代数学続論
体と Galois 理論

目次

1 体の拡大

以降の議論では特に述べない限り体は可換体とする。可換体は以下のように言い換えられる。

$\Leftrightarrow$ 可換整域で (0) と (1) 以外のイデアルがない。

$\Leftrightarrow$ Krull 次元が 0 の可換整域。

$\Leftrightarrow$ 可換整域で 0 以外の元は可逆。

ただし Krull 次元とは環の素イデアルの包含関係による順序の鎖の長さの上限のことである。

K:体とするとき $K^\times$:可逆元の集合とし、上の同値からこれは $K^\times = K - \{0\}$ としたものと等しい。

例 1.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}\,(p:$ 素数$), \mathbb{Q}_p\,(p$ 進体$)$

例 1.2. $K;$ 体としたとき

$K(x)$:有理関数体 $= \{$ 多項式/多項式 $(\neq 0)|$ 多項式 $\in K[x]\ \}$

$K[[x]]$:形式的冪級数体 $\{\sum_{i\in\mathbb{Z}, i\leq n} c_i x^i | c_i \in K, \in \mathbb{Z}\}$

$\mathbb{Q}$ に α を添加した体 $\Leftrightarrow \mathbb{Q}(\alpha)\,(\alpha \in \mathbb{C}) = (\alpha$ を含む最小の体 $\subset \mathbb{C}) = \{f(\alpha)|f \in \mathbb{Q}(x), (f$ の分母 $)(\alpha) \neq 0\} = \{\alpha$と有理数からできる元全体 $\}$

Fact 1.3. R:可換環 $\supset I:$ イデアル のとき、R/I:体 $\Leftrightarrow I$:極大イデアル

例 1.4. $R = K[x], I = (f)$ とするとき *Fact* から

I が極大 $\Leftrightarrow I$:素イデアル $\Leftrightarrow f$:既約

よって $K[x]/(f)$ が体 $\Leftrightarrow f$ が既約

Rem 1.5. $\mathbb{Z}/\mathbb{Z} = 0$ は零環で体ではない。$\mathbb{F}_1$:一元体 $\subset \mathbb{Z}$ は実際にはない。

定義 1.6. K, L:体 $K \subset L$ とする。

$(K$ の体構造$) = (L$ の体構造を K に制限したもの$)$ 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、体の拡大 (field extension) L/K とも言う。

定義 1.7. 体の準同型とは環としての準同型のこと。

Note 1.8. 体の準同型は全て単射。

Proof. K, L:体 , $\phi : K \longrightarrow L$:準同型とするとき $\ker(\phi)$ は K のイデアルであるから体であることより $\ker(\phi) = (0)$ または $(1) = K$ となる。$\ker(\phi) = K$ のとき $\phi(K) = 0$ から準同型であるための $\phi(1) = 1$ を満たしていないからこれは不適。したがって $\ker(\phi) = (0)$ より ϕ は単射。 □

hom : $\phi : K \longrightarrow L$ があると単射より K は L の部分体 $\phi(K)$ と同一視できる。これより L が K を含んでいなくても K の拡大体と見ることができる。

L/K が拡大のときとくに L は K 上のベクトル空間とみなせるため $\dim_K(L)$ が定義できる。$(\in \mathbb{Z}_{\geq 1} \cup \{\infty\})$

定義 1.9. $[L : K] := \dim_K(L)$ と書きこれを L/K の 拡大次数 (extension degree)という。この値により拡大は有限次拡大、無限次拡大に分けられる。

例 1.10. $K(x)/K$ とするとき x が不定元なのでこれは無限次拡大。

$K[x]/(f)$ で $f = a_0 + a_1 x + \cdots + a_n x^n$ で既約とすると $a_n = 1$ とできて、$x^n \equiv -(a_0 + \cdots + a_{n-1}x^{n-1}), (\bmod (f))$ となり n 次以上の多項式の次数を下げられるので結局基底は $1, x, \cdots x^{n-1}$ より $[K(x)/(f) : K] = n$ となるのでこれは有限次拡大。

補題 1.11. *$L/M, L/K$:体の有限次拡大、 $M \supset K$ のとき $[L : M] = [L : K]$ ならば $M = K$。*

Proof. ここで L の M 上の基底を (e_i) とし K 上の基底を (f_i) とするとまず拡大次数の定義からこの個数は等しい。この値を n とすると $M^n \cong L \cong K^n$ であり $M^n \cong K^n$ となる。したがって $M \supset K$ から $M = K$ となるので示された。 □

定義 1.12. 体 L に対しその自己同型写像の集合を

$$\mathrm{Aut}(L) := \{\text{ 体の自己同型 } | \sigma : L \longrightarrow L\}$$

と書きこれは写像の合成について群になっている。また、拡大 L/K に対して K の拡大体としての同型写像 ($K-$ 同型写像) の集合を

$$\mathrm{Aut}_K(L) := \{\sigma \in \mathrm{Aut}(L) | \sigma_K = \mathrm{id}_K\}$$

と書きこれは $\mathrm{Aut}(L)$ の部分群になる。

またこれは K の拡大としての L から L の準同型写像とも言えるため $\mathrm{Hom}_{K\text{ の拡大}}(L, L)$ または明らかなときは $\mathrm{Hom}_K(L, L)$ と書ける。

群になることは写像の結合法則、 id_L が単位元、逆元は同型写像より逆写像を考えればよい。

定義 1.13. L/K が拡大、 $K \subset M \subset L$ で M が L の部分体であるとき M は L/K の<u>中間体 (intermediate field)</u>という。これを $L/M/K$ とかくこともある。

また、 $L/M/K$ のとき $\mathrm{Aut}_K(L) \supset \mathrm{Aut}_M(L)$ が得られる。一般に $\mathrm{Aut}_K(M)$ は包含関係が言えない。

定義 1.14. L:体 $H(\subset \mathrm{Aut}(L))$:部分集合の 2 つに対し

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

は L の部分体になり、L の H による<u>固定部分体</u>という。このような元を H により固定される元ともいう。

部分体になることは $\sigma \in H \subset \mathrm{Aut}(L)$ は同型写像より加法乗法を保存し、 $1, 0$ は常に動かないことからわかる。

Rem 1.15. $H_1 \subset H_2 \subset \mathrm{Aut}(L) \Longrightarrow L^{H_1} \supset L^{H_2}$ が成り立つ。これは H_2 により固定される元は包含関係より H_1 によっても固定されるからである。

Rem 1.16. $L/M/K$ のとき $[L : K] = [L : M][M : K]$ が成り立つ。何れかが無限次元であれば成立する。

有限次元の場合は次のようになる。L を M 上のベクトル空間と見たとき、その基底は $[L : M]$ 個でその係数は M の元であるから M を K 上のベクトル空間と見たときの $[M : K]$ 個の基底で書かれるため L を K 上のベクトル空間と見たときはその基底の積で書かれるからである。

一般に $V : M-\mathrm{vect.sp}, M/K$:拡大のとき V を K 上のベクトル空間と見れて $\dim_K(V) = \dim_M(V) \cdot [M : K]$ となる。

2　Galois 理論の基本定理

2.1　Dedekind の補題

定義 2.1. 有限次拡大 L/K が Galois 拡大であるとは $L^{\mathrm{Aut}_K(L)} = K$ であること。

このときの $\mathrm{Aut}_K(L)$ をとくに $\mathrm{Gal}(L/K)$ と記し、 L/K の Galois 群という。

Rem 2.2. $L^{\mathrm{Aut}_K(L)}$ は K を固定するような元で固定される L の元であるから $L^{\mathrm{Aut}_K(L)} \supset K$ は定義より明らか。それ以外に固定される元が無いということ。

また、よくある Galois 拡大の定義は正規かつ分離な拡大というものでこれとの同値は後で示す。

Galois 理論の基本定理を示すために準備を行う。

補題 2.3. S:群 L:体とし、 $\sigma_1, \ldots, \sigma_n : S \longrightarrow L^\times$ を相異なる群準同型とする。このとき $c_1, \cdots c_n \in L$ に対し以下が成り立つ。

$$c_1\sigma_1(x) + \cdots + c_n\sigma_n(x) = 0 \ ({}^\forall x \in S) \Longrightarrow c_1 = \cdots = c_n = 0$$

Proof. 成り立たないと仮定し、ある $c_1, \ldots, c_n \in S$ が成り立たないとするもののうち n が最小であるような最短の反例であるとする。まずこのとき $n \leq 2$ である。$n = 1$ のとき $c_1\sigma_1(x) = 0$ であるが $\sigma_1(x) \in L^\times = L - \{0\}$ から $c_1 = 0$ となるからである。

相異なる群準同型より写像として異なるということは $\sigma_n \neq \sigma_1$ より ${}^\exists x_0 \in S, \sigma_n(x_0) \neq \sigma_1(x_0)$ となる。x_0x を入れると準同型より

$$c_1\sigma_1(x_0)\sigma_1(x) + \cdots + c_n\sigma_n(x_0)\sigma_n(x) = 0 \tag{1}$$

となる。これと $\sigma_n(x_0)$ を式にかけたものは

$$c_1\sigma_n(x_0)\sigma_1(x) + \cdots + c_n\sigma_n(x_0)\sigma_n(x) = 0 \tag{2}$$

となりこれを辺々ひくと $c_n\sigma_n(x_0)\sigma_n(x)$ が共通であるからそこが消えて、 $\sigma_1(x_0) - \sigma_n(x_0) \neq 0$ より

$$c_1(\sigma_1(x_0) - \sigma_n(x_0))\sigma_1(x) + \cdots + c_{n-1}(\sigma_{n-1}(x_0) - \sigma_n(x_0))\sigma_{n-1}(x) = 0$$

となり $c_k(\sigma_k(x_0) - \sigma_n(x_0))$ を新しい係数と見れば左辺は少なくとも全ての項が 0 になることは無いので $c_1, \ldots, c_n$ の最短性に矛盾しているから $c_1 = \cdots = c_n = 0$ である。

□

補題 2.4. Dedekind の補題

M, L:体とし、 $\sigma_1, \ldots, \sigma_n : M \longrightarrow L$ が相異なる体の準同型とする。このとき $c_1, \ldots, c_n \in L$ に対し、以下が成り立つ。

$$c_1\sigma_1(x) + \cdots + c_n\sigma_n(x) = 0 \ ({}^\forall x \in M) \Longrightarrow c_1 = \cdots = c_n = 0$$

Proof. 乗法群に制限したものは $\sigma_i|_{M^\times} : M^\times \longrightarrow L^\times$ でありこれは相異なる群準同型なので補題 2.3 より成立。 $\square$

Rem 2.5. 写像 $\mathrm{Hom}_{体}(M, L) \longrightarrow \mathrm{Hom}_{加法群}(M, L)$ を 体の準同型をその加法群の準同型とみるというものにする。また、このとき $\mathrm{Hom}_{加法群}(M, L)$ は $(\phi_1 + \phi_2)(x) = \phi_1(x) + \phi_2(x), (c\phi)(x) = c(\phi(x))$ $c \in L$ とすることで L の加法により L-ベクトル空間と見れる。そしてこの写像でそれぞれの元は変わらず変わるのは始域と終域の演算なので単射であり像は一次独立となることを補題 2.4 は述べている。

補題 2.6. Dedekind の補題$/K$

$L/M, M/K$:拡大で $\sigma_1, \ldots, \sigma_n : M \longrightarrow L$ を相異なる K 上の体準同型 $(\sigma_i|_K = \mathrm{id}_K)$ とする。このとき $c_1, \ldots, c_n \in L$ に対し、以下が成り立つ。

$$c_1\sigma_1(x) + \cdots + c_n\sigma_n(x) = 0 \ ({}^\forall x \in M) \Longrightarrow c_1 = \cdots = c_n = 0$$

Proof. Dedekind の補題から明らか。 $\square$

Rem 2.7. これも 2.4 と同様に K 上の体準同型であることも考えれば写像 $\mathrm{Hom}_{K\,の拡大}(M, L) \longrightarrow \mathrm{Hom}_{K-ベクトル空間}(M, L)$ が単射で像は L 上一次独立である。

2.2 Artin の定理

補題 2.8. $M/K, L/K$:体の拡大として M/K が有限次拡大のとき $|\mathrm{Hom}_{K\,の拡大}(M, L)|$ は有限で $|\mathrm{Hom}_{K\,の拡大}(M, L)| \leq [M : K]$ が成り立つ。

Proof. まず、 $\mathrm{Hom}_K(M, K) \otimes_K L \cong \mathrm{Hom}_K(M, L)$ を示す。

$f \in \mathrm{Hom}_K(M, K), l \in L$ に対し $\varphi(f, l) : M \longrightarrow L, m \longmapsto f(m)l$ とする。このときこれは $f \in \mathrm{Hom}_K(M, K)$ から以下のように K 線形写像であるから $\varphi(f, l) \in \mathrm{Hom}_K(M, L)$ である。

$$\begin{aligned}\varphi(f, l)(m_1 + m_2) &= f(m_1 + m_2)l = (f(m_1) + f(m_2))l = f(m_1)l + f(m_2)l = \varphi(m_1) + \varphi(m_2) \\ \varphi(f, l)(km) &= f(km)l = kf(m)l = k\varphi(m)\end{aligned}$$

そして $\phi : \mathrm{Hom}_K(M, K) \times L \longrightarrow \mathrm{Hom}_K(M, L), (f, l) \longmapsto \phi(f, l) = \varphi(f, l)$ とすると ϕ は以下のように L-双線形写像になる。

$$\begin{aligned}\phi(f_1 + f_2, l)(m) &= (f_1 + f_2)(m)l = f_1(m)l + f_2(m)l = \phi(f_1, l) + \phi(f_2, l) = (\phi(f_1, l) + \phi(f_2, l))(m) \\ \phi(f, l_1 + l_2)(m) &= f(m)(l_1 + l_2) = f(m)l_1 + f(m)l_2 = \phi(f, l_1)(m) + \phi(f, l_2)(m) = (\phi(f, l_1) + \phi(f, l_2))(m) \\ \phi(kf, l)(m) &= (kf)(m)l = k(f(m))l = k\phi(f, l)(m) \\ \phi(f, kl)(m) &= f(m)kl = k(f(m))l = k\phi(f, l)(m)\end{aligned}$$

したがってテンソル積の普遍性から $\theta : \mathrm{Hom}_K(M, K) \otimes_K L \longrightarrow \mathrm{Hom}_K(M, L)$ であり $\theta(f \otimes l) : M \longrightarrow L, m \longmapsto f(m)l$ と定められたものが一意に定まる。

今、有限次拡大であるので M の基底を (m_i)、その双対空間 $\mathrm{Hom}_K(M, K)$ の基底つまり双対基底を (f_i)、L の基底を (l_j) とできる。よって $z \in \mathrm{Hom}_K(M, K) \otimes_K L$ は $z = \sum_{ij} a_i j(f_i \otimes l_j), a_{ij} \in K$ と書ける。そして定義から $\theta(z)(m) = \sum_{ij} a_i j(f_i(m)l_j)$ となる。$m = m_i$ とすると双対基底からクロネッカーのデルタから $f_i(m_j) = \delta_{ij}$ となるので $\theta(z)(m_i) = \sum_j a_i j l_j$ である。$\theta(z) = 0$ になるとき、全ての (m_i) において 0 にな

るので (l_j) が基底より一次独立を考えれば $\forall i, \sum_j a_ijl_j = 0 \Leftrightarrow a_ij = 0$ となるから $z = 0$ より $\ker(\theta) = 0$ より θ は単射。

また、任意の $f \in \mathrm{Hom}_K(M, L)$ に対して $z = \sum_i f_i \otimes f(m_i)$ とおくと $\theta(z)(m) = \sum_i f_i(m)f(m_i)$ から $m = m_i$ とおけば双対基底より同様に $\theta(z)(m_i) = f(m_i)$ であり (m_i) は基底なので $\theta(z) = f$ となるから θ は全射。

よって θ は全単射であり、K-双線形写像より θ は同型写像となるので $\mathrm{Hom}_K(M, K) \otimes_K L \cong \mathrm{Hom}_K(M, L)$ が成り立つ。

次に $\mathrm{Hom}_K(M, K) \otimes_K L \cong L^n$ を示す。

今 $[M : K] = n$ とするとある基底を取れば M が K ベクトル空間より $M \cong K^n$ とできるので $\mathrm{Hom}_K(M, K) \otimes_K L \cong \mathrm{Hom}_K(K^n, K) \otimes_K L$ となる。また、 $\mathrm{Hom}_K(K^n, K)$ は $M = K^n$ の双対空間なので基底を移せるので $\mathrm{Hom}_K(K^n, K) \cong K^n$ より $\mathrm{Hom}_K(K^n, K) \otimes_K L \cong K^n \otimes_K L$ となる。

そして $\phi : K^n \otimes_K L \longrightarrow L^n, (k_1, \ldots, k_n) \otimes l \longmapsto (k_1l, \ldots, k_nl)$ とする。これは $(k_1l, \ldots, k_nl) = (k'_1l', \ldots, k'_nl') \Leftrightarrow \forall i, k_il = k'_il$ であり L が体なので l^{-1} をかければ $k_i = k'_i$ より $(k_1, \ldots, k_n) = (k'_1, \ldots, k'_n)$ から ϕ は単射。そして、任意の $(l_1, \ldots, l_n) \in L^n$ に対して $k_i = l_il^{-1}$ ととれば $\phi((k_1, \ldots, k_n) \otimes l) = (l_1, \ldots, l_n)$ より全射。構造も保たれるから $K^n \otimes_K L \cong L^n$ となる。

したがって同型から、 $[M : K] = n = \dim_L(L^n) = \dim_L(K^n \otimes_K L) = \dim_L(\mathrm{Hom}_K(M, K) \otimes_K L) = \dim_L(\mathrm{Hom}_K(M, L))$ より $\dim_L(\mathrm{Hom}_K(M, L)) = [M : K]$ となる。

そして補題 2.7 から単射で一次独立であることから $\mathrm{Hom}_{K\text{ の拡大}}(M, L)$ は $\mathrm{Hom}_K(M, L)$ に埋め込めるから $|\mathrm{Hom}_{K\text{ の拡大}}(M, L)| \leq |\mathrm{Hom}_K(M, L)| = [M : K]$ より示された。 □

定理 2.9. Artin の定理

L/K が有限次拡大のとき

$$L/K \text{ が Galois 拡大} \Leftrightarrow K = L^G \text{となる部分群 } G \subset \mathrm{Aut}(L) \text{ が存在する。}$$

このとき $G = \mathrm{Gal}(L/K), [L : K] = |G|$ が成り立つ。

Proof. 必要十分性を示す。

$(\Rightarrow)$

$G = \mathrm{Gal}(L/K)$ とすれば Galois 拡大の定義より成立。

$(\Leftarrow)$

$K = L^G$ のとき G の元は K の元を固定するので $G \subset \mathrm{Aut}_K(L)$ であり、1.15 により包含関係が逆になり $L^G \supset L^{\mathrm{Aut}_K(L)}$ となる。$L^{\mathrm{Aut}_K(L)}$ は K の元で固定されるような元により固定される L の元なので K を含む。したがって以下のようになる。

$$K = L^G \supset L^{\mathrm{Aut}_K(L)} \supset K$$

より $K = L^G = L^{\mathrm{Aut}_K(L)} = K$ から $K = L^{\mathrm{Aut}_K(L)}$ より L/K は Galois 拡大。

$L^G = L^{\mathrm{Aut}_K(L)}$ から $G = \mathrm{Aut}_K(L)$ とは言えないので以下のように示す。まず $[L : K] = |G|$ を示す。

補題 2.8 から $G \subset \mathrm{Aut}_K(L)$ より $|G| \leq |\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L, L)| \leq [L : K]$ となるので $|G| \geq [L : K]$ が言えればよい。

$|G| < [L : K]$ と仮定する。

$G=\{\sigma_1,\dots,\sigma_m\}, L$ の K 上の基底を $(w_1,\dots,w_n)$ とする。仮定より $m \le n$ なので $(n\times m)$ の連立方程式系

$$\begin{cases}\sigma_1(w_1)x_1+\cdots+\sigma_1(w_n)x_n=0\\ \vdots\\ \sigma_m(w_1)x_1+\cdots+\sigma_m(w_n)x_n=0\end{cases}$$

が作られ、変数の数 (n) より式の数 m のほうが多いから非自明解が存在する。その解を $(c_1,\dots,c_n)\in L^n$ としそのうち 0 が一番多い最短の解を考え添字を並び替え 0 の解を後ろにまとめ、 0 でない解 $c_i, (1\le i\le r)$ で連立方程式系を以下のようにできる。

$$\begin{cases}c_1\sigma_1(w_1)+\cdots+c_r\sigma_1(w_r)=0\\ \vdots\\ c_1\sigma_m(w_1)+\cdots+c_r\sigma_m(w_r)=0\end{cases}\tag{3}$$

まず、 2.3 のときと同様に $r\le 2$ である。また、 $c_r(\neq 0)\in L$ で割って $c_r=1$ と置き直せる。そして $^{\exists}c_i\in L-K$ となる。もし $^{\forall}c_i\in K$ とすると $\sigma|_K=\mathrm{id_K}$ より $c_i\sigma(w_i)=\sigma(c_iw_i)$ と、準同型より $\sigma_1(c_1w_1+\cdots+c_rw_r)=0 \Rightarrow c_1w_1+\cdots c_rw_r=0$ となる。そして (w_i) は基底だから一次独立より $c_1=\cdots=c_r=0$ となりこれは非自明解であることに矛盾する。よって c_i 全てが K に入ることは無いから $^{\exists}c_i\in L-K$ となりこれを c_1 とおく。このとき K に入っていないから $^{\exists}\sigma\in G, \sigma(c_1)\neq c_1$ が成り立つ。

この σ を連立方程式全体に作用させると以下のようになる。

$$\begin{cases}\sigma(c_1)\sigma(\sigma_1(w_1))+\cdots+\sigma(c_r)\sigma(\sigma_1(w_r))=0\\ \vdots\\ \sigma(c_1)\sigma(\sigma_m(w_1))+\cdots+\sigma(c_r)\sigma(\sigma_m(w_r))=0\end{cases}$$

ここで G は有限なので $\sigma\sigma_i$ は i を動かすことで G のすべての元を出し尽くすから、また添字を付け替えて方程式を並び替えて $\sigma\sigma_i$ を σ_i として以下のようにして良い。

$$\begin{cases}\sigma(c_1)\sigma_1(w_1)+\cdots+\sigma(c_r)\sigma_1(w_r)=0\\ \vdots\\ \sigma(c_1)\sigma_m(w_1)+\cdots+\sigma(c_r)\sigma_m(w_r)=0\end{cases}\tag{4}$$

式 (3) − 式 (4) とすると以下のようになる。

$$\begin{cases}(c_1-\sigma(c_1))\sigma_1(w_1)+\cdots+(c_r-\sigma(c_r))\sigma_1(w_r)=0\\ \vdots\\ (c_1-\sigma(c_1))\sigma_m(w_1)+\cdots+(c_r-\sigma(c_r))\sigma_m(w_r)=0\end{cases}$$

そして $c_1-\sigma(c_1)\neq 0$ と $c_r=1$ から $c_r-\sigma(c_r)=1-1=0$ より r の最短性に矛盾する。よって $|G|<[L:K]$ は不適であるから $|G|\ge[L:K]$ なので $|G|=[L:K]$ が成り立つ。

これより $G \subset \mathrm{Aut}_K(L)$ と一番外側の値が同じであるからその間の不等号も等号になるので $|G| = |\mathrm{Aut}_K(L)| = [L:K]$ より $G = \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$ も成り立つことがわかる。

□

系 2.10. L/K:有限次拡大で $|\mathrm{Aut}_K(L)| \geq [L:K]$ ならば L/K は Galois 拡大。

Proof. $G = \mathrm{Aut}_K(L)$ とおく。Artin の定理から $K' = L^G$ とすれば $G \subset \mathrm{Aut}(L)$ より L/L^G は Galois 拡大。したがって $[L:L^G] = |G|$ となる。ここで L^G は K の元を固定するような元で固定される L の元なので $L^G \supset K$ である。よって $L/L^G, L/K, L^G/K$ はともに体の拡大であるから $[L:K] = [L:L^G][L^G:K]$ が成り立ち、 $[L:L^G] = |G|$ と仮定 $|G| \geq [L:K]$ より $|G| \geq |G|[L^G:K] \Rightarrow [L^G:K] = 1$ となる。よって $|G| = |\mathrm{Aut}_K(L)| = [L:L^G] = [L:K]$ である。

補題 (1.11) より $L^G = K$ となるので Galois 拡大の定義より L/K は Galois 拡大。 □

Rem 2.11. $|\mathrm{Aut}_K(L)| \leq [L:K]$ は補題 2.8 から $M = L$ とすれば $|\mathrm{Aut}_K(L)| = |\mathrm{Hom}_{K\text{ の拡大}}(L,L)| \leq [L,K]$ より L/K が有限次拡大なら Galois 拡大に限らず常に成り立つ。

よって以下の Galois 拡大の特徴づけが言える。

$$|\mathrm{Aut}_K(L)| = [L/K] \Leftrightarrow L/K \text{ が Galois 拡大}$$

系 2.12. L/K:有限次拡大のとき ${}^\forall L'/L$(L の拡大体) で次が成り立つ。L/K:Galois$\Rightarrow$ $\mathrm{Aut}_K(L)(= \mathrm{Gal}(L/K)) \xrightarrow{\sim} \mathrm{Hom}_{K\text{ の拡大}}(L,L')$ つまり $\mathrm{Aut}_K(L)$ と $\mathrm{Hom}_K(L,L')$ の間に同型写像が作れる。

Proof. 終域がより大きいほうが写像の行き先が増え、 L'/L から $\mathrm{Aut}_K(L) = \mathrm{Hom}_{K\text{ の拡大}}(L,L) \subset \mathrm{Hom}_{K\text{ の拡大}}(L,L')$ である。そして L/K から L'/K も体の拡大であるので補題 2.8 から M を L, L を L' とみなすことで $|\mathrm{Hom}_K(L,L')| \leq [L:K]$ となる。また、 L/K が Galois 拡大より Artin の定理から $|\mathrm{Aut}_K(L)| = [L:K]$ なので $[L:K] = |\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L,L)| \leq |\mathrm{Hom}_K(L,L')| = [L:K]$ と包含関係より $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L,L) = \mathrm{Hom}_K(L,L')$ である。よって $\mathrm{Aut}_K(L)$ と $\mathrm{Hom}_K(L,L')$ の間には同型写像を作ることができる。 □

2.3 Galois 理論の基本定理

定理 2.13. Galois 理論の基本定理

L/K:有限次 Galois 拡大、 $G = \mathrm{Gal}(L/K)$ とおく。このとき以下が成立する。

(1) L/K の任意の中間体 M に対し L/M は Galois 拡大であり、次の $1:1$ 対応がある。

$$\begin{aligned} \{L/K \text{ の中間体 }\} &\overset{1:1}{\longleftrightarrow} \{G \text{ の部分群 }\} \\ M &\longmapsto \mathrm{Aut}_M(L) = \mathrm{Gal}(L/M) \\ L^H &\longleftarrow\!\shortmid\ H \end{aligned}$$

(2) この対応で $M_i \longleftrightarrow H_i$ のとき $(i = 1, 2)$

$$M_1 \subset M_2 \Leftrightarrow H_1 \supset H_2$$

(3) $M \longleftrightarrow H$ のとき ${}^\forall\sigma \in G$ に対し

$$\sigma(M) \longleftrightarrow \sigma H \sigma^{-1}$$

(4) $M \longleftrightarrow H$ のとき

$$M/K \text{ が Galois 拡大} \Longleftrightarrow H \triangleleft G (H \text{ が } G \text{ の正規部分群})$$

でありこのとき

$$\mathrm{Gal}(M/K) \cong G/H$$

Proof. ・(1)

両側から写像で写して戻したときにもとに戻ることを示す。

$H \longmapsto L^H \longmapsto \mathrm{Aut}_{L^H}(L)$ となるから $H = \mathrm{Aut}_{L^H}(L)$ を示す。$M = L^H$ とおくと Artin の定理から $M = L^H$ となる $H \subset \mathrm{Aut}(L)$ が存在しているので $L/M = L/L^H$ は Galois であり、 $H = \mathrm{Gal}(L/M) = \mathrm{Gal}(L/L^H)$ となるので $H = \mathrm{Aut}_{L^H}(L)$ が言えた。

次に $M \longmapsto \mathrm{Aut}_M(L) \longmapsto L^{\mathrm{Aut}_M(L)}$ となるから $M = L^{\mathrm{Aut}_M(L)}$ を示す。$H = \mathrm{Aut}_M(L)$ とすると $L^H \supset M$ は定義より明らかでそのことから係数がより大きな範囲で取れることより $[L : L^H] \leq [L : M]$ となる。

$[L^H : K] \leq [M : K]$ を示す。仮定より L/K が、Artin の定理より L/L^H が Galois 拡大なので Rem (2.11) から $[L : K] = |G|, [L : L^H] = |H|$ で $[L : K] = [L : L^H][L^H : K]$ から $|G| = |H|[L^H : K]$ となる。そして H が G の部分群より指数を $(G : H)$ と書くこととすれば $|G| = (G : H)|H|$ であるから $(G : H) = [L^H : K]$ が言える。Lagrange の定理から $r = (G : H)$ としたとき $\phi, \varphi \in G$ において同値関係 $\phi^{-1}\varphi \Leftrightarrow \phi \sim \varphi$ による剰余類分割によって $G = \tau_1 H \cup \cdots \cup \tau_r H$ とできる。ここで $\tau_i \in G$ が M に制限されたとしても $\tau_i|_M$ は相異なるといえる。これはもしある代表元同士、つまり同値ではない元において $\tau_i(x) = \tau_j(x), {}^\forall x \in M$ とすると自己同型写像であるから逆写像が考えられて $\tau_i^{-1}\tau_j|_M = \mathrm{id}_M$ である。よってこの写像は M の元を固定するので $\tau_i^{-1}\tau_j \in H = \mathrm{Aut}_M(L)$ となる。これは同値関係の定義から $\tau_i \sim \tau_j$ となるので同値ではない元を取ったことに矛盾する。したがって代表元は M に制限しても全て相異なる。このことから M に制限された G の元 $\tau|_M$ は少なくとも $r = (G : H)$ 個あるため補題 (2.8) から $r = (G : H) = [L^H : K] \leq |\mathrm{Hom}_{K \text{ の拡大}}(M, L)| \leq [M : K]$ であるので $[L^H : K] \leq [M : K]$ が示された。

よっていま $[L^H : K] \leq [M : K], [L : L^H] \leq [L : M]$ が成り立っている。そして $[L : K] = [L : L^H][L^H : K] = [L : M][M : K]$ から 1 つ目の不等式より $1/[L : L^H] \leq 1/[L : M]$ となるので $[L : L^H] \geq [L : M]$ も成り立つ。したがって $[L : L^H] = [L : M]$ となる。$L^H \supset M$ で拡大次数が等しいので補題 (1.11) から $L^{\mathrm{Aut}_M(L)} = L^H = M$ となる。

よって両側から写像を送って戻したときにもとの元に戻ってくるためこの対応は $1:1$ 対応になっている。

$1:1$ 対応より任意の中間体 M に対して $M = L^H$ となるような G の部分群 H が存在し、それは上の議論より $H = \mathrm{Aut}_M(L)$ となる。したがって定義より L/M は Galois 拡大。実際はこのような H が存在することだけで Artin の定理から L/M が Galois 拡大であることがわかる。

・(2)

双方とも定義より固定する元固定される元を考えれば明らかであるがここでは一つ一つ示していく。

$(\Leftarrow)$

M_1 の任意の元 x をとる。L/M_i は Galois 拡大より $M_1 = L^{H_1}, M_2 = L^{H_2}$ より ${}^\forall\sigma \in H_1, \sigma(x) = x$ である。$H_1 \supset H_2$ より ${}^\forall\sigma \in H_2 \subset H_1, \sigma(x) = (x)$ となるから $x \in L^{H_2} = M_2$ となるので $M_1 \subset M_2$ となり成り立つ。

$(\Rightarrow)$

H_2 の任意の元 σ をとる。$H_2 = \mathrm{Gal}(L/M_2)$ より ${}^\forall x \in M_2, \sigma(x) = x$ となり、$M_1 \subset M_2$ より ${}^\forall x \in M_1 \subset M_2, \sigma(x) = x$ である。したがって $\sigma \in \mathrm{Gal}(L/M_1) = H_1$ より $H_1 \subset H_2$ となり成り立つ。

・(3)

${}^\forall \sigma \in G$ に対して $\sigma(M) \longmapsto \mathrm{Gal}(L/\sigma(M)), \sigma H \sigma^{-1} = \sigma \mathrm{Gal}(L/M)\sigma^{-1}$ より 1 : 1 対応から $\mathrm{Gal}(L/\sigma(M)) = \sigma \mathrm{Gal}(L/M)\sigma^{-1}$ を示せばよい。

${}^\forall \tau \in \mathrm{Gal}(L/M)$ に対して $\sigma\tau\sigma^{-1} \in \sigma H \sigma^{-1}$ であり、 $\tau|_M = \mathrm{id}_M$ から ${}^\forall x \in M, \sigma\tau\sigma^{-1}(\sigma(x)) = \sigma\tau(x) = \sigma(x)$ となる。よって $\sigma\tau\sigma^{-1}$ は $\sigma(M)$ 上恒等写像になるので $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(L/\sigma(M))$ より τ の任意性から $\sigma \mathrm{Gal}(L/M)\sigma^{-1} \subset \mathrm{Gal}(L/\sigma(M))$ である。

また、 $g = \sigma^{-1}, N = \sigma(M)$ とおく。このとき $\sigma^{-1}\mathrm{Gal}(L/\sigma(M))\sigma = g\mathrm{Gal}(L/N)g^{-1}$ となり、これと $\mathrm{Gal}(L/g(N))$ に対して上と全く同じことを考えれば $g\mathrm{Gal}(L/N)g^{-1} \subset \mathrm{Gal}(L/g(N))$ となる。そして左右から g, g^{-1} をかけて、 $g = \sigma{-}1$ から $g(N) = M$ より $\mathrm{Gal}(L/\sigma(M)) \subset \sigma\mathrm{Gal}(L/M)\sigma^{-1}$ である。

以上より $\mathrm{Gal}(L/\sigma(M)) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$ が示されたのでこの対応が成り立つ。

・(4)

${}^\forall \sigma \in G$ に対して (1), (3) より $H \lhd G \Leftrightarrow \sigma H \sigma^{-1} = H \Leftrightarrow \sigma(M) = M$ であるから $\sigma(M) = M \Leftrightarrow M/K$ が Galois 拡大を示せば良い。

$(\Rightarrow)$

${}^\forall \sigma \in G, \sigma(M) = M$ のとき $\sigma|_M : M \longrightarrow M$ となるから σ は M の K 上自己同型写像。これより $\pi : G \longrightarrow \mathrm{Aut}_K(M), \sigma \longmapsto \sigma|_M$ という写像が作れてこれは G の元を M に制限しているだけなので G の構造を保つから群準同型写像である。$M \Leftrightarrow H$ の対応があるから $\ker(\pi) = \{\sigma \in G | \sigma|_M = \mathrm{id}_M\} = \mathrm{Aut}_M(L) = H$ より準同型定理から $G/H \cong \mathrm{Im}(\pi) \subset \mathrm{Aut}_K(M)$ となる。よって $|G/H| = |\mathrm{Im}(\pi)| \leq |\mathrm{Aut}_K(M)|$ と (1) の話から $|G/H| = (G : H) = [M : K]$ なので $[M : K] \leq |\mathrm{Aut}_K(M)|$ となるため、系 (2.10) から M/K は Galois 拡大である。

そして有限次 Galois 拡大より $[M : K] = |G/H| = |\mathrm{Aut}_K(M)|$ でこれらは有限であり、自然な準同型 $\theta : G/H \longrightarrow \mathrm{Aut}_K(M), \sigma H \longmapsto \sigma|_M$ は $\ker(\theta) = \{\sigma H \in G/H | \sigma|_M = \mathrm{id}_M\} = \{\sigma H | \sigma \in H\} = H$ となるので単射。したがって θ は同型写像なので $\mathrm{Gal}(M/K) \cong G/H$ が示された。

$(\Leftarrow)$

M/K が Galois 拡大とすると L/M の拡大に対して系 (2.12) から $\mathrm{Aut}_K(M) = \mathrm{Hom}_K(M, L)$ となる。よって $\mathrm{Hom}_K(M, L) \subset G$ より ${}^\forall \sigma (\in G) : M \longrightarrow L$ は $\sigma \in \mathrm{Hom}_K(M, L) = \mathrm{Aut}_K(M)$ だから K 上の M 自己同型写像となるので $\sigma(M) = M$ となる。

$\square$

3　代数方程式の可解性

以下では K:体 $\supset \mathbb{Q}$ (とくに標数 $\mathrm{char}(K)=0$)(標数は次の章で詳しく述べる) で $f=\sum_{i=0}^{n} c_i X^i \in K[X]$ とする。

定義 3.1. 方程式 $f(X)=0$ が 代数的に解けるとは f の任意の根が f の係数 c_i と加減乗除と $\sqrt[m]{\ }(m\in\mathbb{N})$ を使って書けること。

定義 3.2. L/K_0 が冪根拡大とはある n_i, l と $a_i \in K_i$ によって

$$K_0 \subset K_1 \subset \cdots \subset K_l = L$$
$$K_i = K_{i-1}(\sqrt[n_{i-1}]{a_{i-1}})$$

となるような形の拡大のこと。

つまり、定義 (3.1) は $K_0 := \mathbb{Q}(c_0,\ldots,c_n), \alpha_1,\ldots,\alpha_n : f$ の解とするとき、 $\alpha_j \in (K_0\text{の}^{\exists}\text{冪根拡大})$ ということ。または、 $K_0(\alpha_1,\ldots,\alpha_n) \subset (K_0\text{の}^{\exists}\text{冪根拡大})$ になるということ。

定義 3.3. ある群 G における交換子 (commutator)とは G の元 x,y によってできる $xyx^{-1}y^{-1}$ という形の元のこと。そしてその群における交換子群 (commutatorsubgroup) (G,G) とは G の任意の交換子によって生成される群である。つまり $(G,G) := \langle ghg^{-1}h^{-1} | g,h\in G\rangle$ と定義される。

定理 3.4. 群 G に対してその交換子群は正規部分群であり、商群 $G/(G,G)$ は Abel 群である。さらに (G,G) は G/H が Abel 群になるような任意の正規部分群 H のうち最小の正規部分群である。この $G/(G,G)$ を G の最大 Abel 商といい G^{ab} と書く。

Proof. ・正規部分群になること

任意の交換子 $xyx^{-1}y^{-1}$ のどのような共役な元も

$$g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1}$$

となり交換子として書けるので交換子群に含まれる。(G,G) の任意の元は交換子の積 $c_1c_2\cdots c_k$ で表せられるので

$$g(c_1c_2\cdots c_k)g^{-1} = (gc_1g^{-1})(gc_2g^{-1})\cdots(gc_kg^{-1})$$

となり右辺のそれぞれが (G,G) に含まれるので任意の交換子群の元の共役元はその交換子群に含まれるから (G,G) は G の正規部分群。

・ $G/(G,G)$ が Abel 群になること

$x,y\in G$ に対して $xyx^{-1}y^{-1} \in (G,G)$ より $(G,G)xyx^{-1}y^{-1} = (G,G)$ なので $(G,G)xy = (G,G)yx$ となるので $G/(G,G)$ は Abel 群である。

・ 最小になること

G/H が Abel 群で H が正規部分群であるとする。このとき $^{\forall}x,y\in G$ に対して $Hxy=Hyx$ であるから $Hxyx^{-1}y^{-1}=H$ より任意の交換子 $xyx^{-1}y^{-1}\in H$ でなければならない。よって G/H が Abel 群となるような任意の正規部分群 H は (G,G) を含むためそのような正規部分群のうち最小である。

□

定義 3.5. 群 G が可解であるとは交換子群 $(G_j, G_j) = \langle ghg^{-1}h^{-1} | g, h \in G \rangle$ としたときある有限な l で以下のようになること。この包含関係の列を可解列という。

$$G \supset G_1 \supset G_2 \supset \cdots \supset G_l = 1$$
$$G_j = (G_{j-1}, G_{j-1})$$

定義 3.6. Galois 拡大 L/K が 可解拡大 (solvable extension)とは $\mathrm{Gal}(L/K)$ が可解であること。

Galois 拡大 L/K が Abel 拡大 (abelian extension)とは $\mathrm{Gal}(L/K)$ が Abel 群であること。

定理 3.7. 可解拡大は Abel 拡大を繰り返し行うことでできる拡大である。

Proof. 有限次可解拡大 L/K がありその Galois 群を G とする。このとき G の交換子群 $G_1 = (G, G)$ に対応する体を M_1 とする。ここで Galois 理論の基本定理 (2.13) の (4) から $(G, G) \lhd G$ より M_1/K が Galois で $\mathrm{Gal}(M_1/K) \cong G/(G, G)$ なので $G/(G, G)$ が Abel より $\mathrm{Gal}(M_1/K)$ も Abel なので M_1/K は Abel 拡大となる。

同様に L/K の可解列 $G \subset G_1 \subset \cdots \subset G_l = 1$ の $G_i = (G_{i-1}, G_{i-1})$ に対応する部分体 M_i を考えると $G_i \lhd G_{i-1}$ より基本定理の (4) から M_i/M_{i-1} は Galois で $G_{i-1}/(G_{i-1}, G_{i-1}) = G_{i-1}/G_i \cong \mathrm{Gal}(M_i/M_{i-1})$ となり同様に $\mathrm{Gal}(M_i/M_{i-1})$ は Abel なので M_i/M_{i-1} は Abel 拡大となる。

1 に対応する体は L より上記のことを $i = l$ まで行えば L/M_l まで Abel 拡大になるので有限次可解拡大 L/K は 有限次 Abel 拡大 M_i/M_{i-1} $(1 \leq i \leq l, M_0 = K, M_l = L)$ の繰り返しでできる拡大となっている。 $\square$

定理 3.8. 有限次 Galois 拡大 M/K について

$$M \text{ は } K \text{ の}{}^{\exists}\text{冪根拡大に含まれる} \Leftrightarrow M/K \text{ が可解拡大}$$

がなりたつので

$$\text{方程式 } f(X) = 0 \text{ が代数的に解ける} \Leftrightarrow K_0(\alpha_1, \ldots, \alpha_n)/K_0 \text{が可解拡大}$$

という代数方程式の可解性に関する必要十分条件が言える。

4 標数 素体

4.1 標数 素体

補題 4.1. 任意の環準同型写像 $f: R \longrightarrow S$ にたいして $\ker(f)$ は R のイデアルになる。
とくに、 S が整域のとき $\ker(f)$ は素イデアルである。

Proof. $G = \ker(f)$ とおく。$x, y \in G, f(x+y) = f(x) + f(y) = 0 + 0 = 0$ より加法について、$r \in R, x \in G, f(rx) = f(r)f(x) = r \cdot 0 = 0$ よりスカラー倍について閉じている。したがって R が環であることから $G = \ker(f)$ が R の部分加法群担っていることがわかる。そして $r \in R, x \in G, f(rx) = f(r)f(x) = 0$ より $rx \in G$ より $\ker(f)$ は R のイデアルになる。

S が整域のとき $x, y \in R$ にたいして $xy \in G$ であるとする。このとき $f(xy) = f(x)f(y) = 0$ で S が整域より $f(x) = 0$ または $f(y) = 0 \Rightarrow x \in G$ または $y \in G$ より $\ker(f)$ は素イデアルになる。 □

補題 4.2. $\mathbb{Z}$ は単項イデアル整域であり素イデアルは (0) もしくは $(p), (p$ は素数$)$ である。

Proof. $\mathbb{Z}$ はかけて 0 になるような元は 0 のみなので整域。

$\mathbb{Z}$ の任意のイデアル I をとり ${}^{\forall}m \in I$ に対して I 内の絶対値が最小で 0 でない元を n とすると、$m = k \cdot n + r, (0 \leq r < n)$ となる $k, r \in \mathbb{Z}$ が存在する。そして $m, kn \in I$ から $r = m - kr \in I$ となるが n の最小性から $r = 0$ となるので ${}^{\forall}m \in I, m = kn$ と表せる。よって $I = (n)$ であるから任意のイデアルは単項イデアルになる。逆に任意の元 n の倍数の集合 $n\mathbb{Z} := \{nk | k \in \mathbb{Z}\}$ は $\mathbb{Z}$ 加群であって $\mathbb{Z}$ の部分整域なので n によって生成される単項イデアル $n\mathbb{Z} = (n)$ となる。これより $\mathbb{Z}$ は単項イデアル整域である。

このときイデアルは $(0), (p), (m)$ の 3 つに分けられる。ただしここで $p > 0$ は素数であり $m > 0$ は合成数である。もし負の数による単項イデアルであったとしても絶対値の等しい値をとることで正の値にできる。

$xy \in (0) \Rightarrow xy = 0$ のとき整域より $x = 0$ または $y = 0$ となるので (0) は素イデアル。$xy \in (p) \Rightarrow {}^{\exists}k \in \mathbb{Z}, xy = pk$ となる。$k = k_1 \cdot k_2$ となる $k_1, k_2 \in \mathbb{Z}$ に対して $x = pk_1 \in (p), y = k_2$もしくは $x = k_1, y = pk_2 \in (p)$ であるから (p) は素イデアル。(m) に関しては $m = m_1 \cdot m_2$ となる $m_1, m_2 \in \mathbb{Z} - \{1\}$ に対して $m_1 m_2 \in (m)$ だが $m_1, m_2 \notin (m)$ より素イデアルではない。 □

定義 4.3. K:可換体 (可換環でもよい) に対して以下のような自然な環準同型写像 ϕ を考える。

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow K \\ n &\longmapsto n \cdot 1_K = \underbrace{1_K + \cdots + 1_K}_{n} \end{aligned}$$

ここで補題 (4.2) から $\mathbb{Z}$ は単項イデアル整域であるから補題 (4.1) から $\ker(\phi)$ は素イデアルなので p を素数として $\ker(\phi) = (0)$ もしくは (p) となる。

この 0 もしくは p を K の <u>標数 (characteristic)</u>といい $\mathrm{char}(K), \mathrm{Ch}(K)$ と書く。これは $\ker(\phi) = (p)$ のときこの p は $p \cdot 1_K = 0$ となるような最小の正整数である。

Proof. ϕ が環準同型写像になってることを確かめる。

この ϕ はまず $n = m$ のとき $\phi(n) = n \cdot 1_K = m \cdot 1_K = \phi(m)$ より写像になっている。そして $\phi(1) = 1 \cdot 1_K = 1_K, \phi(n+m) = (n+m) \cdot 1_K = \underbrace{1_K + \cdots + 1_K}_{n+m} = n \cdot 1_K + m \cdot 1_K = \phi(n) + \phi(m), \phi(n)\phi(m) =$

$(n\cdot 1_K)(m\cdot 1_K)=(\underbrace{1_K+\cdot+1_K}_{n})(\underbrace{1_K+\cdot+1_K}_{m})=\underbrace{1_K+\cdot+1_K}_{nm}=\phi(nm)$ であるから準同型写像になっている。

そして $\ker(\phi)=(p)=\{pl|l\in\mathbb{Z}\}$ から絶対値が p 以下の元は $\ker(\phi)$ に含まれないので p が $\ker(\phi)$ の 0 ではない元で絶対値が最小であるから $\phi(p)=0$ より p は $p\cdot 1_k=0$ となる最小の正整数。 □

定義 4.4. 任意の体 K は $\mathbb{Q}$ または $\mathbb{F}_p$ と同型な体を含む。この $\mathbb{Q},\mathbb{F}_p$ と同型な体のことを 素体 (prime field) という。

つまり素体とは真の部分体を含まない体とも言える。

Proof. 上記の設定で $\ker(\phi)=(0)$ のとき単射であるから $\mathrm{Im}(\phi)\cong\mathbb{Z}$ となり $\ker(\phi)=(p)$ のとき準同型定理から $\mathrm{Im}(\phi)\cong\mathbb{Z}/(p)=\mathbb{F}_p$ となる。よって K は体であるから $\mathbb{Z}$ を含む最小の体が $\mathbb{Q}$ で $\mathbb{F}_p$ は p 元体であることより $K\supset\mathrm{Im}(\phi)\cong\mathbb{Q}$ もしくは $\mathbb{F}_p$ より素体を含む。 □

系 4.5. $\mathrm{char}(K)=0$ の体 K の元は無限個存在する。

Proof. $\mathrm{char}(K)=0$ のとき $\mathbb{Q}$ と同型な体を含むので元の個数は少なくとも $\mathbb{Q}$ 以上であり $|\mathbb{Q}|=\infty$ より成立。 □

系 4.6. 有限体 K における素体は $\mathbb{F}_p$ と同型で K は $\mathbb{F}_p$ の有限次拡大であり拡大次数を n としたら $K\cong\mathbb{F}_p^n$ がなりたつ。そして有限体の元の個数は素数冪、つまり $|K|=p^n$ となる。$q=p^n$ として $K=\mathbb{F}_q$ とも書く。

Proof. 上記の系で K の元の個数が有限ならば $\mathrm{char}(K)\neq 0$ より $\mathrm{char}(K)=p>0$ であるので素体は $\mathbb{F}_p$ と同型。簡単のために素体を $\mathbb{F}_p$ と書くこととすると $K\supset\mathbb{F}_p$ であり $\mathbb{F}_p$ は K の演算で閉じているから K は $\mathbb{F}_p$ の拡大体。無限次拡大とすると基底が無限個あることになりそれは有限体であることに反するので $K/\mathbb{F}_p$ は有限次拡大。よって有限次拡大より拡大次数を n とすると $K\cong\mathbb{F}_p^n$ が成り立ち、$|K|=|\mathbb{F}_p^n|=|\mathbb{F}_p|^n=p^n$ より有限体の元の個数は素数冪になる。 □

4.2 Frobenius 自己準同型

定義 4.7. K が可換体で $\mathrm{char}(K)=p>0$ のとき以下は体の準同型でありこれを K の Frobenius 自己準同型という。

$$\begin{aligned}\phi: K&\longrightarrow K\\ a&\longmapsto a^p\end{aligned}$$

Proof. K が可換体であるから $\phi(ab)=(ab)^p=a^pb^p=\phi(a)\phi(b)$ より積に関しては準同型が成立。

同様に可換であるので $\phi(a+b)=(a+b)^p=\sum_{i=0}^{p}{}_pC_ia^ib^{p-i}$ となる。$0<i<p$ のとき ${}_pC_i=p!/i!(p-i)!=p\cdot(p-1)\cdots(p-i+1)/i\cdot(i-1)\cdots 2\cdot 1$ より p が係数にあるので $\mathrm{char}(K)=p>0$ よりその項は 0 になる。したがって $i=0,p$ の項だけ残るので $\phi(a+b)=(a+b)^p=a^p+b^p=\phi(a)+\phi(b)$ となるから結果として ϕ は体の自己準同型になっている。 □

定義 4.8. 体 K が 完全体 (perfect field)とは $\mathrm{char}(K)=0$ または $\mathrm{char}(K)=p>0$ で Frobenius$\phi: K\longrightarrow K$ が同型 (もともと体の準同型より全射であるということ)

($\Leftrightarrow K$ の非自明な非分離拡大が存在しない) これは示さない。

命題 4.9. 有限体は完全体。

Proof. 系 (4.6) より有限体 $K = \mathbb{F}_q$ にたいして Frobenius $\phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ は体の準同型より単射で有限集合より全射だから同型写像となるので有限体は完全体。 □

例 4.10. 逆に完全体ではない例として以下のようなものがある。

$(\sum a_j X^j / \sum b_i X^i) \in K = \mathbb{F}_p(X)$ $(X$: 変数$, a_j, b_i \in \mathbb{F}_p, \sum b_i X^i \neq 0)$ となっている $\mathbb{F}_p$ 上の有理関数体 K を考える。Frobenius $\phi : K \longrightarrow K, a \longmapsto a^p$ は p 乗準同型写像なのでまず $\mathbb{F}_p$ は完全体より全単射であるから係数は $\mathbb{F}_p$ の元全てを取るので像の有理関数体の係数は $\mathbb{F}_p$ のままである。そして準同型より $\phi(\sum a_j X^j / \sum b_i X^i) = \sum a_j^p (X^p)^j / \sum b_i^p (X^p)^i \in \mathrm{Im}(\phi) = \mathbb{F}_p(X^p) \subset K$ であるので全射ではない。したがって K は完全体ではない。

5　体上の代数

5.1　K-代数

定義 5.1. 環 A の中心 $Z(A)$ とは任意の A の元と可換な A の元でありつまり $Z(A) := \{x \in A | {}^{\forall}a \in A, ax = xa\}$ となる集合でありこれは A の部分環を成す。

Proof. 部分環を成すことを示す。

結合則や分配則は A が環であることより保証される。${}^{\forall}a \in A$ について単位元は定義より $a1 = a = 1a, a0 = 0 = 0a$ より中心に含まれる。また、${}^{\forall}x, y \in Z(A), a(x+y) = ax+ay = xa+ya = (x+y)a, a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$ より加法乗法について閉じているから $Z(A)$ は A の部分環である。 $\square$

定義 5.2. K:体とする。(可換環でもよい)

このとき $\underline{K-\text{代数}\ \ (K-\mathrm{algebra})}$ A とは以下の同値な条件のうち一つを、すなわち全てを満たすような零環にならないものである。

(1). 単位的環であって環準同型 $\phi : K \longrightarrow A$ が与えられており $\mathrm{Im}(\phi) \subset Z(A) = (A$ の中心$)$ となるもの。K が体であれば $\mathrm{Im}(\phi) = K \subset Z(A) \subset A$ とみなすことができる

(2). $K-$ 加群であり環としての構造を持ち、積が任意の $k \in K, x, y \in A$ にたいして $k(xy) = (kx)y = x(ky)$ が成り立つような $K-$ 双線型となるもの。

とくに K 倍できてそれが双線型であり K が体であれば $K-$ ベクトル空間とみなすこともできる。そして $[A : K] := \dim_K(A)$ を A の K 上の次数という。

$K-$ 代数 A を $K-alg, \phi : K \longrightarrow A$ と書くときもある。

Proof. 両方共環であることは共通しているから $\mathrm{Im}(\phi) \subset Z(A)$ と $K-$ 加群であり積が上記のように成り立つことが同値であることを示せば良い。

まずスカラー乗法を "$\cdot$" $: K \times A \longrightarrow A, (k, a) \longmapsto \phi(k)a$ と定めれば $ka := \phi(k)a$ とすることで K によるスカラー乗法が定義でき、これにより $K-$ 加群の構造を持つことができる。

また、$\mathrm{Im}(\phi) \subset Z(A)$ より A の結合則から ${}^{\forall}a, b \in A, k(ab) = \phi(k)(ab) = (\phi(k)a)b = (ka)b = (a\phi(k))b = (ak)b = a(\phi(k)b) = a(kb)$ より成り立つ。双線型であることも環 A の定義から明らか。

逆は環準同型 $\phi : K \longrightarrow A$ を適切につくれば $k(xy) = (kx)y = x(ky)$ より像は中心に含まれるので成り立つ。

K が体のとき Note (1.8) から ϕ が単射準同型より $K = \mathrm{Im}(\phi)$ と同一視できるため $K-$ 代数 A は実際に K を部分環として含んでいる。 $\square$

例 5.3. K を体としたときその多変数多項式環 $A := K[X_1, \ldots, X_n]$ は可換環で K 係数より $K - alg$ である。また、I を A のイデアルとしたときその剰余環 $K[X_1, \ldots, X_n]/I$ も同様の理由で $K - alg$ である。

L_i/K を K のある体拡大とするときその拡大の直積 $A := L_1 \times \cdots \times L_n$ はそれぞれの成分ごとに拡大体の演算によって L_i/K より $a \in K$ 倍を $(a, \ldots, a) \in K \times \cdots \times K$ と同一視することで $K - alg$ とみなせる。

以上の *2* つはもともと可換な構造の上であったのでそのまま中心に埋め込めたが $A = \mathrm{M}_n(K)$ とした行列

環は非可換でありこのときは以降のように定めることで非可換な $K-alg$ になる。すなわち、

$$\begin{aligned} K &\longrightarrow A \\ a &\longmapsto \begin{pmatrix} a & & \\ & \ddots & \\ & & a \end{pmatrix} \end{aligned}$$

となる環準同型でこの像は単位行列の定数倍なので A の中心に入るため $K-alg$ になる。

以下では $K-$ 代数は断らない限り全て可換であるとする。

定義 5.4. $K-alg, \phi: K \longrightarrow A, \psi: K \longrightarrow B$ があるとする。このとき $K-$ 代数の準同型 $\varphi: A \longrightarrow B$ とは環準同型であって $K-alg$ としての構造と可換なもの、つまり $\psi = \varphi \circ \phi$ となるもののこと。

これと同値なものとして φ が $K-$ 加群の準同型写像であることという定義でも良い。

Proof. 同値性を示す。

$\psi = \varphi \circ \phi$ となっているとき $^\forall x, y \in A, \varphi(xy) = \varphi(x)\varphi(y), \varphi(x+y) = \varphi(x) + \varphi(y)$ が環準同型であることより成り立つ。$k \in K$ について $K-alg$ のスカラー倍の定義から $\phi(k) \cdot 1 = k \in A, \psi(k) \cdot 1 = k \in B$ とみなせる。このとき $\varphi(k) = \varphi(\phi(k) \cdot 1) = \varphi \circ \phi(k) \cdot \varphi(1) = \varphi \circ \phi(k) = \psi(k) = \psi(k) \cdot 1 = k$ より K の元について不変となる。

□

5.2 元の添加

定義 5.5. L/K : 体の拡大、 $S : L$ の部分集合のとき、$K(S) := (S$ を含む最小の K の拡大体 $\subset L)$ と定義し、これを K 上 S で生成される部分体という。$S = \{a_1, \ldots, a_n\}$ なら $K(S) = K(a_1, \ldots, a_n)$ とも書く。

S, T と 2 つの L の部分集合があるときその 2 つのを含む最小の K の拡大体は集合 $S \cup T$ を含むと考えれば良いので $K(S \cup T) = K(S)(T) = K(T)(S)$ となりこれを $K(S, T)$ とも書く。

定義 5.6. L/K が有限生成とは $L = K(S)$ となる有限集合 $S \subset L$ が存在すること。

特に一元集合で生成されるとき L/K は<u>単生、単元生成 (monogenic)</u>という。

Rem 5.7. 有限次拡大 $\Rightarrow$ 有限生成

Proof. $[L : K] = n$ とするとき L の K 上の基底を $\{w_1, \ldots, w_n\}$ とする。$K(w_1, \ldots, w_n)$ はこの基底を含む体なので K 上の線形結合も含むことを考えればこれは L と一致するから有限生成。 □

ここで逆は成り立たない。$K(X), X$: 変数とするとこれは有理関数体で単生だが $1, X, \cdots, X^n, \cdots$ が全て異なるので K の無限次拡大となるような反例があるためである。

5.3 体の合成

定義 5.8. $M_1/K, M_2/K$: 体の拡大としたときこの 2 つの<u>合成、合成体、合成拡大 (a composite extension)</u>とは三組 (L, u_1, u_2) で

1. L は K の拡大体。

2. $u_i : M_i \longrightarrow L$ は K の拡大の準同型で L は $u_1(M_1) \cup u_2(M_2)$ により生成される。

となるようなもののことである。したがって写像のとり方の自由性から $M_1/K, M_2/K$ に対しこれらの合成はいくつもありえる。

系 5.9. $M_1/K, M_2/K$: 拡大で $(M_1 \otimes_K M_2)$ の極大イデアルを $\mathfrak{m}$ としたとき $L = (M_1 \otimes_K M_2)/\mathfrak{m}$ は K の拡大でありかつ M_1, M_2 を埋め込める。またこれより $(M_1 \otimes_K M_2)$ は $M_1 - alg, M_2 - alg$ である

Proof. 拡大の準同型を $u_i : K \longrightarrow M_i$ とする。そして $v_1 : M_1 \longrightarrow L, x \longmapsto u_1(x) \otimes 1 \mod \mathfrak{m}$ と $v_2 : M_2 \longrightarrow L, x \longmapsto 1 \otimes u_2(x) \mod \mathfrak{m}$ を考える。$(\mod \mathfrak{m})$ を除けば $M_1 - alg, M_2 - alg$ であることがわかる。これは体の準同型になるから単射でこれを拡大の準同型と取れば $L/M_1, L/M_2$ は拡大になり、$v_1 \circ u_1 = v_2 \circ u_2$ を満たし K の拡大でもある。

□

6　代数拡大

6.1　代数的、超越的

K : 体、 $A : K-$ 代数とする。

定義 6.1. $x \in A$ が K 上代数的、代数的数 (algebraic)とは

$$^{\exists} f\ (\neq 0)\ \in K[X] : K \text{ 係数多項式 } s.t.\ f(x) = 0$$

となることで代数的でないときこれを超越的、超越的数 (transcendental)という。

命題 6.2. $x \in A$ に対して以下は同値

(1) $1, x, x^2, \cdots$ が K 上一次独立ではない

(2) $K[x]$ が有限次元

(3) x は K 上代数的

Proof. $3 \Rightarrow 1$

x が代数的なので、ある $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ $(0 \neq a_i \in K)$ において $f(x) = \sum_{i=0}^{n} a_i x^i = 0$ より $1, x, x^2, \cdots$ は一次独立ではない。

$1 \Rightarrow 3$

一次独立でないのである有限な m で $\sum_{i=0}^{m} a_i x^i = 0$ となる全ては 0 ではない $a_i \in K$ が存在するのでこれを $f = \sum_{i=0}^{m} a_i X^i$ とすれば $f \in K[X], f(x) = 0$ となるため x は K 上代数的である。

$2 \Leftrightarrow 3$

$x \in A$ に対し写像 $\phi : K[X] \longrightarrow A, X \longmapsto x$ は環準同型であり、$^{\exists} f \in K[X], \ker(\phi) = (f)$ となる。このとき x : 代数的 $\Leftrightarrow$ $f \neq 0$ が定義より言える。したがって環準同型定理より $\mathrm{Im}\phi = K[x] \cong K[X]/(f)$ となる。そして $K[X]/(f)$ は $\deg(f) = n$ 以上の次数の多項式を割り算によりその次数以下にするから $K[X]/(f) = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} | a_i \in K\}$ で表せるので $K[x]$ も同型より有限次元である。

とくに $1, x, \cdots, x^{n-1}$ は $n-1$ 次以下の $K[x]$ の元が一次結合で表わせ、一次独立であるから K 上の $K[x]$ における基底となる。

□

定義 6.3. x が K 上代数的数のとき $f(x) = 0$ となる $f(\neq 0) \in K[X]$ のうち次数が最小で monic (最高次の係数が 1) であるものを x の K における最小多項式 (minimal polynomial) という。$\deg(f)$ を x の次数ともいう。

$f \in K[X]$ に対して $f = gh \Rightarrow f = g$ または $f = h$ となるとき f を既約多項式という。

例 6.4. $a \in \mathbb{Q}$ で平方数でないものにおいて $\sqrt{a} \in \mathbb{C}$ の $\mathbb{Q}$ の最小多項式は $X^2 - a \in \mathbb{Q}[X]$ である。

e, π は $\mathbb{Q}$ 上超越的である。

定義 6.5. K : 可換環、 $A : K - alg$ のとき $x \in A$ が K 上整 (integral)とは

$$^{\exists} f\ (\neq 0)\ \in K[X] : K \text{ 係数 monic 多項式 } s.t.\ f(x) = 0$$

となること。

例 6.6. $\sqrt{2}, 1/\sqrt{2}$ は $X^2-2, X^2-1/2$ を考えれば $\mathbb{Q}$ 上整。
しかし、 $1/\sqrt{2}$ は $\mathbb{Z}$ 上で代数的であるが $2X^2-1 \in \mathbb{Z}[X]$ の根で monic にならないので $\mathbb{Z}$ 上整ではない。

命題 6.7. K : 体、 $A : K-alg$ で $x \in A$ が代数的、その最小多項式を $f \in K[X]$ とする。
このとき以下が成立。
(1) $g \in K[X]$ について $g(x)=0 \Leftrightarrow f|g$
(2) $K[X]/(f) \xrightarrow{\sim} K[x], X(\mod f) \longmapsto x$ とできてとくに $1, x, \cdots, x^{n-1}$ は $K[x]$ の基底 $(n=\deg f)$
(3) $x \in A^\times \Leftrightarrow f(0) \neq 0$ でありこのとき $x^{-1} \in K[x]$

Proof. (1)
Euclid の割り算から $g=q\cdot f+r$ となる $q, r \in K[X], \deg r < \deg f$ がある。$g(x)=0$ より $q(x)f(x)+r(x)=r(x)=0$ となるが $\deg f$ の最小性から $r=0$ であるので $g=q\cdot f$ となるため $f|g$ である。
逆は $f|g \Rightarrow g=f\cdot(x$ の多項式$)$ で $f(x)=0$ より従う。
(2)
命題 (6.2) の (2) より従う。
(3)
$\Rightarrow$
$f=X^n+a_{n-1}X^{n-2}+\cdots+a_1X+a_0$ とする。$x \in A^\times$ より $f(x)=0$ から

$$-\frac{a_0}{x}=-(x^{n-1}+a_{n-1}x^{n-2}+\cdots+a_1)$$

であり $\deg f$ の最小性からこの右辺は $\neq 0$ なので $-a_0/x \neq 0 \Rightarrow a_0 \neq 0$ より $f(0)=a_0 \neq 0$ となる。
$\Leftarrow$
$f(0)=a_0 \neq 0$ とすると $a_0 \in K^\times$ より

$$1=x\cdot\frac{-(x^{n-1}+a_{n-1}x^{n-2}+\cdots+a_1)}{a_0}$$

となりこの $-(x^{n-1}+a_{n-1}x^{n-2}+\cdots+a_1)/a_0$ は $K[x]$ の元であり x の逆元 x^{-1} になるので $x \in A^\times$ と $x^{-1} \in K[x]$ が言えた。 □

6.2 代数拡大

定義 6.8. 体の拡大 L/K が<u>代数的 (algebraic)</u>とは ${}^\forall x \in L$ が K 上代数的であること。
<u>超越的 (transcendental)</u>とは代数的でないこと

Rem 6.9. L/K : 有限次拡大 $\Rightarrow$ L が代数的

Proof. ${}^\forall x \in L$ に対して $1, x, x^2, \cdots, x^n, \cdots$ を考えると $[L:K]$ が有限よりこれは K 上一次独立でないからある有限な n で $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ となるような全てが 0 ではない $a_0, \ldots, a_{n-1} \in K$ が存在する。よって $f=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$ とすればこれは x を根にもつ $f \in K[X]$ より x は代数的でしたがって L は代数的。 □

一般に逆は成り立たない。

例 6.10. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots)/\mathbb{Q}$ は代数的だが有限次ではない。

Fact 6.11. 後に示す $x \in K$ の最小多項式 f に対して $[K(x):K] = \deg_K f$ を認めれば $[\mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$ が示される。上記の例ではこれを用いれば有限次ではないことがわかる。

補題 6.12. $A : K - alg$ で整域とする。このとき $x \in A$ が K 上代数的ならば x は $K[x]$ で可逆。

Proof. x の最小多項式を f とすると命題 (6.7) の (2) より $K[x] \xrightarrow{\sim} K[X]/(f)$ である。$x \in A$ より $K[x] \subset A$ より $K[x]$ も整域だから $K[X]/(f)$ も整域。したがって (f) は素イデアルなので f は既約多項式より $f(0) \neq 0$ である。これより命題 (6.7) の (3) から $x \in A^{\times}, x^{-1} \in K[x]$ となる。 □

命題 6.13. L/K において次は同値。
(1) L/K は代数的
(2) L/K の任意の部分 $K - alg$ は体。

Proof. (1) ⇒ (2)
任意の部分 $K - alg, A$ をとる。これは $A \subset L$ より整域であるので補題 (6.12) より $^{\forall} x \in A \subset L$ に対して L/K が代数的で x が代数的なので x は $K[x] \subset A$ で可逆。したがって A は体。
(2) ⇒ (1)
L の任意の元 x をとる。このとき $K[x]$ は $K - alg$ より仮定から体なので $x^{-1} \in K[x]$ をもつ。よってある n 次多項式で $x^{-1} = a_n x^n + \cdots + a_1 x + a_0$ と書ける。$1 = x \cdot x^{-1} = a_n x^{n+1} + \cdots a_0 x$ で $a_n \in K^{\times}$ より $f = X^{n-1} + \cdots a_0/a_n X - 1/a_n$ とすればこれは $f \in K[X]$ で $f(x) = 0$ となるから x は K 上代数的。よって L/K は代数的。 □

命題 6.14. L/K において $x \in L$ が K 上代数的ならばその最小多項式を f として $K[x] = K(x) \cong K[X]/(f)$ であり、$[K(x):K] = \deg_K(x)$ となる。

Proof. 命題 (6.13) と (6.7) より $K[x]$ は体であり $K[x] \cong K[X]/(f)$ で $\dim_K K[x] = n = \deg f$ が成り立つ。よって体 $K(x) = \{q(x) | q(X) \in K[X]\}$ の定義より $K(x) = K[x]$ となる。そして $\dim_K K[x] = \dim_K K(x) = [K(x):K] = n = \deg_K f$ である。 □

系 6.15. L/K : 有限次拡大は $L = K(a_1, \ldots, a_r), (a_i \in L)$ の形で $K \subset K(a_1) \subset \cdots \subset K(a_1, \ldots, a_r) = L$ と体の拡大の列ができる。
a_i の $K(a_1, \ldots, a_{i-1})$ 上の拡大次数を n_i とし最小多項式を $f_i \in K(a_1, \ldots, a_{i-1})[X]$ とすると $[L:K] = n_1 \cdots n_r$ で $\{a_1^{\nu_1} \cdots a_r^{\nu_r} | 0 \leq \nu_i \leq n_i\}$ は L の K 上の基底となる。

$$L \cong \left(\left(\left(\frac{K[X_1]}{(f_1)} \right) [X_2]/(f_2) \right) \cdots \right) [X_r]/(f_r)$$

が成り立つ。

Proof. 命題 (6.14) を繰り返し用いれば良い。 □

補題 6.16. K 上代数的数 x, y に関して、 $x + y, xy, x - y$ も代数的であり、y が 0 で無いのなら x/y も代数的である。

Proof. $x + y, xy, x - y, xy \in K(x, y)$ であり、x, y の最小多項式をそれぞれ f, g とするとともに有限次。したがって $K(x, y) = K(x)(y)$ は拡大次数が最小多項式の次数と等しいことから有限次拡大である。よって K

上の代数拡大であるのでそこに含まれる元は K 上代数的。 □

命題 6.17. $L/M/K$ を拡大の列とするとき以下が成り立つ。

$$L/K \text{ が代数的} \Leftrightarrow L/M, M/K \text{ がともに代数的}$$

Proof. $(\Rightarrow)$ は $M \supset K$ より明らか。

$(\Leftarrow)$

$^\forall x \in L$ が K 上代数的であることを示す。x は M 上代数的なので $^\exists f = \sum_{i=0}^{n} a_i X^i \in M[X], f(x) = 0$ となる。また、 $a_i \in M$ よりこれは K 上代数的であるので命題 (6.14) で L を M と、 x を a_i とみれば $K' = K[a_0, \ldots, a_n]$ は体で $K(a_0, \ldots, a_n)$ と等しい。したがって K の有限次拡大であり $f \in K'[X]$ で x は K' 上代数的である。同様に命題 (6.14) から $K'[x] \cong K'[X]/(f)$ となる。ここでこの右辺は命題 (6.7) の (2) から $\dim_{K'} K'[X]/(f) = n$ なので左辺は K' 上有限次拡大。そして K' は K 上有限次拡大であったので $K'[x]$ は K 上有限次拡大。したがって Rem(6.9) より $K'[x]/K = K[a_1, \ldots, a_n, x]/K$ は代数拡大なので $x \in K'[x] \subset L$ は K 上代数的。 □

命題 6.18. $M_1/K, M_2/K$: 代数拡大 $\Rightarrow$ 任意の合成拡大 (L, u_1, u_2) は K 上代数的

Proof. $^\forall x \in M_1$ は K 上代数的より最小多項式 $f = \sum_{i=0}^{n} a_i X^i, f(x) = 0$ が存在する。そして u_1 は $K-$準同型より $0 = u_1(f(x)) = u_1(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} u_1(a_i) u_1(x)^i = \sum_{i=0}^{n} a_i u_1(x)^i = f(u_1(x))$ となるから $u_1(x)$ は K 上代数的になる。u_2 も同様に考えると $u_1(M_1), u_2(M_2)$ は K 上代数的である。補題 (6.16) よりこの集合間の四則演算は全て代数的なので $L = K(u_1(M_1), u_2(M_2))$ は代数的である。 □

定義 6.19. L/K : 拡大とする。

K の L の中での<u>相対的代数閉包</u> M とは

$$M := \{x \in L | x \text{ は } K \text{ 上代数的 }\}$$

となるもの。これを $\overline{K}$ と書くこともある。

また、 K が <u>L の中で (相対的に) 閉じている</u>とは $K = M$ となること。

命題 6.20. 上の定義における相対的代数閉包 M は体。

Proof. 補題 (6.16) より和と積について M は閉じている。

$K(x) \subset M$ であり、 $K(x)$ は x を含む最小の L の部分体より $x^{-1}, -x \in K(x) \subset M$ なので逆元も存在する。 □

例 6.21. K の $K(X)$ (X は変数) の中での相対的代数閉包は X は変数なのでそれが含まれると K 上代数的でなくなるため K である。

$\mathbb{R}$ の $\mathbb{C}$ の中での相対的代数閉包は $\mathbb{C}$ と一致するが $\mathbb{Q}$ の $\mathbb{C}$ の中での相対的代数閉包 $\overline{\mathbb{Q}}$ は $\mathbb{C}$ と一致しない。

7　代数閉体、分解体、代数閉包

7.1　代数閉体

命題 7.1. 体 K について次は同値。

(AC1) $^\forall f \in K[X] - K$ は $K[X]$ において一次の積に分解できる。

(AC2) $^\forall f \in K[X] - K$ は K において少なくとも一つの根を持つ。

(AC3) 任意の $K[X]$ の既約多項式は一次。

(AC4) K の代数拡大は K のみ。

Proof. (1) $\Rightarrow$ (2)

一次の積に分解できればそれが根になるので明らか。

(2) $\Rightarrow$ (1)

f のある根を $k \in K$ とすると $f(X) = (X-k)g(X)$ となる $g \in K[X]$ がある。この g に対しても同様なことをして繰り返せば $f = (X-k_1)(X-k_2)\cdots(X-k_n)$ と一次の積に分解できる。

(1) $\Leftrightarrow$ (3)

K 上の既約多項式はそれ以上 $K[X]$ 上で分解できない多項式なので全ての $f \in K[X] - K$ が一次に分解できるので既約多項式は一次。また、分解は既約多項式まで分解できるので一次の積に分解できる。

(3) $\Rightarrow$ (4)

任意の代数拡大 L/K をとると $^\forall x \in L$ に対し最小多項式 $f \in K[X]$ がある。これは既約多項式なので (3) より $f(x) = x - k, k \in K$ となっているから $x = k \in K$ より $L = K$ なので代数拡大は K のみ。

(4) $\Rightarrow$ (1)

任意の $f \in K[X] - K$ における任意の既約成分を g とする。g のある一つの根を x とするとこの元は K 上代数的であるから $[K(x) : K] = \deg_K g$ で有限次拡大なので $K(x) \cong K[X]/(g)$ は K 上の代数拡大。(4) よりこれは K なので $\deg_K g = \dim_K(K[X]/(g)) = \dim_K K = 1$ だから $\deg_K g = 1$ より一次式になる。よって任意の既約成分が一次式になるので $f = (\text{一次の積})$ となる。 □

定義 7.2. 体 K が上記の命題 (7.1) の (AC1) $\sim$ (AC4) を成り立たせる、つまり全てを満たすとき K を代数閉体 (algebraically closed)という。

相対的代数閉包とはことなり K を含む上の体が最初からは無い。

例 7.3. 代数学の基本定理は $\mathbb{C}$ が代数閉体であることを述べている。

命題 7.4. Ω/K : 拡大、 Ω : 代数閉体とする。このとき K の Ω の中での相対的代数閉包 $\overline{K}$ は代数閉体。

Proof. $\overline{K}$ が (AC2) を満たすことを示す。

$^\forall f = \sum_{i=0}^n a_i X^i \in \overline{K}[X] - \overline{K} \subset \Omega[X] - \Omega$ は Ω が代数閉体よりある根 $x \in \Omega$ が存在する。$a_i \in \overline{K}$ より K 上代数的だからそれぞれの最小多項式の次数を考えれば $K' = K(a_0, \ldots, a_n)$ は K 上有限次拡大。x は K' 上代数的より $K'(x)$ は K' 上有限次拡大。この有限次拡大を合わせれば $K(a_0, \ldots, a_n)(x)/K = K(a_0, \ldots, a_n, x)/K$ は有限次拡大なので代数拡大。よって x は K 上代数的なので $x \in \overline{K}$ より $\overline{K}$ に少なくとも一つの根を持っている。 □

定理 7.5. Steinitz の定理

$L/K, \Omega/K$: 拡大とし、 L は代数拡大、 Ω は代数閉体とする。このときある K の拡大の準同型写像 $\varphi : L \longrightarrow \Omega$ が存在する。(任意の代数拡大はΩに埋め込める)

Proof. 系 (5.9) から $\Omega' := (L \otimes_K \Omega)/\mathfrak{m}$ は L, Ω の拡大体である。

この拡大の準同型を $\phi : L \longrightarrow \Omega', \psi : \Omega \longrightarrow \Omega'$ とするとれは体の準同型より単射。単射準同型なのでそれぞれの像において構造を保つことを考えれば $\phi(L)$ は $\phi(K)$ 上代数拡大、 $\psi(\Omega)$ は代数閉体。よって $\psi(K)$ 上代数的な元を $\psi(\Omega)$ はすべて含む。また写像が可換より $\psi(K) = \phi(K)$ なので $\psi(\Omega)$ は $\phi(K)$ 上代数的な元をすべて含む。よって $\phi(L) \subset \psi(\Omega)$ で単射なので $\psi^{-1}\phi : L \longrightarrow \Omega$ となる体の準同型をつくれる。 □

7.2 分解体

定義 7.6. K : 体で $(f_i)_{i \in I}$: 多項式の族 $(f_i \in K[X] - K)$ に対し、K の拡大体 L が $(f_i)_{i \in I}$ の最小分解体 (minimal spilitting field) (もしくはここでは MS 体) とは以下の条件を満たすものである。

(1) $^\forall i \in I, f_i$ は $L[X]$ で一次の積に分解される。(ここではこの条件が成り立つものを分解体という)

(2) $L = K(^\forall i \in I, ^\forall f_i \text{の根})$ となる、つまり f_i の根で K 上生成される最小の体であること。

Rem 7.7. $(f_i) = (f_1, \dots, f_n)$ のように有限個の多項式の場合、$f = f_1 \cdots f_n$ とすると (f_i) の MS 体 $=$ f の MS 体である。

命題 7.8. $^\forall (f_i)_{i \in I}$ に対しその MS 体は存在し、それは K 上の同型を除き一意的である。