Psi^{-1}$ である. よって,

$$|\mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K})| = |\mathrm{Hom}_K^{\mathrm{al}}(M,\overline{K})||\mathrm{Hom}_M^{\mathrm{al}}(L,\overline{K})|$$

を得る. また,

$$[L:K]_{\mathrm{ins}} = \frac{[L:K]}{[L:K]_{\mathrm{sep}}} = \frac{[L:M][M:K]}{[L:M]_{\mathrm{sep}}[L:M]_{\mathrm{sep}}} = [L:M]_{\mathrm{ins}}[M:K]_{\mathrm{ins}}$$

■

Thm 5.1
L/K を有限次拡大とする. このとき,

$$[L:K]_{\mathrm{sep}} \leq [L:K]$$

さらに,

$$L/K \text{ が分離拡大} \Leftrightarrow [L:K]_{\mathrm{sep}} = [L:K]$$

Proof. L/K は有限次拡大なので,

$$\exists \alpha_1, \cdots, \alpha_n \in L, L = K(\alpha_1, \cdots, \alpha_n)$$

このとき,

$$M_0 := M, M_i := M_{i-1}(\alpha_i)\ (1 \le i \le n)$$

とおく．各 $1 \le i \le n$ に対し，M_i/M_{i-1} は代数拡大であるから **Prop 5.8** から

$$[M_i : M_{i-1}]_{\mathrm{sep}} \le [M_i : M_{i-1}]$$

Prop 5.9 を繰り返して,

$$\begin{aligned} [L:K]_{\mathrm{sep}} &= [M_n : M_0]_{\mathrm{sep}} = [M_n : M_{n-1}]_{\mathrm{sep}} \cdots [M_1 : M_0]_{\mathrm{sep}} \\ &\le [M_n : M_{n-1}] \cdots [M_1 : M_0] = [M_n : M_0] = [L : K] \end{aligned} \tag{$*$}$$

($\Rightarrow$) L/K が有限次分離拡大のときは各 i に対し $[M_i : M_{i-1}]_{\mathrm{sep}} = [M_i : M_{i-1}]$ なので ($*$) において $\le$ が $=$ になる．
($\Leftarrow$) $[L:K]_{\mathrm{sep}} = [L:K]$ とする．$\alpha \in L$ に対して,

$$\begin{aligned} |\operatorname{Hom}_K^{\mathrm{al}}(L, \overline{K})| &= |\operatorname{Hom}_K^{\mathrm{al}}(K(\alpha), \overline{K})||\operatorname{Hom}_{K(\alpha)}^{\mathrm{al}}(L, \overline{K})| \\ &\le [L : K(\alpha)][K(\alpha) : K] = [L : K] = |\operatorname{Hom}_K^{\mathrm{al}}(L, \overline{K})| \end{aligned}$$

よって $|\operatorname{Hom}_K^{\mathrm{al}}(K(\alpha), \overline{K})| = [K(\alpha) : K]$ であるから，α は K 上分離的．従って，L/K は分離拡大. ■

Remark 5.6. **Prop 5.8** と **Thm 5.1** 後半より,

$$K(\alpha)/K \text{ が分離拡大} \Leftrightarrow \alpha \text{ が } K \text{ 上分離的}$$

Remark 5.7. L/K が有限次拡大であるとき，$[L:K]_{\mathrm{sep}} \le [L:K] < \infty$ であるから分離次数は有限値であることがわかる．

Prop 5.10 (分離拡大の推移律)
L/K を体拡大とする．

$$L/M, M/K \text{ が分離拡大} \Leftrightarrow L/K \text{ が分離拡大}$$

$$\begin{tikzcd} L \arrow[d, dash] \\ M \arrow[u, bend right, "\mathrm{sep}"'] \arrow[d, dash] \\ K \arrow[u, bend right, "\mathrm{sep}"'] \arrow[uu, bend left=60, "\mathrm{sep}"] \end{tikzcd}$$

Proof. ($\Leftarrow$) L/K が分離拡大なら $M \subset L$ の元は K 上分離的なので M/K は分離拡大．また，*Remark* 5.8．300 より L/M も分離拡大である．

($\Rightarrow$) まず $[L:K] < \infty$ の場合，**Prop 5.9** と **Prop 5.1** 後半より，

$$[L:K]_{\mathrm{sep}} = [L:M]_{\mathrm{sep}}[M:K]_{\mathrm{sep}} = [L:M][M:K] = [L:K]$$

従って，**Prop 5.1** より L/K は分離拡大．

一般の場合も有限次拡大に帰着できる．$\alpha \in L$ とする．α の M 上最小多項式を $p(T) = T^n + a_1T^{n-1} + \cdots + a_n$，$F_1 = K(a_1, \cdots, a_n), F_2 = F_1(\alpha)$ とする．このとき，α の F_1 上最小多項式は $p(T)$ であることに注意したい．また，$F_2/F_1, F_1/K$ は有限次拡大なので F_2/K も有限次拡大．

$$\begin{tikzcd}
L \arrow[d, dash] \\
F_2 \arrow[d, dash] \\
M \arrow[uu, bend left, "\mathrm{sep}"] \arrow[d, dash] \\
F_1 \arrow[uu, bend right, "\mathrm{sep}"'] \arrow[d, dash] \\
K \arrow[uu, bend left, "\mathrm{sep}"] \arrow[u, bend right, "\mathrm{sep}"']
\end{tikzcd}$$

M/K は分離拡大かつ $F_1 \subset M$ であるから F_1/K は分離拡大．また L/M は分離拡大なので $p(T)$ は分離的であるから α は F_1 上分離的である．よって *Remark* 5.6 より F_2/F_1 は分離拡大．

従って有限次の場合より F_2/K は分離拡大で，α は K 上分離的である．■

Cor 5.3

$K(\alpha_1, \cdots, \alpha_n)/K$ を有限次拡大とする．$\alpha_1, \cdots, \alpha_n$ が K 上分離的なら $K(\alpha_1, \cdots, \alpha_n)/K$ は分離拡大である．

Proof.

$$M_0 := K, M_i := M_{i-1}(\alpha_i)\ (1 \leq i \leq n)$$

とおく．各 $1 \leq i \leq n$ に対し，M_i/M_{i-1} は代数拡大であるから **Prop 5.8** から *Remark* 5.1 と *Remark* 5.6 とより M_i/M_{i-1} は分離拡大．よって **Prop 5.10** から $K(\alpha_1, \cdots, \alpha_n)/K$ は分離拡大．■

5.4　分離閉包

Def 5.8
L/K を代数拡大とする.

$$L_s := \{\alpha \in L \mid \alpha \text{ is separable over } K\}$$

を L における K の**分離閉包 (separable closure)** という．また $K^{\mathrm{sep}} := (\overline{K})_s$ を K の分離閉包という.

Remark 5.9. $\alpha, \beta \in L_s$ とすると $K(\alpha,\beta)/K$ は分離拡大なので，$\alpha+\beta, \alpha\beta \in L_s, \alpha^{-1} \in L_s (\alpha \neq 0)$．よって L/L_s である．また当然 K の元は K 上分離的なので $L/L_s/K$.

$$\begin{tikzcd}
L \arrow[d, dash] \\
L_s \arrow[u, bend right, "\text{purely.insep.}"'] \arrow[d, dash] \\
K \arrow[uu, bend left=60, "\text{alg}"] \arrow[u, bend right, "\text{sep}"']
\end{tikzcd}
\qquad
\begin{tikzcd}
\overline{K} \arrow[d, dash] \\
K^{\mathrm{sep}} \arrow[u, bend right, "\text{purely.insep.}"'] \arrow[d, dash] \\
K \arrow[uu, bend left=60, "\text{alg}"] \arrow[u, bend right, "\text{sep}"']
\end{tikzcd}$$

Remark 5.10. K が完全体 $\Leftrightarrow$ $K^{\mathrm{sep}} = \overline{K}$

Prop 5.11
Def 5.8 の状況で L/L_s は純非分離拡大である.

Proof. $\mathrm{ch}\, K = 0$ なら $L_s = L$ より明白．$\mathrm{ch}\, K = p > 0, \alpha \in L$ なら，**Prop 5.4** より，

$$\exists g(T) \in K[T] : K\text{上既約分離}, \exists n \geq 0, g(\alpha^{p^n}) = 0$$

よって $\alpha^{p^n} \in L_s$ なので，L/L_s は純非分離拡大である. ■

Prop 5.12
L/K を有限次拡大とする.

(1) F/K が純非分離拡大なら $\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ に対し，延長 $\widetilde{\varphi} \in \mathrm{Hom}_K^{\mathrm{al}}(F, \overline{K})$ が unique に存在する.

(2) $[L_s : K] = [L : K]_{\mathrm{sep}}$

(3) $[L : L_s] = [L : K]_{\mathrm{ins}}$

Proof. (1) **Thm 4.3** より延長 $\widetilde{\varphi}$ が存在する．一意性を示す．$F = L$ なら明白．$F \neq L$ とする．このとき $\mathrm{ch}\, F = p > 0$ なので，$\alpha \in F$ とすると，$\exists q \in \{p^n \mid n \geq 0\}, \alpha^q =: \beta \in L$.

よって $\varphi(\alpha)^q=\varphi(\beta)$．方程式 $T^q=\varphi(\beta)$ の解は 1 つのみなので，$\varphi(\alpha)$ は $\varphi(\beta)$ により定まり，延長は unique である．

(2) L_s/K は有限次分離拡大なので，$[L_s:K]=[L_s:K]_{\mathrm{sep}}$．(1) より $\mathrm{Hom}^{\mathrm{al}}_K(L_s,\overline{K})$ の元は $\mathrm{Hom}^{\mathrm{al}}_K(L_s,\overline{K})$ の元に unique に延長されるので，$[L_s:K]_{\mathrm{sep}}=[L:K]_{\mathrm{sep}}$．従って $[L_s:K]=[L:K]_{\mathrm{sep}}$．

(3) (2) より，

$$[L:L_s]=\frac{[L:K]}{[L_s:K]}=\frac{[L:K]}{[L:K]_{\mathrm{sep}}}=[L:K]_{\mathrm{ins}}$$

■

5.5　原始元定理

Thm 5.2 (**原始元定理**)
有限次分離拡大は単拡大である．このときの生成元を**原始元** (**primitive element**) という．

Proof. L/K を有限次分離拡大とする．

まず $|K|<\infty$ の場合，$|L|<\infty$ である．$L^\times$ は巡回群なので $\exists\gamma\in L, L^\times=\langle\gamma\rangle$．このとき，$L=K(\gamma)$．

$|L|=\infty$ の場合を次の 2 つの Steps に分けて示す．

Step 1　L/K を有限次分離拡大，$\alpha\in L$ とする．

$$\forall\varphi,\psi\in\mathrm{Hom}^{\mathrm{al}}_K(L,\overline{K})\ \ [\varphi\neq\psi\Rightarrow\varphi(\gamma)\neq\psi(\gamma)]$$

が成り立つとき，$L=K(\gamma)$．

$\gamma\in L$ は条件を充たすとすると，$|\mathrm{Hom}^{\mathrm{al}}_K(L,\overline{K})|\leq|\mathrm{Hom}^{\mathrm{al}}_K(K(\gamma),\overline{K})|$ であるから，

$$[L:K]=[L:K]_{\mathrm{sep}}\leq[K(\gamma):K]_{\mathrm{sep}}\leq[K(\gamma):K]$$

より，$L=K(\gamma)$ である．

Step 2　$|K|=\infty$ のとき，Step 1 の γ は存在する．

$[L:K]=n$ とすると，

$$\exists\alpha_1,\cdots,\alpha_n\in L, L=K(\alpha_1,\cdots,\alpha_n)$$

であるが，$L=K(\alpha,\beta)$ の場合に

$$\exists\gamma\in L, K(\gamma)=K(\alpha,\beta)$$

を示せば帰納的に示される．$\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}) = \{\varphi_1, \cdots, \varphi_n\}$ とすると，L/K は分離拡大なので，$\varphi_1, \cdots, \varphi_n$ は全て異なる．

$$f(T) := \prod_{i \neq j} ((\varphi_i(\alpha) + \varphi_i(\beta)T) - (\varphi_j(\alpha) + \varphi_j(\beta)T)) \in \overline{K}[T]$$

とおく．このとき，$f(T)$ は零多項式ではない．

> $(\because)$ $f(T) = 0$ とすると，$i \neq j$ が存在して，
>
> $$\begin{aligned} &(\varphi_i(\alpha) + \varphi_i(\beta)T) - (\varphi_j(\alpha) + \varphi_j(\beta)T) = 0 \\ \Leftrightarrow &(\varphi_i(\alpha) - \varphi_j(\alpha)) + (\varphi_i(\beta) - \varphi_j(\beta))T = 0 \\ \Leftrightarrow &\varphi_i(\alpha) - \varphi_j(\alpha) = \varphi_i(\beta) - \varphi_j(\beta) = 0 \end{aligned}$$
>
> $$\therefore \varphi_i(\alpha) = \varphi_j(\alpha),\ \varphi_i(\beta) = \varphi_j(\beta)$$
>
> $L = K(\alpha, \beta)$ より，$\varphi_i = \varphi_j$ を得る．これは $i \neq j \Rightarrow \varphi_i \neq \varphi_j$ に矛盾．

零でない多項式の根は有限個であり，$|K| = \infty$ なので，$f(c) \neq 0$ なる $c \in K$ が取れる．このとき，$\gamma := \alpha + c\beta$ とすれば，$i \neq j$ のとき，

$$\varphi_i(\gamma) = \varphi_i(\alpha) + c\varphi_i(\beta) \neq \varphi_j(\alpha) + c\varphi_j(\beta) = \varphi_j(\gamma)$$

よって，

$$\varphi_i \neq \varphi_j \Rightarrow \varphi_i(\gamma) \neq \varphi_j(\gamma)$$

以上より，$K(\alpha, \beta) = K(\gamma)$ ■

Example 5.5. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

6 Galois 拡大

6.1 正規拡大

Def 6.1

L/K を代数拡大とする．任意の $\alpha \in L$ に対して α の K 上最小多項式 $p(T)$ が L 上で 1 次式の積に分解できるとき，L/K を**正規拡大** (**normal extension**) という．

Remark 6.1. L/K が正規拡大とは，任意の $\alpha \in L$ に対し，α の K 上共軛が全て L に属すること，と言い換えられる．

Example 6.1. $\mu(d) = 0$ とする．[†12] $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ は正規拡大．実際，$\sqrt{d}$ の $\mathbb{Q}$ 上最小多項式は $T^2 - d$ であり，$\mathbb{Q}$ 上共軛 $\pm\sqrt{d}$ は $\mathbb{Q}(\sqrt{d})$ に属する．

Example 6.2. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ は正規拡大でない．実際，$\sqrt[3]{2}$ の $\mathbb{Q}$ 上最小多項式は $T^3 - 2$ であり，$\sqrt[3]{2}\omega \notin \mathbb{Q}(\sqrt[3]{2})$ を $\mathbb{Q}$ 上共軛に持つ．

Prop 6.1

L/K を有限次拡大とする．このとき (1),(2) は同値

(1) L/K は正規拡大

(2) $\forall \varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}), \varphi(L) \subset L$

Proof. (1)⇒(2) $\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}), \alpha \in L$ とする．$\varphi(\alpha)$ は α の K 上の共軛であるから仮定より $\varphi(\alpha) \in L$．よって $\varphi(L) \subset L$

(2)⇒(1) $\alpha \in L$ とし，$\beta \in \overline{K}$ を α の K 上の共軛とする．このとき，Prop より

$$\exists \varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}), \varphi(\alpha) = \beta$$

仮定 $\varphi(L) \subset L$ より $\beta \in L$．よって L/K は正規拡大． ■

Cor 6.1

L/K を代数拡大，$L = K(\alpha_1 \cdots, \alpha_n)$ とする．$\alpha_1 \cdots, \alpha_n$ の K 上の共軛が全て L に属するとき，L/K は正規拡大である．

Proof. $\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ とすると，仮定より $\varphi(\alpha_1), \cdots, \varphi(\alpha_1) \in L$．$K$ 準同型は K 上の生成元で決定され，$\varphi(L) = K(\varphi(\alpha_1), \cdots, \varphi(\alpha_1)) \subset L$ が従う．**Prop 6.1** より L/K は正規拡大である． ■

[†12] μ は Möbius 関数.

Def 6.2
L/K を代数拡大とするとき，L を包む K の最小の正規拡大体を L の K 上の**正規閉包 (normal closure)** といい，$\mathrm{NC}_K(L)$ で表す．

Remark 6.2. 正規閉包 $\mathrm{NC}_K(L)$ は（$\overline{K}$ において）L の全ての元の全ての K 上共軛を L に添加して得られる．

Prop 6.2
$L = K(\alpha_1, \cdots, \alpha_n)$ のとき，$\mathrm{NC}_K(L)$ は $\alpha_1, \cdots, \alpha_n$ の全ての K 上共軛を L に添加して得られる．

Proof. F を $\alpha_1, \cdots, \alpha_n$ の全ての K 上共軛を L に添加した体とすると，**Cor 6.1** により，F/K は正規拡大．よって $\mathrm{NC}_K(L)$ の定義から，$\mathrm{NC}_K(L) \subset F$．また，$F \subset \mathrm{NC}_K(L)$ は明白なので $\mathrm{NC}_K(L) = F$． ■

Example 6.3. $L = \mathbb{Q}(\sqrt[3]{2})$ とすると，L の $\mathbb{Q}$ 上の正規閉包は

$$\mathrm{NC}_K(L) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

Prop 6.3
$L_1/K, L_2/K$ を代数拡大とする．次は同値．

(1) L_1 と L_2 は K 同型
(2) $\exists \sigma \in \mathrm{Aut}_K^{\mathrm{al}}(\overline{K}), \sigma(L_1) = L_2$
(3) $\exists \varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L_1, \overline{K}), \varphi(L_1) = L_2$

このとき，L_1 と L_2 は K 上の**共軛体 (conjugate field)** という．

Proof. (1)⇒(2) $\sigma_0 : L_1 \to L_2$ を K 同型とすると，**Thm 4.3** より σ_0 の拡張 $\sigma \in \mathrm{Aut}_K^{\mathrm{al}}(\overline{K})$ があって，$\sigma(L_1) = L_2$．
(2)⇒(3) $\varphi := \sigma|_{L_1}$ とすればよい．
(3)⇒(1) φ の終域を L_2 に設定し直せばよい． ■

Example 6.4. $\mathbb{Q}(\sqrt[3]{2}, \omega)$ の中間体 $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2)$ はそれぞれ $\mathbb{Q}$ 上の共軛体である．例えば，$\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\omega), \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$ としたとき，$\mathbb{Q}(\sqrt[3]{2}\omega) = \sigma(\mathbb{Q}(\sqrt[3]{2}))$ である．

Remark 6.3. L/K が正規拡大 ⇔ L の K 上の共軛体は L 自身のみ

6.2　Galois 拡大

Def 6.3
代数拡大 L/K が分離拡大かつ正規拡大であるとき，L/K は **Galois 拡大** (**Galois extension**) という．このとき，

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_K^{\mathrm{al}}(L)$$

を L/K の **Galois 群** (**Galois group**) という．
$\mathrm{Gal}(L/K)$ が Abel 群であるとき，L/K を **Abel 拡大** (**abelian extension**) という．
$\mathrm{Gal}(L/K)$ が巡回群であるとき，L/K を**巡回拡大** (**cyclic extension**) という．

Example 6.5. $\mu(d) = 0$ とする．$\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ は 2 次 Galois 拡大であり，$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong C_2$ なので特に巡回拡大．また，$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \cdots)/\mathbb{Q}$ は無限次の Galois 拡大．

Example 6.6. $\mathbb{F}_p(\sqrt[p]{X})/\mathbb{F}_p(X)$ は正規だが分離でないので Galois 拡大でない．実際，$\sqrt[p]{X}$ の $\mathbb{F}_p(X)$ 上最小多項式は $T^p - X = (T - \sqrt[p]{X})^p$ であるから，分離拡大ではない．しかし，$\mathbb{F}_p(X)$ 上共軛は $\sqrt[p]{X}$ のみであるから **Cor 6.1** より正規拡大.

Remark 6.4. 体 K に対し，K^{sep}/K は Galois 拡大である．Galois 群

$$G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$$

を K の**絶対 Galois 群** (**absolute Galois group**) という．

Def 6.4
K を体とする．$K^{\mathrm{sep}}/L/K$ なる L に対し，$\widetilde{L} := \mathrm{NC}_K(L)$ は K の Galois 拡大体であり，これを L の K 上の **Galois 閉包** (**Galois closure**) という．

以降では主に有限次 Galois 拡大について考える．

Prop 6.4
L/K は有限次拡大とする．

(1) $\mathrm{Hom}_K^{\mathrm{al}}(L, L) = \mathrm{Aut}_K^{\mathrm{al}}(L)$
(2) L/K が分離拡大のとき，$|\mathrm{Aut}_K^{\mathrm{al}}(L)| \le [L : K]$

Proof. (1) $(\supset)$ は明白．$\sigma \in \mathrm{Hom}_K^{\mathrm{al}}(L, L)$ とすると，σ は単射．よって σ は同次元の有限次 K 線型空間の間の単射線型写像なので同型である．

(2) $\mathrm{Aut}_K^{\mathrm{al}}(L) = \mathrm{Hom}_K^{\mathrm{al}}(L, L) \subset \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ であり，L/K が有限次分離拡大なら，

$$|\mathrm{Aut}_K^{\mathrm{al}}(L)| \leq |\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})| = [L : K]$$

■

Example 6.7. $\mathbb{Q}(T)/\mathbb{Q}$ は無限次拡大である．$\varphi \in \mathrm{Hom}_{\mathbb{Q}}^{\mathrm{al}}(\mathbb{Q}(T), \mathbb{Q}(T))$ を $T \mapsto T^2$ で定めると，これは全射でないので $\varphi \notin \mathrm{Aut}_{\mathbb{Q}}^{\mathrm{al}}(\mathbb{Q}(T))$．よって $\mathrm{Hom}_{\mathbb{Q}}^{\mathrm{al}}(\mathbb{Q}(T), \mathbb{Q}(T)) \supsetneq \mathrm{Aut}_{\mathbb{Q}}^{\mathrm{al}}(\mathbb{Q}(T))$.

Prop 6.5

L/K を有限次分離拡大のとき，以下は同値.

(1) L/K が Galois 拡大
(2) $\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}) = \mathrm{Aut}_K^{\mathrm{al}}(L)$
(3) $|\mathrm{Aut}_K^{\mathrm{al}}(L)| = [L : K]$

特に，有限次 Galois 拡大 L/K に対し，

$$\mathrm{Gal}(L/K) = \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}),\ |\mathrm{Gal}(L/K)| = [L : K]$$

である.

Proof. (1)⇒(2) ($\supset$) は明らか．$\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ とすると，L/K は正規拡大なので，$\varphi(L) \subset L$．よって $\varphi \in \mathrm{Hom}_K^{\mathrm{al}}(L, L) = \mathrm{Aut}_K^{\mathrm{al}}(L)$ であり，$\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}) \subset \mathrm{Aut}_K^{\mathrm{al}}(L)$.
(2)⇒(1) $\alpha \in L$ とし，$\beta \in \overline{K}$ をその K 上の共軛とする．このとき，K 同型 $\varphi : K(\alpha) \to K(\beta)$ が存在する．**Prop 5.1**(1) より，φ は $\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ の元へ延長できるが，$\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K}) = \mathrm{Aut}_K^{\mathrm{al}}(L)$ なので，$\beta \in K(\beta) \subset L$．よって L/K は正規拡大であり，Galois 拡大である.
(2)⇔(3) **Prop 6.4**(2) と **Prop 5.1**(2) より，

$$|\mathrm{Aut}_K^{\mathrm{al}}(L)| = [L : K] \ \Leftrightarrow\ \mathrm{Aut}_K^{\mathrm{al}}(L) = \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$$

■

Cor 6.2

L/K が有限次 Galois 拡大，$L/M/K$ のとき，L/M も Galois 拡大であり，

$$\mathrm{Gal}(L/M) \geq \mathrm{Gal}(L/K)$$

$$\begin{tikzcd} L \arrow[d, dash] \\ M \arrow[d, dash] \arrow[u, bend right=60, "\text{fin.Gal}"'] \\ K \arrow[uu, bend left=60, "\text{fin.Gal}"] \end{tikzcd}$$

Proof. *Remark* 5.1 より，L/M は分離拡大．$L = K(\alpha_1 \cdots, \alpha_n)$ とすると，L は $\alpha_1 \cdots, \alpha_n$ の K 上共軛を全て含む．$\alpha_1 \cdots, \alpha_n$ の M 上共軛は K 上共軛でもあるので，**Cor 6.1** により，L/M は正規拡大．よって L/M も Galois 拡大.

また，$K \subset M$ なので，$\sigma \in \mathrm{Gal}(L/M)$ は K の元を動かさない．よって $\sigma \in \mathrm{Gal}(L/K)$ で，$\mathrm{Gal}(L/M) \geq \mathrm{Gal}(L/K)$ が従う． ■

Prop 6.6

L/K を有限次拡大とする．以下は同値.

(1) L/K は Galois 拡大

(2) L はある分離多項式 $f(T) \in K[T]$ の最小分解体

Proof. (1)⇒(2) L/K は有限次分離拡大であるから，$\exists \alpha \in L, L = K(\alpha)$

$p(T)$ を α の K 上最小多項式とすると，これは分離多項式である．

$$\exists \alpha_i \in \overline{K},\ p(T) = (T-\alpha)(T-\alpha_2)\cdots(T-\alpha_n)$$

L/K が正規拡大であることから，$K(\alpha, \alpha_2, \cdots, \alpha_n) \subset L = K(\alpha)$．また，逆の包含は明らかなので，$K(\alpha, \alpha_2, \cdots, \alpha_n) = L$ であり，L は $p(T)$ の最小分解体.

(2)⇒(1) L は分離多項式 $f(T) = (T-\alpha_1)\cdots(T-\alpha_n) \in K[T]$ の最小分解体とすると，$L = K(\alpha_1, \cdots, \alpha_n)$ である．$\alpha_1, \cdots, \alpha_n$ は K 上分離的である．

> ($\because$) $p_i(T)$ を α_i の K 上最小多項式とすると，$p_i(T) | f(T)$．$f(T)$ は分離多項式なので $p_i(T)$ も分離多項式.

よって L/K は分離拡大である．また，α_i の K 上共軛はある $\alpha_j \in L$ なので **Cor 6.1** により，L/K は正規拡大でもある．よって L/K は Galois 拡大. ■

7 Galois の基本定理

7.1 Galois 群の作用

Def 7.1
X を集合，$\mathfrak{S}(X)$ を X 上の対称群，G を群とする．群準同型 $\rho : G \to \mathfrak{S}(X)$ が存在するとき，G は X に**作用する** (**act**) といい $G \curvearrowright X$ とかく．このとき，

$$a_\rho : G \times X \to X,\ (g, x) \mapsto \rho(g)(x)$$

を G の X への**作用** (**action**)，ρ を G の**置換表現** (**permutation representation**) という．また G を**変換群** (**transformation group**)，X を G **空間** (G-**space**) という．$x \in X, g \in G$ に対し，ρ を省略して $\rho(g)(x)$ を gx と表すことが多い．
$x \in X$ に対し，

(a1) $\mathrm{Orb}_G(x) := \{gx \in X \mid g \in G\}$ を x の G **軌道** (G-**orbit**) という．
(a2) $\mathrm{Stab}_G(x) := \{g \in G \mid gx = x\} \leq G$ を x の**固定化部分群** (**stabilizer**) という．
(a3) $\mathrm{Orb}_G(x) = \{x\}$ となるとき，x を**固定点** (**fixed point**) という．固定点全体を**固定点集合** (**fixed point set**) といい，X^G で表す．

(b1) $\exists x \in X, \mathrm{Orb}_G(x) = X$ となるとき，$G \curvearrowright X$ は**推移的** (**transitive**) であるという．
(b2) $\forall x \in X, \mathrm{Stab}_G(x) = \{1\}$ となるとき，$G \curvearrowright X$ は**自由** (**free**) であるという．
(b3) $G \curvearrowright X$ が推移的かつ自由であるとき**正則** (**reguler**) であるという．
(b4) ρ が単射のとき，$G \curvearrowright X$ は**忠実** (**faithful**) であるという．[†13]

Remark 7.1. $G \curvearrowright X$ とする．$x, y \in X$ に対し，

$$x \sim y \ :\Leftrightarrow\ \exists g \in G, y = gx$$

と定める[†14]とこれは同値関係であり，$X/G := X/\sim$ を X の G による**軌道空間** (**orbit space**) という．G 軌道は軌道空間の元として定義することもできる．

Remark 7.2 (**Orbit-stabilizer theorem**). $G \curvearrowright X$ とする．$x \in X$ に対し，

$$G/\mathrm{Stab}_G(x) \to \mathrm{Orb}_G(x),\ g\,\mathrm{Stab}_G(x) \mapsto gx$$

[†13] $x \in X$ が固定点 $\Leftrightarrow$ $\mathrm{Stab}_G(x) = G$ $\Leftrightarrow$ $\forall g \in G, gx = x$
$G \curvearrowright X$ が推移的 $\Leftrightarrow$ $\forall x, y \in X, \exists g \in G, y = gx$
$G \curvearrowright X$ が正則 $\Leftrightarrow$ $\forall x, y \in X, \exists! g \in G, y = gx$
$G \curvearrowright X$ が忠実 $\Leftrightarrow$ $(\rho(g) = \mathrm{id}_X \Rightarrow g = 1)$

[†14] $x \sim y \ :\Leftrightarrow\ \exists g \in G, y = gx \ \Leftrightarrow\ y \in \mathrm{Orb}_G(x) \ \Leftrightarrow\ \mathrm{Orb}_G(x) = \mathrm{Orb}_G(y) \ \Leftrightarrow\ \mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y) \neq \emptyset$

は well-defined な全単射である．[†15]特に，

$$(G : \mathrm{Stab}_G(x)) = |G|/|\mathrm{Stab}_G(x)| = |\mathrm{Orb}_G(x)|$$

Remark 7.3. 作用が自由なら忠実である．

> (∵) ρ による作用 $G \curvearrowright X$ は自由とする．
>
> $$\begin{aligned}\mathrm{Ker}\,\rho &= \{g \in G \mid \rho(g) = \mathrm{id}_X\} \\ &= \{g \in G \mid \forall x \in X, \rho(g)(x) = x\} \\ &= \{g \in G \mid \forall x \in X, g \in \mathrm{Stab}_G(x)\} \\ &= \{g \in G \mid \forall x \in X, g = 1\} = \{1\}\end{aligned}$$

Example 7.1. G を群とする．$L : G \to \mathfrak{S}(G), g \mapsto L_g$ を $L_g(h) = gh$ で定めると，L によって $G \curvearrowright G$．この作用は正則である．特に忠実であることから任意の群はある対称群に埋込み可能，すなわちある対称群の部分群に同型であることが従う．(**Cayley の定理**)

Example 7.2. G を群とする．$\mathrm{Ad} : G \to \mathfrak{S}(G), g \mapsto \mathrm{Ad}_g$ を $\mathrm{Ad}_g(h) = g^{-1}hg$ で定めると，Ad によって $G \curvearrowright G$．この作用を G 上の**共軛作用** (**conjugation**) という．[†16]

$\mathrm{Ker}\,\mathrm{Ad} = \{g \in G \mid \forall h \in G, g^{-1}hg = h\} = Z(G)$ より，Ad が忠実 $\Leftrightarrow$ $Z(G) = \{1\}$

$G \neq \{1\}$ なら $\mathrm{Orb}_G(1) = \{1\}$ より推移的でない．

$G \neq \{1\}$ なら $\mathrm{Stab}_G(1) = G$ より自由でない．

また固定点集合は

$$G^G = \{h \in G \mid \forall g \in G, g^{-1}hg = h\} = Z(G)$$

である．

> **Def 7.2**
>
> k, A を可換環，A を k 代数，G を群とする．群準同型 $\rho : G \to \mathrm{Aut}_k^{\mathrm{al}} A$ が存在するとき，G は A に k **上作用する** (**act over** k) という．[†17]

Remark 7.4. 任意の可換環 A は $\mathbb{Z}$ 代数なので群準同型 $\rho : G \to \mathrm{Aut}^{\mathrm{al}}(A)$ は $\mathbb{Z}$ 上の作用．同様に，任意の体 L は素体 K 上の代数なので群準同型 $\rho : G \to \mathrm{Aut}^{\mathrm{al}}(L)$ は K 上の作用．

Example 7.3. L/K を体拡大とする．$\mathrm{id} : \mathrm{Aut}_K^{\mathrm{al}} L \to \mathrm{Aut}_K^{\mathrm{al}} L$ によって $\mathrm{Aut}_K^{\mathrm{al}}(L)$ は L に忠実に K 上作用する．特に L/K が Galois 拡大のとき，$\mathrm{Gal}(L/K) \curvearrowright L$ は忠実作用．

[†15] 一般に $\mathrm{Stab}_G(x) \not\trianglelefteq G$ なので $G/\mathrm{Stab}_G(x)$ は群ではない．

[†16] $\mathrm{Ad}_g : G \to G$ は同型であり，$\mathrm{Ad} : G \to \mathrm{Aut}(G)$ とできる．

[†17] $\mathrm{Aut}_K^{\mathrm{al}}(L) \leq \mathfrak{S}(L)$ なので k 上の作用は当然作用である．

Def 7.3
K を体，$f(T) \in K[T]$ を分離多項式とする．$f(T)$ の根を $\alpha_1, \cdots, \alpha_n \in \overline{K}$ とすると，$L = K(\alpha_1, \cdots, \alpha_n)$ は $f(T)$ の最小分解体である．このとき L/K は正規かつ分離なので Galois 拡大である．$\mathrm{Gal}(L/K)$ を $f(T)$ の Galois 群といい，$\mathrm{Gal}(f/K)$ で表す．

Remark 7.5. $\rho : \mathrm{Gal}(f/K) \to \mathfrak{S}(\{\alpha_1, \cdots, \alpha_n\}) \cong \mathfrak{S}_n$ を $\rho(\sigma) = \sigma|_{\{\alpha_1, \cdots, \alpha_n\}}$ によって定めると，$\mathrm{Gal}(f/K) \curvearrowright \{\alpha_1, \cdots, \alpha_n\}$ である．この作用は忠実なので

$$\mathrm{Gal}(f/K) \leq \mathfrak{S}(\{\alpha_1, \cdots, \alpha_n\}) \cong \mathfrak{S}_n$$

と見做せる．

Prop 7.1
Def 7.3 の状況において，次は同値．

(1) $f(T)$ は K 上既約
(2) 作用 $\mathrm{Gal}(f/K) \curvearrowright \{\alpha_1, \cdots, \alpha_n\}$ は推移的

Proof. (1) $\Rightarrow$ (2) **Prop 4.3** より従う．
(2) $\Rightarrow$ (1) α_1 の K 上最小多項式を $g(T)$ と, $g(T) \mid f(T)$ である. また $\sigma \in \mathrm{Gal}(f/K), \sigma(\alpha_1) = \alpha_i$ とすると **Prop 4.3** より α_i は α_1 の K 上共軛．推移的作用の仮定から $\alpha_1, \cdots, \alpha_n$ は α_1 の K 上共軛であるから，$f(T) \mid g(T)$．よって $\exists c \in K^\times$，$f(T) = cg(T)$ で $f(T)$ は K 上既約. ■

Example 7.4. $f(T) = (T^2 - 2)(T^2 - 3) \in \mathbb{Q}[T]$ とすると，$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ で，$\mathrm{Orb}_{\mathrm{Gal}(f/\mathbb{Q})}(\sqrt{2}) = \{\pm\sqrt{2}\}$ より $\mathrm{Gal}(f/\mathbb{Q}) \curvearrowright \{\pm\sqrt{2}, \pm\sqrt{3}\}$ は推移的でない.

Def 7.4
L を体，G を有限群とし，群準同型 $\rho : H \hookrightarrow \mathrm{Aut}^{\mathrm{al}}(L)$ によって忠実に $H \curvearrowright L$ とする．この作用の固定点集合

$$L^H := \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}$$

を H の**固定体** (**fixed field**) または**不変体**という．

Example 7.5. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}), H = \{\mathrm{id}_L, \sigma\} \leq \mathrm{Aut}^{\mathrm{al}}(L)$ とする．但し，σ は

$$\sigma(\sqrt{2}) = -\sqrt{2},\ \sigma(\sqrt{3}) = \sqrt{3}$$

で定まる $\mathbb{Q}$ 自己同型とする．このとき，$L^H = \mathbb{Q}(\sqrt{3})$.

Thm 7.1 (**Artin の定理**)
L/K を有限次 Galois 拡大，$H \leq \mathrm{Gal}(L/K)$ とすると，忠実に $H \curvearrowright L$ である．このとき L/L^H は Galois 拡大であり，

$$[L : L^H] = |H|,\ \mathrm{Gal}(L/L^H) = H$$

Proof. $L/L^H/K$ なので，**Cor 6.2** より，L/L^H も有限次 Galois 拡大．有限次分離拡大は単拡大なので，$\exists \alpha \in L, L = L^H(\alpha)$．ここで

$$f(T) = \prod_{\sigma \in H} (T - \sigma(\alpha)) \in L[T]$$

とする．$\tau \in \mathrm{Gal}(L/K)$ は自己準同型 $L[T] \to L[T], g(T) \to \tau(g)(T)$ を誘導する．

$$\tau(f)(T) = \prod_{\sigma \in H} (T - \tau(\sigma(\alpha)))$$

$\tau \in H$ のとき，$\tau H = H$ なので，$\tau(f)(T) = f(T)$．つまり $f(T)$ の係数は $\tau \in H$ で動かず，$f(T) \in L^H(T)$．$f(\alpha) = 0$ であり，$f(T)$ は $|H|$ 次多項式なので，$[L : L^H] \leq |H|$ である．また，$H \subset \mathrm{Gal}(L/L^H)$ に注意すれば，

$$|H| \leq |\mathrm{Gal}(L/L^H)| = [L : L^H] \leq |H|$$

よって結論を得る． ∎

Remark 7.6. 一般に体 L と有限部分群 $H \leq \mathrm{Aut}^{\mathrm{al}}(L)$ に対して成立する．

Def 7.5
L/K を有限次 Galois 拡大とする．$L/M/K$ に対して，

$$\Gamma(M) := \{\sigma \in \mathrm{Gal}(L/K) : \sigma|_M = \mathrm{id}_M\}$$

を M の**固定化部分群** (**stabilizer**) または**不変部分群** (**invariant subgroup**) という．[†18]

Remark 7.7. **Cor 6.2** より，L/M は Galois 拡大であり，$\Gamma(M) = \mathrm{Gal}(L/M)$

[†18] 作用 $G \curvearrowright X$ の固定化部分群を 1 点 $x \in X$ に対して定義したが，同様に $S \subset X$ に対しても

$$\mathrm{Stab}_G(S) := \{g \in G \mid \rho(g)|_S = \mathrm{id}_S\}$$

と定義できる．これを用いれば，$\mathrm{Gal}(L/K) \curvearrowright M$，$\Gamma(M) = \mathrm{Stab}_{\mathrm{Gal}(L/K)}(M)$ である．

7.2 Galois の基本定理

Thm 7.2 (**Galois の基本定理**)
L/K を有限次 Galois 拡大とする．

$$\mathcal{F} := \{M : L/M/K\},\ \mathcal{G} := \{H : H \leq \mathrm{Gal}(L/K)\}$$

とする．写像 Γ, Φ を，

$$\Gamma : \mathcal{F} \to \mathcal{G},\ M \mapsto \Gamma(M)$$
$$\Phi : \mathcal{G} \to \mathcal{F},\ H \mapsto L^H$$

により定める．このとき，

(1) $[L : M] = |\Gamma(M)|,\ [L : \Phi(H)] = |H|$
(2) Γ, Φ は互いに逆写像である．つまり，

$$\Phi \circ \Gamma = \mathrm{id}_{\mathcal{F}},\ \Gamma \circ \Phi = \mathrm{id}_{\mathcal{G}}$$

この対応 (Γ, Φ) を **Galois 対応** (**Galois correspondence**) という．
(3) $M_1, M_2 \in \mathcal{F}$ と $H_1, H_2 \in \mathcal{G}$ に対し，

$$M_1 \subset M_2 \Rightarrow \Gamma(M_1) \geq \Gamma(M_2)$$
$$H_1 \leq H_2 \Rightarrow \Phi(H_1) \supset \Phi(H_2)$$

$$\begin{tikzcd} L \arrow[r, dash, dashed] \arrow[d, dash] & \{1\} \arrow[d, dash] \\ M \arrow[r, "\Gamma"] \arrow[d, dash] & \Gamma(M) \arrow[d, dash] \\ K \arrow[r, dash, dashed] & \mathrm{Gal}(L/K) \end{tikzcd} \qquad \begin{tikzcd} L \arrow[r, dash, dashed] \arrow[d, dash] & \{1\} \arrow[d, dash] \\ L^H \arrow[d, dash] & H \arrow[l, "\Phi"'] \arrow[d, dash] \\ K \arrow[r, dash, dashed] & \mathrm{Gal}(L/K) \end{tikzcd}$$

Proof. (1) Artin の定理を書き直しただけである．

(2) (a) $\alpha \in M$ とすると，$\forall \sigma \in \Gamma(M), \sigma(\alpha) = \alpha$ なので，$\alpha \in \Phi(\Gamma(M))$．よって，$M \subset \Phi \circ \Gamma(M)$．さらに，

$$[L : M] = |\,\mathrm{Gal}(L/M)| \overset{\downarrow}{=} [L : L^{\mathrm{Gal}(L/M)}] = [L : \Phi \circ \Gamma(M)] \geq [L : M]$$

従って，$[L : M] = [L : \Phi \circ \Gamma(M)]$ であり，$\Phi \circ \Gamma(M) = M$

(b) $\sigma \in H$ とすると，$\forall \alpha \in \Phi(H), \sigma(\alpha) = \alpha$ なので，$\alpha \in \Gamma(\Phi(H))$．よって，$H \subset \Gamma \circ \Phi(H)$．さらに，

$$|H| \stackrel{\downarrow}{=} [L : L^H] = |\operatorname{Gal}(L/L^H)| = |\Gamma \circ \Phi(H)| \geq |H|$$

従って，$|H| = |\Gamma \circ \Phi(H)|$ であり，$\Gamma \circ \Phi(H) = H$．

但し，$\downarrow$ において Artin の定理（もしくは (1)）を用いた．

(3) **Cor 6.2** で $M = M_2, K = M_1$ として前半を得る．また，$\alpha \in \Phi(H_2)$ とすると，H_2 の元で固定される．$H_1 \subset H_2$ より α は H_1 の元でも固定されるので，$\alpha \in \Phi(H_1)$．よって $\Phi(H_1) \supset \Phi(H_2)$

■

Example 7.6. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ とすると $L/\mathbb{Q}$ は Galois 拡大である．$\sigma, \tau \in \operatorname{Gal}(L/\mathbb{Q})$ を，

$$\sigma(\sqrt{2}) = -\sqrt{2},\ \sigma(\sqrt{3}) = \sqrt{3}$$
$$\tau(\sqrt{2}) = \sqrt{2},\ \tau(\sqrt{3}) = -\sqrt{3}$$

で定まる $\mathbb{Q}$ 自己同型とする．このとき，

$$\sigma\tau(\sqrt{2}) = -\sqrt{2},\ \sigma\tau(\sqrt{3}) = -\sqrt{3}$$

である．$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$ から，$\operatorname{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ である．さらに $\sigma^2 = \tau^2 = 1, \sigma\tau = \tau\sigma$ であるから，

$$\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$$

Galois 対応は，

$$\begin{tikzcd}[column sep=small]
 & L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\sigma\rangle \arrow[dr, dash] & \langle\tau\rangle \arrow[d, dash] & \langle\sigma\tau\rangle \arrow[dl, dash] \\
 & \operatorname{Gal}(L/\mathbb{Q}) &
\end{tikzcd}$$

Remark 7.8. $(X, \preceq), (Y \preceq)$ を半順序集合とする．$\gamma : X \to Y, \varphi : Y \to X$ の組 (γ, φ) が次の条件を充たすとき，(γ, φ) を **Galois 系** (**Galois connection**) という．

(1) $x, y \in X, z, w \in Y$ に対し，

$$x \preceq y \ \Rightarrow\ \gamma(x) \succeq \gamma(y),\ z \preceq w \ \Rightarrow\ \varphi(z) \succeq \varphi(w)$$

(2) $x \in X, y \in y$ に対し，

$$x \preceq \varphi \circ \gamma(x), \quad y \preceq \gamma \circ \varphi(y)$$

Galois の基本定理から Galois 対応 (Γ, Φ) は Galois 系である．

Def 7.6

G を群とする．$H_1, H_2 \leq G$ が G における**共軛部分群** (**conjugate subgroup**) であるとは,

$$\exists \sigma \in G, H_2 = \sigma^{-1} H_1 \sigma$$

Example 7.7. $\mathfrak{S}_3$ の部分群 $\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$ はそれぞれ共軛部分群である．例えば, $\langle(1\ 3)\rangle = (2\ 3)^{-1}\langle(1\ 2)\rangle(2\ 3)$ である．

Prop 7.2

Thm 7.2 と同じ状況とする．$M_1, M_2 \in \mathcal{F}$ とする．次は同値.

(a1) M_1, M_2 は K 上の共軛体

(a2) $\mathrm{Gal}(L/M_1), \mathrm{Gal}(L/M_2)$ は $\mathrm{Gal}(L/K)$ における共軛部分群

特に，$M \in \mathcal{F}$ に対し，次は同値.

(b1) M/K が Galois 拡大

(b2) $\mathrm{Gal}(L/M) \trianglelefteq \mathrm{Gal}(L/K)$

このとき，$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$

Proof. (a1)⇔(a2) $\sigma \in \mathrm{Gal}(L/K)$ とする．このとき，

$$\begin{aligned}
\sigma(M_1) \subset M_2 &\Leftrightarrow \forall \alpha \in M_1, \sigma(\alpha) \in M_2 \\
&\Leftrightarrow \forall \alpha \in M_1, \forall \tau \in \mathrm{Gal}(L/M_2), \tau(\sigma(\alpha)) = \sigma(\alpha) \\
&\Leftrightarrow \forall \alpha \in M_1, \forall \tau \in \mathrm{Gal}(L/M_2), \sigma^{-1}\tau\sigma(\alpha) = \alpha \\
&\Leftrightarrow \forall \tau \in \mathrm{Gal}(L/M_2), \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M_1) \\
&\Leftrightarrow \sigma^{-1}\mathrm{Gal}(L/M_2)\sigma \subset \mathrm{Gal}(L/M_1)
\end{aligned}$$

また，$\sigma^{-1}(M_2) \subset M_1$ に置き換えれば,

$$(\sigma^{-1})^{-1}\mathrm{Gal}(L/M_1)\sigma^{-1} \subset \mathrm{Gal}(L/M_2) \text{ i.e. } \sigma^{-1}\mathrm{Gal}(L/M_2)\sigma \supset \mathrm{Gal}(L/M_1)$$

を得る．よって，$M_2 = \sigma(M_1) \iff \sigma^{-1}\mathrm{Gal}(L/M_2)\sigma = \mathrm{Gal}(L/M_1)$ である．

$$
\begin{tikzcd}[column sep=small]
 & L \arrow[rrrr, dash, dashed] \arrow[dl, dash] \arrow[dr, dash] & & & & \{1\} \arrow[dl, dash] \arrow[dr, dash] & \\
M_1 \arrow[rr, "\sigma"] \arrow[dr, dash] & & M_2 \arrow[dl, dash] & & \mathrm{Gal}(M_1/K) \arrow[rr, "\mathrm{Ad}_\sigma\ \dagger 19"] \arrow[dr, dash] & & \mathrm{Gal}(M_2/K) \arrow[dl, dash] \\
 & K \arrow[rrrr, dash, dashed] & & & & \mathrm{Gal}(L/K) &
\end{tikzcd}
$$

(b1)⇔(b2) $M \in \mathcal{F}$ に対し,

$$
\begin{aligned}
M/K \text{ は Galois 拡大} &\Leftrightarrow M \text{ の任意の共軛体が } M \\
&\Leftrightarrow \forall \sigma \in \mathrm{Gal}(L/K), \sigma(M) = M \\
&\Leftrightarrow \forall \sigma \in \mathrm{Gal}(L/K) = \sigma^{-1}\,\mathrm{Gal}(L/M)\sigma = \mathrm{Gal}(L/M) \\
&\Leftrightarrow \mathrm{Gal}(L/M) \trianglelefteq \mathrm{Gal}(L/K)
\end{aligned}
$$

このとき，制限を対応させる写像 $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K), \sigma \mapsto \sigma|_M$ は well-defined な全射準同型である．$\mathrm{Ker}\,\pi = \mathrm{Gal}(L/M)$ であるから,

$$
\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/M)
$$

を得る． ■

$$
\begin{tikzcd}
L \arrow[r, dash, dashed] \arrow[d, dash] & \{1\} \arrow[d, dash] \\
M \arrow[r, dash, dashed] \arrow[d, dash] & \mathrm{Gal}(M/K) \arrow[d, dash, "\trianglelefteq"] \\
K \arrow[r, dash, dashed] \arrow[u, bend left, "\mathrm{Gal.}"] & \mathrm{Gal}(L/K)
\end{tikzcd}
$$

Example 7.8. $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ とすると $L/\mathbb{Q}$ は Galois 拡大である．

$$
[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(T^2 + T + 1)\deg(T^3 - 2) = 2 \cdot 3 = 6
$$

であるから，*Remark* 7.5 より $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_3$ である．$\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ を,

$$
\sqrt[3]{2} \overset{\sigma}{\longmapsto} \sqrt[3]{2}\omega \overset{\sigma}{\longmapsto} \sqrt[3]{2},\ \ \sqrt[3]{2}\omega^2 \overset{\sigma}{\longmapsto} \sqrt[3]{2}\omega^2
$$

$$
\sqrt[3]{2} \overset{\tau}{\longmapsto} \sqrt[3]{2}\omega \overset{\tau}{\longmapsto} \sqrt[3]{2}\omega^2 \overset{\tau}{\longmapsto} \sqrt[3]{2}
$$

[†19] 群 G と $\sigma \in G$ に対し，Ad_σ は σ による共軛作用 $\mathrm{Ad}_\sigma : G \to G, \tau \mapsto \sigma^{-1}\tau\sigma$ を表す．

で定まる $\mathbb{Q}$ 自己同型とする．$(\alpha_1, \alpha_2, \alpha_3) := (\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ とし，群同型 ρ を

$$\rho : \mathrm{Gal}(f/K) \overset{\cong}{\to} \mathfrak{S}_n,\ \mu(\alpha_i) = \alpha_{\rho(\mu)(i)}$$

で定めれば，$\sigma \leftrightarrow (1\ 2)$, $\tau \leftrightarrow (1\ 2\ 3)$ と対応する．よって Galois 対応は,

$$\begin{tikzcd}
& L=\mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt[3]{2}\omega^2) & \mathbb{Q}(\sqrt[3]{2}) & \mathbb{Q}(\sqrt[3]{2}\omega) & \mathbb{Q}(\omega) \\
& \mathbb{Q} \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] \arrow[urr, dash] \arrow[urr, bend right, "\text{Gal.}"'] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle\sigma\rangle & \langle\sigma\tau\rangle & \langle\sigma\tau^2\rangle & \langle\tau\rangle \\
& \mathrm{Gal}(L/\mathbb{Q}) \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] \arrow[urr, dash, "\triangleleft"'] & &
\end{tikzcd}$$

ここで，$\langle(1\ \ 2)\rangle, \langle(2\ \ 3)\rangle, \langle(1\ \ 3)\rangle \leq \mathfrak{S}_3$ は共軛部分群，$\langle(1\ \ 2\ \ 3)\rangle \trianglelefteq \mathfrak{S}_3$ であるから，$\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2)$ は共軛体，$\mathbb{Q}(\omega)/\mathbb{Q}$ は Galois 拡大である．

7.3 Galois の推進定理

Thm 7.3 (**Galois の推進定理**)
L/K を体拡大とし，M, N をその中間体で $L = MN, K = M \cap N$ なるものとする．

$$\begin{tikzcd}
& L=MN \arrow[dl, dash] \arrow[dr, dash] & \\
M & & N \\
& K=M\cap N \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

(1) M/K が有限次 Galois 拡大のとき,[†20] L/N も有限次 Galois 拡大で,

$$\mathrm{Gal}(L/N) \cong \mathrm{Gal}(M/K)$$

(2) $M/K, N/K$ が有限次 Galois 拡大のとき，L/K も有限次 Galois 拡大で,

$$\mathrm{Gal}(L/N) \cong \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$$

[†20] N/K には代数拡大を仮定しないことに注意されたい．

$$\begin{tikzcd}
 & L & \\
M \arrow[ur, no head] & & N \arrow[ul, no head] \arrow[ul, dashed, bend right, "\text{fin.Gal.}"'] \\
 & K \arrow[ul, no head] \arrow[ur, no head] \arrow[ul, bend left, "\text{fin.Gal.}"] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & L & \\
M & & N \\
 & K \arrow[uu, no head] \arrow[ul, no head] \arrow[ur, no head] \arrow[ul, bend left, "\text{fin.Gal.}"] \arrow[ur, bend right, "\text{fin.Gal.}"'] \arrow[uu, dashed, bend right, "\text{fin.Gal.}"'] &
\end{tikzcd}$$

Proof. (1) M/K は有限次分離拡大なので，$\exists \alpha \in M, M = K(\alpha)$ である．$K \subset N$ より，

$$L = MN = K(\alpha)N = N(\alpha)$$

$f(T)$ を α の K 上最小多項式，$g(T)$ を α の N 上最小多項式とする．このとき，$g(T) \mid f(T)$ で $f(T)$ は分離多項式であるから $g(T)$ も分離多項式．よって L/N も有限次分離拡大.

また M は $f(T)$ の根を全て含むので，$g(T)$ の根も全て含む．よって L/N は正規拡大であり，有限次 Galois 拡大である．

ここで群準同型 φ, ψ を，

$$\varphi : \mathrm{Gal}(L/N) \to \mathrm{Gal}(M/K),\ \varphi(\sigma) = \sigma|_M$$

$$\psi : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/N),\ \psi(\tau)(x) = \begin{cases} \tau(x) & \text{if } x \in M \\ x & \text{if } x \in N \end{cases}$$

と定める．これらは well-defined である．

> (φ の well-definedness) $\sigma \in \mathrm{Gal}(L/N)$ とする．$\sigma(\alpha)$ は $g(T)$ の根なので $f(T)$ の根．よって $\sigma(\alpha) \in M$ なので $\sigma(M) \subset M$ で，$\sigma|_M \in \mathrm{Gal}(M/K)$.

> (ψ の well-definedness) $\tau \in \mathrm{Gal}(M/K), x \in M \cap N = K$ とすると，τ は K 上同型なので $\tau(x) = x$.

このとき，$\varphi^{-1} = \psi$ である．

> ($\because$) $\sigma \in \mathrm{Gal}(L/N), x \in L$ に対し，
>
> $$(\psi \circ \varphi)(\sigma)(x) = \begin{cases} \sigma|_M(x) & \text{if } x \in M \\ x & \text{if } x \in N \end{cases} = \begin{cases} \sigma(x) & \text{if } x \in M \\ x & \text{if } x \in N \end{cases} = \sigma(x)$$
>
> より，$\psi \circ \varphi = \mathrm{id}$．一方，$\tau \in \mathrm{Gal}(M/K)$ に対し，
>
> $$(\varphi \circ \psi)(\tau) = \tau|_M = \tau$$
>
> より，$\varphi \circ \psi = \mathrm{id}$.

以上より，$\mathrm{Gal}(L/N) \cong \mathrm{Gal}(M/K)$ を得る．

(2) 仮定と (1) から，$L/N, N/K$ は有限次 Galois 拡大なので L/K も有限次 Galois 拡大である．

$$
\begin{tikzcd}
& L & \\
M \arrow[ur, no head] \arrow[ur, dashed, bend left, "\text{fin.Gal.}"] & & N \arrow[ul, no head] \arrow[ul, dashed, bend right, "\text{fin.Gal.}"'] \\
& K \arrow[ul, no head] \arrow[ul, bend left, "\text{fin.Gal.}"] \arrow[ur, no head] \arrow[ur, bend right, "\text{fin.Gal.}"'] &
\end{tikzcd}
$$

群準同型 λ を，

$$\lambda : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K),\ \sigma \mapsto (\sigma|_M, \sigma|_N)$$

と定めると，これは同型である．

(単射性) $\sigma \in \mathrm{Gal}(L/K)$ に対し，

$$\begin{aligned}
\sigma \in \mathrm{Ker}\,\lambda &\Leftrightarrow (\sigma|_M, \sigma|_N) = \mathrm{id} \\
&\Leftrightarrow \sigma|_M = \mathrm{id}_M, \sigma|_N = \mathrm{id}_N \\
&\Leftrightarrow \sigma = \mathrm{id}_L
\end{aligned}$$

よって λ は単射.

(全射性) $\downarrow$ で (1) を用いて，

$$\begin{aligned}
|\mathrm{Gal}(L/K)| = [L:K] &= [L:M][M:K] \\
&= |\mathrm{Gal}(L/M)||\mathrm{Gal}(M/K)| \overset{\downarrow}{=} |\mathrm{Gal}(N/K)||\mathrm{Gal}(M/K)| \\
&= |\mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)|
\end{aligned}$$

よって λ は全射.

■

Example 7.9. (1) $\mathbb{Q}(\sqrt{2}, T) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(T), \mathbb{Q} = \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(T)$ である．$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ は 2 次 Galois 拡大であるから，

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, T)/\mathbb{Q}(T)) \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$$

(2) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}, \omega), \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}$ であり，$\mathbb{Q}(\sqrt{2})/\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ はそれぞれ 2 次，3 次 Galois 拡大であるから，

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong \mathbb{Z}/(2) \times \mathfrak{S}_3$$

参考文献

[1] 雪江明彦,『代数学 2 環と体とガロア理論 [第 2 版]』, 日本評論社，2010

[2] 雪江明彦,『整数論 1 初等整数論から p 進数へ』, 日本評論社，2013