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 $f=a_0+a_1x+\cdots+a_nx^n$ 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 の中間体 (intermediate field)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 による固定部分体という。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。$x_0 x$ 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 $\mathrm{Hom}_{K\text{の拡大}}(M,L) \longrightarrow \mathrm{Hom}_{K-\text{ベクトル空間}}(M,L)$ 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 $|\mathrm{Hom}_{K\text{の拡大}}(M,L)|$ は有限で $|\mathrm{Hom}_{K\text{の拡大}}(M,L)| \leq [M:K]$ 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 $z = \sum_{ij} a_ij(f_i\otimes l_j), a_{ij} \in K$ と書ける。そして定義から $\theta(z)(m) = \sum_{ij} a_ij(f_i(m)l_j)$ 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 $\theta(z)(m_i) = \sum_j a_ijl_j$ 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

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

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、 $\alpha_j \in (K_0$の$^{\exists}$冪根拡大$)$ ということ。または、 $K_0(\alpha_1, \ldots, \alpha_n) \subset (K_0$の$^{\exists}$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 (commutator subgroup) (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 $(G, G) \triangleleft G$ 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 $G_i \triangleleft G_{i-1}$ 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。 □

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 の部分加法群にな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幂、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幂になる。 □

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 $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$ より積に関しては準同型が成立。

同様に可換であるので $\phi(a+b) = (a+b)^p = \sum_{i=0}^{p} {}_pC_i a^i b^{p-i}$ 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。 □

定義 5.2. K:体とする。(可換環でもよい)

このとき $\underline{K-\text{ 代数 } (K-\text{algebra})}$ 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 $\mathrm{Im}(\phi) \subset Z(A) = (A \text{ の中心})$ 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。 □

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環準同型 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) $\Rightarrow$ (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) $\Rightarrow$ (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。 $\square$

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。 $\square$

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。 $\square$

命題 6.19. $M_1/K, M_2/K$:

定義 6.20. L/K : 拡大とする。

K の L の中での<u>相対的代数閉包 (relative algebraic closure)</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 6.21. 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。 $\square$

例 6.22. 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 = $ (一次の積) となる。 □

定義 7.2. 体 K が上記の命題 (7.1) の (AC1) ∼ (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 $K' = K(a_0, \dots, a_n)$ 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 $K(a_0, \dots, a_n)(x)/K = K(a_0, \dots, a_n, x)/K$ 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 $\phi : L \longrightarrow \Omega', \psi : \Omega \longrightarrow \Omega'$ とするとこ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) $L = K(\forall i \in I, \forall f_i の根)$ 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. $(f_i) = (f_1, \ldots, f_n)$ 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. K 上の多項式の族 $\forall(f_i)_{i\in I}$ 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。

Proof. $(f_i)_{i\in I} = (f)$ のときを考える。体上の多項式なので最高次の係数を 1 にしても一般性を失わない。$f = X^n + \sum_{i=1}^n a_i X^{n-i}, a_i \in K$ とおき、$A_i := K[X_1, \ldots, X_n]/I$ を考えるとこれは $K - alg$ である。ただしここで I とは $K[X_1, \ldots, X_n]$ において $s_k - (-1)^k a_k$ $(k = 1, \ldots, n)$ で生成されるイデアルとする。s_k は $X_1, \ldots, X_n$ の k 次基本対称式でありつまり $(X - X_1)\cdots(X - X_n) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$ を満たすものである。$x_j := X_j \mod I = X_j + I$ とおき、x_j の k 次基本対称式を上と同様に t_k とするとき $t_k = s_k + I$ であり、$s_k - (-1)^k a_k \in I \Leftrightarrow s_k + I = (-1)^k a_k + I$ なので

$$\begin{aligned}
(X - x_1)\cdots(X - x_n) &= X^n - t_1 X^{n-1} + \cdots + (-1)^n t_n \\
&= X^n + \sum_{i=1}^n (-1)^i t_i X^{n-i} \\
&= X^n + \sum_{i=1}^n (-1)^i (s_i + I) X^{n-i} \\
&= X^n + \sum_{i=1}^n (-1)^i ((-1)^k a_k + I) X^{n-i} \\
&= X^n + \sum_{i=1}^n (a_k + I) X^{n-i} \\
&= X^n + (a_1 + I) X^{n-1} + \cdots + (a_n + I)
\end{aligned}$$

となる。これより f は $A_i[X]$ において $f = (X - x_1)\cdots(X - x_n)$ と分解される。A_i の任意の極大イデアル $\mathfrak{m}$ に対し $L_i = A_i/\mathfrak{m}$ とおくとこれは体で標準的射像を考えれば f は $L[X]$ 上で一次の積に分解される。f の根が $x_1, \ldots, x_n (= X_1, \ldots, X_n \mod I)$ より A_i の作り方からこの L_i は (f) の MS 体である。

一般の $(f_i)_{i\in I}$ に対しては $L := (\otimes_{i\in I} A_i)/(\text{極大イデアル})$ とするとこれは体で (f_i) の MS 体なので存在性が示された。

一意性は定義 (2) より従う。 □

7.3 代数閉包

定義 7.9. 体 K の代数閉包 (algebraic closure)とは K の代数拡大であって代数閉体であるもののこと。これを代数閉な拡大ともいう。

つまり、任意の元に対して最小多項式が存在して、さらに任意の多項式に対してその根が全て含まれる体である。

命題 7.10. Steinitz の定理

任意の体 K に対しその代数閉包が存在してそれは K 上の同型を除き一意的。

Proof. $(f_i)_{i\in I} = K[X] - K$ として命題 (7.8) を適用すればよい。 □

系 7.11. K, K' : 体、 Ω, Ω' : それらの代数閉包としたとき同型 $\psi : K \xrightarrow{\sim} K'$ に対しそれを延長する同型 $\phi : \Omega \xrightarrow{\sim} \Omega'$ が存在する

Proof. 前述の命題 (7.10) の証明より代数閉包は $(f_i)_{i\in I} = K[X] - K \cong K'[X] - K'$ の MS 体なのでその一意性から同型 $\phi : \Omega \xrightarrow{\sim} \Omega'$ が存在する。 □

8 etale 代数

8.1 対角化

以下ではとくに述べない限り K を可換体とする。

定理 8.1. $A : K-alg$ と L/K : 拡大としたときに集合 $\mathscr{H} := \mathrm{Hom}_{K-alg}(A,L)$ は $L-$ ベクトル空間 $\mathrm{Hom}_{K-vect.sp}(A,L)$ の中で L 上一次独立。

Proof. A を $K-vect.sp$ として見ればこれは加法群であるので Dedekind の補題から従う。 □

補題 8.2. $\dim_L(\mathrm{Hom}_{K-vect.sp}(A,L)) = [\mathrm{Hom}_{K-vect.sp}(A,L) : L] = [A : K]$ が成り立つ。

Proof. $A_{(L)} := L \otimes_K A$ としてその双対空間を $(A_{(L)})^* := \mathrm{Hom}_L(A_{(L)}, L)$ とする。以下簡単のため $\mathrm{Hom}_{K-vect.sp}(A,L)$ を $\mathrm{Hom}(A,L)$ と書く。$\overline{\cdot} : (A_{(L)})^* \longrightarrow \mathrm{Hom}(A,L), u \longmapsto \overline{u}$ で $\overline{u} : A \longrightarrow L, x \longmapsto \overline{u}(x) = u(1 \otimes x)$ とすればこの $\overline{\cdot}$ は同型であり双対空間であることから $\dim_L A_{(L)} = \dim_L (A_{(L)})^* = \dim_L \mathrm{Hom}(A,L)$ である。$\dim_L A_{(L)} = \dim_K A$ より従う。 □

系 8.3. 上の状況において $h(L)(= h_A(L)) := |\mathrm{Hom}_{K-alg}(A,L)| \leq [A : K]$ が成り立つ。

Proof. $\mathrm{Hom}_{K-alg}(A,L)$ は $\mathrm{Hom}_{K-vect.sp}(A,L)$ で一次独立より $h(L) \leq \dim_L(\mathrm{Hom}_{K-vect.sp}(A,L))$ である。補題 (8.2) の $\dim_L(\mathrm{Hom}_{K-vect.sp}(A,L)) = [A : K]$ より従う。 □

定義 8.4. $K-alg$ の A が<u>対角化可能 (diagonalizable)</u>とは $^\exists n \geq 1, A \cong K^n$ であること。とくに $n = [A : K]$ である。K^n は成分ごとの演算を行う直積代数である。

Proof. $n = [A : K]$ であることは A を $K-$ ベクトル空間と見ることからわかる。 □

定義 8.5. A が拡大 L/K により<u>対角化される (diagonaled by L)</u>とは $L-alg$ の $L \otimes_K A$ が対角化可能であること。

定義 8.6. A が K 上<u>etale</u>とは $^\exists$拡大 L/K により対角化されること。

Rem 8.7. $(e_1, \ldots, e_n)$ が $K^n(\cong A)$ の標準基底とすると成分ごとの演算を行うから $e_i^2 = e_i, e_i e_j = 0 (i \neq j), e_1 + \cdots + e_n = 1_A$ となる。

命題 8.8. 有限次 $K-alg$ A について次は同値 ($n = [A : K]$ とする)

(1) A は対角化可能。

(2) A の K 上の基底 $(e_1, \ldots, e_n)$ で $e_i^2 = e_i, e_i e_j = 0 (i \neq j)$ を満たすものが存在する。

(3) $\mathrm{Hom}_{K-alg}(A,K)$ は $\mathrm{Hom}_{K-vect.sp}(A,K)$ を生成する。

Proof. (1) $\Rightarrow$ (2) は Rem (8.7) より成立。

(2) $\Rightarrow$ (1)

$A_i = Ke_i$ とすると $A_i \cong K$ で $A = \{k_1 e_1 + \cdots + k_n e_n | k_i \in K\} = A_1 \times \cdots \times A_n \cong K^n$ より対角化可能。

(3) $\Rightarrow$ (1)

有限次 $K-alg$ なので $\mathrm{Hom}_{K-alg}(A,K) = \{\pi_1, \ldots, \pi_n\}$ とする。これは定理 (8.1) より一次独立で

仮定から全体を張るので $\mathrm{Hom}_{K-vect.sp}(A,K)$ の基底になる。そしてそれを並べた $K-$ 代数の準同型 $\pi := (\pi_1,\ldots,\pi_n) : A \longrightarrow K^n, a \longmapsto (\pi_1(a),\ldots,\pi_n(a))$ とする。 □

系 8.9. 系 (8.3) における $|\mathrm{Hom}_{K-alg}(A,L)| \leq [A:K]$ について

$$|\mathrm{Hom}_{K-alg}(A,L)| = [A:K] \Leftrightarrow A \text{ は } L \text{ で対角化される。}$$

Proof. $\pi : \mathrm{Hom}_{K-vect.sp}(A,L) \longrightarrow \mathrm{Hom}_{L-vect.sp}(L\otimes_K A, L), u \longmapsto \pi u$ とし、$L-$ 線形写像で $\pi u : A_{(L)} \longrightarrow L, (1\otimes x) \longmapsto (\pi u)(1\otimes x) := u(x)$ とする。π は準同型で $\pi u = 0 \Rightarrow {}^{\forall}x \in A, u(x) = 0 \Leftrightarrow u = 0$ で単射。${}^{\forall}v \in \mathrm{Hom}_{L-vect.sp}(A_{(L)},L), u(x) := v(1\otimes x)$ とおけば $\pi u = v$ となるので全射より π は同型なので $\dim_L \mathrm{Hom}_{K-vect.sp}(A,L) = \dim_L \mathrm{Hom}_{L-vect.sp}(L\otimes_K A, L)$ が成立する。

また、始域と終域を代数の準同型に制限して $\pi : \mathrm{Hom}_{K-alg}(A,L) \longrightarrow \mathrm{Hom}_{L-alg}(L\otimes_K A, L)$ でも同様に全単射になるから $|\mathrm{Hom}_{K-alg}(A,L)| = |\mathrm{Hom}_{L-alg}(L\otimes_K A, L)|$ である。

命題 (8.8) の (1) $\Leftrightarrow$ (3) で A を $L\otimes_K A$ で置き換えて、補題 (8.2) も用いれば

$$\begin{aligned}
A \text{ は } L \text{ で対角化される} &\Leftrightarrow L\otimes_K A \text{ は対角化可能}\\
&\Leftrightarrow \mathrm{Hom}_{L-alg}(A_{(L)},L) \text{ は } \mathrm{Hom}_{L-vect.sp}(A_{(L)},K) \text{ を生成する。(基底になる)}\\
&\Leftrightarrow |\mathrm{Hom}_{L-alg}(A_{(L)},L)| = \dim_L \mathrm{Hom}_{L-vect.sp}(A_{(L)},K)\\
&\Leftrightarrow |\mathrm{Hom}_{K-alg}(A,L)| = |\mathrm{Hom}_{L-alg}(A_{(L)},L)|\\
&\qquad = \dim_L \mathrm{Hom}_{L-v.s}(A_{(L)},L) = \dim_L \mathrm{Hom}_{K-v.s}(A,L) = [A:K]\\
&\Leftrightarrow |\mathrm{Hom}_{K-alg}(A,L)| = [A:K]
\end{aligned}$$

□

命題 8.10. $K-alg\ A$ について次は同値。

(1) A は K 上 etale である。(:$\Leftrightarrow$ ${}^{\exists}$拡大により対角化される)

(2) A は K の ${}^{\exists}$<u>有限次</u>拡大により対角化される。

(3) A は K の ${}^{\forall}$<u>代数閉</u>な拡大により対角化される。

(4) A は K の ${}^{\exists}$<u>代数閉</u>な拡大により対角化される。

Proof. (3) $\Rightarrow$ (4) $\Rightarrow$ (1) は明らか。

(1) $\Rightarrow$ (2) $\Rightarrow$ (3) を示す。

(1) $\Rightarrow$ (2)

(1) :$\Leftrightarrow$ ${}^{\exists}L/K$ により対角化される。系 (8.9) から $|\mathrm{Hom}_{K-alg}(A,L)| = [A:K] = n$ となる。$\mathrm{Hom}_{K-alg}(A,L) = \{\phi_1,\ldots,\phi_n\}$ とすると $\phi_i(A)$ は L の部分体で対角化可能だから $\phi_i(A)\otimes_K A \subset L\otimes_K A \cong K^n$ より $\phi_i(A)$ は K 上 n 次以下。よって $M := (\phi_i(A)$ たちの合成$)(\subset L)$ も K の有限次拡大となり、$\mathrm{Im}(\phi_i) \subset M$ より終域を制限することができるから $\mathrm{Hom}_{K-alg}(A,M) = \{\phi_1,\ldots,\phi_n\}$ である。系 (8.9) より $|\mathrm{Hom}_{K-alg}(A,M)| = [A:K]$ だから A は K 上有限次拡大の M で対角化されるから (2) が示された。

(2) $\Rightarrow$ (3)

A はある有限次拡大 M で対角化されるとする。有限次拡大より Rem (6.9) から M は代数拡大でもある。また、K の任意の代数閉体 Ω をとると定理 (7.5)(Steinitz の定理) から M は Ω に埋め込める。よって $\mathrm{Hom}_{K-alg}(A,M) \subset \mathrm{Hom}_{K-alg}(A,\Omega)$ である。ここで対角化されるので系 (8.9) から $|\mathrm{Hom}_{K-alg}(A,M)| = [A:K]$ になることと系 (8.3) から $|\mathrm{Hom}_{K-alg}(A,\Omega)| \leq [A:K]$ より

$|\operatorname{Hom}_{K-alg}(A,M)| = |\operatorname{Hom}_{K-alg}(A,\Omega)| = [A:K]$ となる。よって A は任意の代数閉体 Ω で対角化される。 □

8.2 etale 代数の部分代数

以下では etale 代数 $A = K^n$ とし、その標準基底を $\{e_1,\dots,e_n\}$ とする。

命題 8.11. $[n] := \{1,\dots,n\}$ でこれを共通部分が無いように $[n] = I_1 \bigsqcup \cdots \bigsqcup I_r$ $(I_j \neq \emptyset)$ と分割する。$I \subset [n]$ に対して $e_I := \sum_{i\in I} e_i$ とする。$[n] = I_1 \bigsqcup \cdots \bigsqcup I_r$ に対し、$A_{(I_1,\dots,I_r)} := Ke_{I_1} + \cdots + Ke_{I_r}$ は A の部分 $K-alg$ である。

そして A の任意の部分 $K-alg$ は対角化可能で $A_{(I_1,\dots,I_r)}$ のもので尽き、とくに有限個である。

Proof. e_{I_j} が $A_{(I_1,\dots,I_r)}$ の標準基底になること。

$A_{(I_1,\dots,I_r)}$ の定義より全体を張り、一次独立性も保つ。e_i は標準基底より打ち消し合って冪等元より $I_k \neq I_l$ とするとき

$$e_{I_k}^2 = \left(\sum_{i\in I_k} e_i\right)^2 = \sum_{i\in I_k} e_i^2 = e_{I_k}$$
$$e_{I_k}e_{I_l} = \left(\sum_{i\in I_k} e_i\right)\left(\sum_{i\in I_l} e_i\right) = 0$$
$$e_{I_1} + \cdots + e_{I_r} = \sum_{i\in[n]} e_i = 1$$

より標準基底になるのでそれで K 上張られている $A_{(I_1,\dots,I_r)}$ は A の部分 $K-alg$ であり、命題 (8.8) の (2) から対角化可能である。

また、 B を A の任意の部分代数とするとき射影

$$v_i : A(=K^n) \longrightarrow K$$
$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \longmapsto a_i$$

の定義域を B に制限したものを考える。これを再度 v_i とおくときこれは $v_i \in \operatorname{Hom}_{K-alg}(B,K)$ である。

$$\alpha = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \beta = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in B, k \in K$$

とするとき $v_i(\alpha+\beta) = a_i + b_i = v_i(\alpha) + v_i(\beta), v_i(\alpha\beta) = a_ib_i = v_i(\alpha)v_i(\beta), v_i(k\alpha) = ka_i = kv_i(\alpha), v_i(1_{K^n}) = 1_K$ より $v_i \in \operatorname{Hom}_{K-alg}(B,K)$ である。そして定義より $v_i(e_j) = \delta_{ij}$ なので $\{v_1,\dots,v_n\}$ は $\operatorname{Hom}_{K-vect.sp}(B,K)$ を生成する。つまり、$f \in \operatorname{Hom}_{K-vect.sp}(B,K)$ に対して $v_i(c_1e_1+\cdots+c_ne_n) = c_i$ より $f = f(e_1)v_1 + \cdots + f(e_n)v_n$ とすればよい。

したがって $\operatorname{Hom}_{K-alg}(B,K)$ の元 $v_1,\dots,v_n$ が $\operatorname{Hom}_{K-vect.sp}(B,K)$ を生成するので命題 (8.8) から任意の部分代数は対角化可能である。また、基底として $(\varepsilon_1,\dots,\varepsilon_m)$ で $\varepsilon_i^2 = \varepsilon, \varepsilon_i\varepsilon_j = 0 (i \neq j)$ となるものが存在する。

この基底は A の元なので $e_1,\dots,e_n$ で作られるが冪等性と総和が 1 になることを考えれば $e_{I_1},\dots,e_{I_r}$ で出し尽くされる。したがって全ての部分代数は $A_{(I_1,\dots,I_r)}$ であり、$[n]$ の分割を考えれば部分代数は有限個。 □

命題 8.12. 各 $I \subset [n]$ に対し $\mathfrak{a}_I := \sum_{i\in I} Ke_i$ とするとこれは A のイデアルになる。そして A のイデアルはこれに尽き、とくに有限個である。

Proof. $\mathfrak{a}_I$ は明らかに A のイデアルになる。

A のイデアル $\mathfrak{a}$ が $^\forall i \in I, e_i \in \mathfrak{a}$ で $^\forall j \in J := [n]-I, e_j \notin \mathfrak{a}$ となっているとする。定義より明らかに $\mathfrak{a}_I \subset \mathfrak{a}$ である。$x = x_1e_1 + \cdots + x_ne_n \in \mathfrak{a}, x_i \in K$ と $j \in J$ に対して $e_j \in A, x \in \mathfrak{a}$ から $xe_j \in \mathfrak{a}$ なので $xe_j = x_1e_1e_j + \cdots + x_ne_ne_j = x_je_j \in \mathfrak{a}$ となる。ここで $x_j = 0$ のとき $x_je_j = 0_{K^n} \in \mathfrak{a}$ である。$x_j \neq 0$ のとき $x_je_j \in \mathfrak{a}$ とすると K が体より x_j^{-1} が存在して、$x_j^{-1}e_j \in A$ であるからイデアルより $x_j^{-1}e_jx_je_j = e_j \in \mathfrak{a}$ となり、これは矛盾。したがって $x_je_j \in \mathfrak{a}$ であるときは $x_j = 0$ である。これより $x \in \mathfrak{a}$ は $\sum_{i\in I} x_ie_i$ とかけるから $\mathfrak{a} \subset \mathfrak{a}_I$ なので $\mathfrak{a} = \mathfrak{a}_I$。任意のイデアルはそれが含んでいる標準基底によってのみ決まるから $\mathfrak{a}_I$ で全てであり I のとり方より有限個である。 □

Rem 8.13. $A = K^n$ のイデアル $\mathfrak{a}$ はそれ自身は $K - alg$ の構造を持つが、一般に A の部分 $K - alg$ ではない。また、 $\mathfrak{a} = \mathfrak{a}_I$ は A のイデアル $\mathfrak{b} = \mathfrak{a}_J = \mathfrak{a}_{[n]-I}$ の商 $K - alg$ $A/\mathfrak{b}$ と同型である。

Proof. $K - alg$ の構造を持つことは $\mathfrak{a} = \mathfrak{a}_I$ で $I = \{1,\dots,k(\neq n)\}$ とすると

$$\begin{aligned} \phi : K &\longrightarrow \mathfrak{a} \\ k &\longmapsto \begin{pmatrix} k \\ \vdots \\ k \\ 0 \\ \vdots \\ 0 \end{pmatrix} \end{aligned}$$

とするとこれは環準同型で K が可換体より $\mathrm{Im}(\phi) \subset (\mathfrak{a}$ の中心$)$ より $K - alg$ になる。一般の I についても同様。

また、$\mathfrak{a}$ の単位元 $1_\mathfrak{a}$ は $(\underbrace{1,\dots,1}_{k},0,\dots,0)$ であり、これは A の単位元 $1_A = (1,\dots,1)$ と一致しないので A の部分 $K - alg$ ではない。

$I = \{1,\dots,k\}$ として考える。このとき $J = \{k+1,\dots,n\}$ である。$\psi : A \longrightarrow \mathfrak{a}, (a_1,\dots,a_n) \longmapsto (a_1,\dots,a_k)$ とするとこれは $K - alg$ 準同型で全射であり、 $\ker(\psi) = (a_{k+1},\dots,a_n) = \mathfrak{b}$ であるから準同型定理より $A/\mathfrak{b} \cong \mathfrak{a}$ となるので示された。 □

命題 8.14. etale $K - alg$ A は部分 $K - alg$ 及びイデアルを有限個しか持たない。

Proof. etale より $^\exists L/K$ により $L \otimes_K A \cong L^n$ であるので命題 (8.11)(8.12) より $L \otimes_K A$ の部分代数とイデアルは有限個。よって $A \subset L \otimes_K A$ の部分代数とイデアルも有限個。 □

Rem 8.15. $\mathrm{Hom}_{K-alg}(A, L)$ は A の素イデアルの集合 $\mathrm{Spec}(A)$ の ”$L-$ 有理点”の集合である。

例 8.16. $A := K[X,Y]/(f)$ で $f(X,Y) = X^3 + 1 - Y^2$ とする。このとき $\phi \in \mathrm{Hom}_{K-alg}(A,L)$ を取り、$x = X(\mod f), y = Y(\mod f), \phi(x) = a, \phi(y) = b$ とする。すると A で $f(X,Y) = 0_A$ から

$\phi(f) = f(a,b) = 0$ よりこの a, b が f の L 上の有理点になる。ϕ は準同型より x, y の送り先 a, b のみで $\phi(g(X,Y) + f\ (\in A)) = g(a,b)$ と定まるので $\mathrm{Hom}_{K-alg}(A, L) \cong \{(a,b) \in L^2 | f(a,b) = 0\}$ という同型が定まる。

8.3 分離次数

A : 有限次 $K - alg$ で $^\forall L/K$ に対して $h_A(L) := |\mathrm{Hom}_{K-alg}(A, L)|$ とおく。このとき系 (8.3) より $h(L) \leq n = [A : K]$ が成り立っている。

補題 8.17. Ω/K : 拡大、 Ω : 代数閉体とするとき $^\forall L/K$ に対し $h(L) \leq h(\Omega)$

Proof. L' : K の相対的代数閉包とすると $^\forall \phi \in \mathrm{Hom}_{K-alg}(A, L)$ において A の K 上の基底を $(e_1, \ldots, e_n)$ とする。このとき $^\forall x = a_1e_1 + \cdots + a_ne_n \in A$ と書けて $\phi(x) = a_1\phi(e_1) + \cdots + a_n\phi(e_n)$ となる。$\{\phi(e_1), \ldots, \phi(e_n)\}$ の部分集合が $\phi(A)$ の基底になるので $[\phi(A) : K] \leq [A : K] = n$ より $\phi(A)/K$ は有限次拡大より代数拡大である。よって $\phi(A) \subset L'$ だから $\phi \in \mathrm{Hom}_{K-alg}(A, L')$ なので $h(L) = h(L')$ になる。定理 (7.5) より L' は代数閉体と見た Ω に埋め込めるので終域が小さくなるから $\mathrm{Hom}_{K-alg}(A, L) = \mathrm{Hom}_{K-alg}(A, L') \subset \mathrm{Hom}_{K-alg}(A, \Omega)$ より $h(L) \leq h(\Omega)$ である。 □

定義 8.18. $[A : K]_s := \max_{L/K} h_A(L) = h_A(\Omega)$ ($\Omega : K$ の代数閉包, 補題 (8.17) から言える。)
を A の K 上の<u>分離次数 (separable degree)</u>という。系 (8.3) から $[A : K]_s \leq [A : K]$ が言える。

定義 8.19. ・$K - alg$ A が<u>分離的</u>とは $[A : K]_s = [A : K]$ となること。
・とくに有限次拡大 L/K が<u>分離的</u>とは $K - alg$ として L が分離的であること。
・代数拡大 L/K が<u>分離的</u>とは $\forall$ 有限次部分体 (中間体) が分離的であること。
・分離的な拡大を分離拡大、代数的かつ分離的な拡大を分離的代数拡大という。
・分離的でないとき非分離的という。

命題 8.20. A, B : 有限次 $K - alg$、 L/K : 拡大、 $A_{(L)} = L \otimes_K A$ とする。
(1) $[A \otimes_K B : K]_s = [A : K]_s[B : K]_s$
(2) $[A_{(L)} : L]_s = [A : K]_s$
(3) C : 有限次 $L - alg$ で L/K が有限次のとき $[C : K]_s = [C : L]_s[L : K]_s$

Proof. (1)
Ω を K の代数閉包とする。定義より $[A \otimes_K B : K]_s = h_{A \otimes_K B}(\Omega), [A : K]_s = h_A(\Omega), [B : K]_s = h_B(\Omega)$ である。そして

$$\begin{aligned} * : \mathrm{Hom}_{K-alg}(A, \Omega) \times \mathrm{Hom}_{K-alg}(B, \Omega) &\longrightarrow \mathrm{Hom}_{K-alg}(A \otimes_K B, \Omega) \\ (v, u) &\longmapsto v * u \\ v * u : A \otimes_K B &\longrightarrow \Omega \\ a \otimes b &\longmapsto v(a)u(b) \end{aligned}$$

と定める。まず、 $v' * u' = v * u$ のとき $^\forall a \otimes b \in A \otimes_K B, v'(a)u'(b) = v(a)u(b)$ で Ω の元だから $a \otimes b \neq 0$ で逆元が存在するから $v'(a) = v(a), u'(b) = u(b)$ より $(v', u') = (v, u)$ なので単射。
$u_1 : A \longrightarrow A \otimes_K B, a \longmapsto u_1(a) = a \otimes 1$ と $u_2 : B \longrightarrow A \otimes_K B, b \longmapsto u_2(b) = 1 \otimes b$ とすると

$^\forall a \otimes b(\in A \otimes_K B) = u_1(a)u_2(b)$ となる。任意の $w \in \mathrm{Hom}_{K-alg}(A \otimes_K B, \Omega)$ に対し、$v_i = w \circ u_i$ とすると準同型より $w(a \otimes b) = w(u_1(a)u_2(b)) = w \circ u_1(a) w \circ u_2(b) = v_1(a)v_2(b)$ となる。よって w に対して $v_1 \in \mathrm{Hom}_{K-alg}(A, \Omega), v_2 \in \mathrm{Hom}_{K-alg}(B, \Omega)$ をとれば $w = v_1 * v_2$ となるので全射。したがって $*$ は全単射だから $h_{A \otimes_K B}(\Omega) = h_A(\Omega)h_B(\Omega)$ より成立。

(2)

$\mathrm{Hom}_{K-alg}(A, \Omega)$ と $\mathrm{Hom}_{L-alg}(L \otimes_K A, \Omega)$ の間は系 (8.9) での π を用いれば L を Ω として見てもよく、これは全単射であるから $[L \otimes_K A : L]_s = [A : K]_s$ が成り立つ。

(3)

$S = \mathrm{Hom}_{K-alg}(L, \Omega), T = \mathrm{Hom}_{K-alg}(C, \Omega)$ とする。$\sigma \in S$ に対して $T_\sigma = \{f \in T | ^\forall \alpha \in L, f(\alpha) = \sigma(\alpha)\}$ とするとこれは以下で示されるように T を分割する。$\sigma, \tau \in S$ に対して $f \in T_\sigma \cap T_\tau$ としたとき $^\forall \alpha \in L, f(\alpha) = \sigma(\alpha) = \tau(\alpha)$ より $\sigma = \tau$ から $T_\sigma = T_\tau$ となる。また、 $^\forall g \in T$ に対して $\sigma := g|_L$ とすれば $\sigma(\alpha) = g(\alpha)$ だから $g \in T_\sigma$ であるので確かに T を分割する。

σ は体の準同型より単射だから Ω の中に $\sigma(L)$ として L を埋め込めるからその 2 つを同一視することで K の代数閉包 Ω を L の代数閉包と見ることもできる。このとき $^\forall f \in T_\sigma$ は定義より $^\forall \alpha \in L, f(\alpha) = \sigma(\alpha) \in \sigma(L) \cong L$ で $\sigma(L) \cong L$ 上恒等写像になる。したがって $f \in \mathrm{Hom}_{L-alg}(C, \Omega)$ より $T_\sigma \subset \mathrm{Hom}_{L-alg}(C, \Omega)$ である。また、この $\sigma(L)$ と L の同一視から $\alpha \in L$ は Ω の中で $\alpha = \sigma(\alpha) \in \sigma(L)$ であるので $\phi \in \mathrm{Hom}_{L-alg}(C, \Omega)$ に対して $\phi(\alpha) = \alpha = \sigma(\alpha)$ より $\phi \in T_\sigma$ だから $\mathrm{Hom}_{L-alg}(C, \Omega) \subset T_\sigma$ である。これより $T_\sigma = \mathrm{Hom}_{L-alg}(C, \Omega)$ から $|T_\sigma| = [C : L]_s$ となるので分割であることも考えれば $|T| = [C : K]_s = \sum_{\sigma \in S} |T_\sigma| = |S||T_\sigma| = [C : L]_s[L : K]_s$ より示された。 □

Note 8.21. 分離次数ではなく拡大次数でも (1) $\sim$ (3) と同様のことが成り立つ。

命題 8.22. A : 有限次 $K - alg$ について

$$A \text{ が } K \text{ 上分離的} \Leftrightarrow A \text{ は } K \text{ 上 etale}$$

Proof. 系 (8.9) と命題 (8.10) から

$$\begin{aligned} A \text{ が } K \text{ 上分離的} &\Leftrightarrow [A : K]_s = [A : K] \\ &\Leftrightarrow |\mathrm{Hom}_{K-alg}(A, \Omega)| = [A : K] \\ &\Leftrightarrow A \text{ はある } K \text{ の代数閉包}\Omega\text{で対角化される。} \\ &\Leftrightarrow A \text{ は } K \text{ 上 etale} \end{aligned}$$

□

系 8.23. 次の 3 つが成り立つ

(1) $A \otimes_K B$ が etale/K $\Leftrightarrow$ A と B がともに etale

(2) A/K : etale $\Leftrightarrow$ $A_{(L)}/L$: etale

(3) $C/L/K$ のとき C が K 上 etale $\Leftrightarrow$ C が L 上 etale でかつ L が K 上 etale

Proof. 代数が分離的であるときその分離次数は拡大次数と等しいという定義とその拡大次数を常に超えないということから命題 (8.20)(8.22) と拡大次数について命題 (8.20) が成り立つことより示される。 □

8.4 微分加群

定義 8.24. A/K の微分加群 $\Omega_{A/K}$ とは $I := \ker(A \otimes_K A \longrightarrow A, a \otimes b \longmapsto ab)$ としたとき $\Omega_{A/K} := I/I^2$ と定義される。定義より $\Omega_{A/K} \subset B := A \otimes_K A/I^2$ は明らか。ここで $A \otimes_K A$ を $a \longmapsto a \otimes 1$ と見ることで A 加群と考える。そして $d : A \longrightarrow \Omega_{A/K}, a \longmapsto d(a)(= da) := 1 \otimes a - a \otimes 1(\mod I^2)$ とする。このとき $a, b \in A$ と $k \in K$ に対して

$$
\begin{aligned}
d(ab) &= bd(a) + ad(b) \\
d(k) &= 0
\end{aligned}
$$

が成り立つ。実際、$d(ab) = 1 \otimes ab - ab \otimes 1 = (1 \otimes a)(1 \otimes b) - (a \otimes 1)(b \otimes 1) = (1 \otimes b)(1 \otimes a - a \otimes 1) + (a \otimes 1)(1 \otimes b - b \otimes 1) + (1 \otimes b)(a \otimes 1) - (a \otimes 1)(1 \otimes b) = bd(a) + ad(b)$ であり、$d(k) = 1 \otimes k - k \otimes 1 = k(1 \otimes 1) - k(1 \otimes 1) = 0$ より成立。

例 8.25. $A = K[X]$ とすると $\Omega_{A/K} = A \cdot dX(= d(X) = 1 \otimes X - X \otimes 1)$ であり $d : A \longrightarrow \Omega_{A/K}, f \longmapsto f'dX$ となる

例 8.26. $A = K[X]/(f)$ のとき $\Omega_{A/K} = A/(f')dX = K[X]/(f)/(f')dX = K[X]/(f, f')dX$ となる。

命題 8.27. 有限次 $K - alg$ A について

$$
A \text{ は } K \text{ 上で etale} \Leftrightarrow \Omega_{A/K} = 0
$$

が成り立つ。

系 8.28. $A = K[X]/(f)$ で etale/K $\Leftrightarrow (f, f') = 1$ (f とその形式微分 f'によって作られるイデアルが 1_Kを含む $\Leftrightarrow$ f と f'が互いに素)

Proof. 例 (8.26) と命題 (8.27) から $\Omega_{A/K} = 0 \Leftrightarrow (f, f') = K[X] = (1_K)$ より成り立つ。 □

8.5 被約

定義 8.29. 可換環 A が<u>被約 (reduced)</u>とは 0 以外の冪零元を持たないこと。 ($\Leftrightarrow$ $a \neq 0$ なら $a^2 \neq 0$) $K - alg$ A が被約とはそれが可換環として被約であること。

例 8.30. 体、整域は被約。被約 $\times$ 被約 $=$ 被約

図形的には重なっていないことと見ることができる。

補題 8.31. 可換環 A に冪等元 $e(\neq 0, 1)$ が存在するとき $A = A_1 \times A_2$ となる $\{0\}, A$ ではない部分環 A_1, A_2 が存在する。

Proof. $e' := 1 - e$ とするとこれも $(1 - e)(1 - e) = 1 - 2e + e^2 = 1 - e$ より冪等元である。また、$ee' = e(1 - e) = e - e^2 = 0$ をみたす。$A_1 := Ae, A_2 := Ae'$ とするとこれは 和と積について閉じているから A の部分環になっていて以下の準同型写像を考える。

$$
\begin{aligned}
\phi : A &\longrightarrow A_1 \times A_2 \\
x &\longmapsto (ex, e'x)
\end{aligned}
$$

ここで $\phi(x)=0 \Leftrightarrow ex=0 \wedge e'x=(1-e)x=0 \Rightarrow (1-e)x+ex=0 \Rightarrow x=0$ より $\ker(\phi)=\{0\}$ から単射。また、$^\forall(ea,e'b)$ に対して $ea+e'b\in A$ をとると $\phi(ea+e'b)=(e(ea+e'b),e'(ea+e'b))=(ea,e'b)$ より全射。したがって同型写像になるから $A\cong A_1\times A_2(=Ae\times Ae')$ となる。 □

補題 8.32. M : 有限生成 A 加群で $\mathfrak{a}$ を A のイデアルとして ϕ を M の A 加群の自己準同型であり $\phi(M)\subset \mathfrak{a}M$ を満たすとする。このとき M の生成系を $(x_1,\dots,x_n)$ として ϕ はある $a_i\in\mathfrak{a}$ により $\phi^n+a_1\phi^{n-1}+\cdots+a_n=0$ となる。

Proof. 定義から $^\forall i,\phi(x_i)\in\mathfrak{a}M$ から $\phi(x_i)=\sum_{j=1}^n a_{ij}x_j$ となる a_{ij} が存在するので以下の式変形で

$$\phi(x_i)-\sum_{j=1}^n a_{ij}x_j=0$$

$$\sum_{j=1}^n \delta_{ij}\phi(x_i)-a_{ij}x_j=0$$

$$\sum_{j=1}^n (\delta_{ij}\phi-a_{ij})x_j=0$$

となる。ここで n 次正方行列 $A:=(\delta_{ij}\phi-a_{ij})$ を考えることが出来てこれは $\vec{x}:={}^T(x_1,\dots,x_n)$ に対して $A\vec{x}=0$ となる。$\vec{x}$ の元は M の生成系から 0 ではないのでこの連立方程式は非自明解を持つからその行列式 $\det A=\det(\delta_{ij}\phi-a_{ij})=0$ である。この行列式は ϕ の n 次式になり、n 次部分は A の対角線上の積のみであるので n 次の係数は 1 でその他の係数は $a_{ij}\in\mathfrak{a}$ の積の和だからある $a_i\in\mathfrak{a}$ で $\phi^n+a_1\phi^{n-1}+\cdots+a_n=0$ となるので示された。 □

系 8.33. M を有限生成 A 加群として、$\mathfrak{a}$ を $\mathfrak{a}M=M$ となる A のイデアルとする。このとき $xM=0$ と $x\equiv 1(\mod \mathfrak{a})$ となる $x\in A$ が存在する。

Proof. 補題 (8.32) で $\phi=\mathrm{id}_M$ とすると $\phi(M)=M=\mathfrak{a}M$ から条件を満たしているので $\phi^n+a_1\phi^{n-1}+\cdots+a_n=1+a_1+\cdots+a_n=0$ となる $a_1,\dots,a_n\in\mathfrak{a}$ が存在する。ここで $x=1+a_1+\cdots+a_n$ とおくと $x\in A$ であり、$xM=0M=0$ と $a_1+\cdots+a_n\in\mathfrak{a}$ から $x\equiv 1(\mod \mathfrak{a})$ となる。 □

命題 8.34. 有限次 $K-alg$ A において次は同値。

(1) A は被約。

(2) A はある有限次体拡大 L_i/K により $A\cong L_1\times\cdots\times L_n$ となる。

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

体は被約であることより明らか。

(1) $\Rightarrow$ (2)

A が体であれば K の拡大体と見ることで $L:=A$ で成立する。

A が体でないとして A の次元について帰納法を用いる。$[A:K]=1$ のとき $A\cong K$ から K が可換体より成立。$[A_i:K]=m\le n$ の $K-alg$ A_i について題意が満たされているとする。$[A:K]=n$ のときもし A が冪等元 $e(\neq 0,1)$ を持っていれば補題 (8.31) より $A\cong A_1\times A_2$ となる 0 でも A でもない部分環が存在して部分環であることから $[A_1:K],[A_2:K]\le[A:K]$ となるので帰納法の仮定から A は題意を満たす。

よって A が冪等元 $e(\neq 0,1)$ を持っていることを示す。$\mathfrak{a}(\neq(0),(1))$ は A のイデアルで $K-$ ベクトル空間としてみたときに次数が最小のものとする。$\mathfrak{a}\neq(0)$ より 0 でない $x\in\mathfrak{a}$ がとれる。A が被約より $x^2\neq 0$ な

ので $\mathfrak{a}^2 \neq \{0\}$ であり $\mathfrak{a}^2 \subset \mathfrak{a}$ を満たす。そして $\mathfrak{a}$ の次数の最小性から $\mathfrak{a}^2 = \mathfrak{a}$ となる。

A が有限次 $K-alg$ よりそのイデアル $\mathfrak{a}$ も有限生成であるので系 (8.33) において $M = \mathfrak{a}$ としてもよく、$\mathfrak{a}$ 自身は $\mathfrak{a}\mathfrak{a} = \mathfrak{a}$ を満たしているので $xM = 0, x \equiv 1(\mod \mathfrak{a})$ となる $x \in A$ が存在する。$e := 1-x$ とすると $e \equiv 0(\mod \mathfrak{a})$ より $e \in \mathfrak{a}$ で $(1-e)\mathfrak{a} = 0$ となる。したがって $^\forall x \in \mathfrak{a}, (1-e)x = 0 \Leftrightarrow ex = x$ となるから $x = e \in \mathfrak{a}$ をとると $e^2 = e$ から冪等元 e が存在して $\mathfrak{a} = Ae$ となる。$\mathfrak{a} \neq (0), (1)$ から $e \neq 0, 1$ であるので A は冪等元 $e(\neq 0, 1)$ を持っているので示された。 □

定理 8.35. 有限次 $K-alg$ A について次は同値。

(1) A は K 上 etale。

(2) $^\forall L/K$ に対し $L \otimes_K A$ は被約。とくに、 A は被約。

(3) ある K の完全拡大体 P が存在して $P \otimes_K A$ が被約になる。

(4) $A \cong L_1 \times \cdots \times L_n, L_i/K$ は有限次分離拡大。分離拡大は次の章で説明する。

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

L を K の任意の体拡大とし、その代数閉包を Ω とおくと $L \subset \Omega$ より $L \otimes_K A$ は $\Omega \otimes_K A$ の部分環と同型である。また、 A は K 上 etale より命題 (8.10) から Ω で対角化されるから $\Omega \otimes_K A \cong \Omega^n$ となり、これは体の直積代数から被約であるから $L \otimes_K A$ も被約である。 □

例 8.36. $\mathrm{char}(K) = p > 0$ で K が完全体でないとすると Frobenius が同型でないので $a \in K^\times - (K^\times)^p$ という元が少なくとも一つとれる。このとき $A = K[X]/(X^p - a)$ は体で、とくに被約。これは $L := K(\alpha), (\alpha = \sqrt[p]{a})$ と同型になる。

その係数拡大は標数を考えて $L \otimes_K A = L[X]/(X^p - a) = L[X]/(X-\alpha)^p$ となる。よって $\xi := (X-\alpha) \mod (X-\alpha)^p$ は冪零元なので $L \otimes_K A$ は被約でない。

9　分離的代数拡大

9.1　多項式の分離性

命題 9.1. 代数拡大 L/K について次は同値。

(1) L/K : 分離的。

(2) L/K の $^\forall$ 部分拡大 M/K は分離的。

Proof. 定義 (8.19) から明らか。 □

命題 9.2. $f \in K[X] - K$ について以下は同値。

(1) $(f, f') = 1$ ($\Leftrightarrow f$ とその形式微分 f'が互いに素)

(2) f の判別式 $\mathrm{disc}(f) \neq 0$ ($f = \prod_{i=1}^n (X - \alpha_i)$ のとき $\mathrm{dics}(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2$と定義する)

(3) K のある拡大 L 上で f は相異なる一次式の積になる。

(4) f の任意の根は単根 (重解でない)

(5) $K[X]/(f)$ は etale$/K$ ($\Leftrightarrow K$ 上分離的)

Proof. (5) $\Leftrightarrow$ (1)

系 (8.28) で示した。

(2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4)

明らか。

(1) $\Rightarrow$ (2) ($\deg f > 1$ のときを考える) 対偶 $\mathrm{disc}(f) = 0 \Rightarrow (f, f') \neq 1$ を示す。

$\mathrm{dics}(f) = 0$ よりある $0 \leq i < j \leq n$ があり $\alpha_i = \alpha_j$ となる。$i = 1, j = 2$ としても一般性を失わない。これは f の根なので $f = (X - \alpha_1)^2 Q(X)$ となる $Q(X) \in K[X]$ が存在する。よって $f' = 2(X - \alpha_1)Q(X) + (X - \alpha_1)^2 Q'(X) = (X - \alpha_1)(2Q(X) + (X - \alpha_1)^2 Q'(X))$ となるから f, f' は共通の α_1 という根を持つので互いに素でないから $(f, f') \neq 1$ となる。

(2) $\Rightarrow$ (1) ($\deg f > 1$ のときを考える) 対偶 $(f, f') \neq 1 \Rightarrow \mathrm{disc}(f) = 0$ を示す。

$(f, f') \neq 1$ よりある α があってそれを $f = (X - \alpha)Q_1(X), f' = (X - \alpha)Q_2(X)$ として共通根として持つ。この二つから $f' = Q_1(X) + (X - \alpha)Q_1'(X) = (X - \alpha)Q_2(X)$ より $(X - \alpha)(Q_1'(X) - Q_2(X)) = Q_1(X)$ となるから $f = (X - \alpha)^2(Q_1'(X) - Q_2(X))$ より重根をもつ。したがって根の差の積である $\mathrm{disc}(f) = 0$ である。

$\deg f = 1$ のときは f の根は 0 より常に $\mathrm{disc}(f) = 0$ となるからこの命題には不適。 □

定義 9.3. これらが成り立つとき f を分離的という。そうでないとき非分離的という。

命題 9.4. 既約多項式 $f \in K[X]$ について次は同値。

(1) f は分離的。

(2) f は ($^\exists L$ に) 少なくとも一つの単根をもつ。

(3) $f' \neq 0$

(4) $\mathrm{char}(K) = 0$ か、または $\mathrm{char}(K) = p > 0$ で $f \notin K[X^p]$

Proof. (1) $\Rightarrow$ (2) は命題 (9.2) で示した。

(2) $\Rightarrow$ (3)

α を f の単根とする。$f'(\alpha)=0$ とすると命題 (9.2) の (2) $\Rightarrow$ (1) の証明より $f=(X-\alpha)^2Q(X)$ となるから α が単根に矛盾するので $f'(\alpha)\neq 0$ である。よって $f'\neq 0$

(3) $\Rightarrow$ (1)

体上の多項式より f を monic としてよい。α を f の任意の根とする。f が既約多項式で monic より f は最小多項式であるからその次数の最小性と $f'\neq 0$ より f' は多項式で $f'(\alpha)\neq 0$ であるから α は単根。これが任意の f の根について成り立つから f は分離的。

(3) $\Leftrightarrow$ (4)

$f=\sum_{i=0}^{n}a_iX^i\in K[X]$ について

$$\begin{aligned} f' &= \sum_{i=0}^{n}a_iiX^{i-1}=0 \\ &\Leftrightarrow \begin{cases} a_1=\cdots=a_n=0 & (\mathrm{char}(K)=0) \\ a_i=0\ (p\nmid i) & (\mathrm{char}(K)=p>0) \end{cases} \\ &\Leftrightarrow \begin{cases} f=a_0 & (\mathrm{char}(K)=0) \\ f=\sum a_{pk}X^{pk}\in K[X^p] & (\mathrm{char}(K)=p>0) \end{cases} \end{aligned}$$

より、 既約多項式は $f\in K[X]-K$ で否定を考えれば成立。 □

系 9.5. 体 K について次は同値。

(1) K は完全体

(2) 任意の既約多項式 $f\in K[X]$ は分離的

((3)$^\forall L/K$: 代数拡大は分離的)

Proof. (1) $\Leftrightarrow$ (2) のみ示す。

$\mathrm{char}(K)=0$ のとき命題 (9.4) の (1) $\Leftrightarrow$ (4) から $^\forall$ 既約多項式 $f\in K[X]$ は分離的。

$\mathrm{char}(K)=p>0$ のとき

$$K \text{ が完全体} \Leftrightarrow {}^\forall f\in K[X^p]-K \text{ は可約}$$

を示す。これより、既約ならば $f\notin K[X^p]-K$ が言えて命題 (9.4) の (4) $\Leftrightarrow$ (1) より既約ならば分離的が言える。

($\Rightarrow$)

$f=\sum a_iX^{pi}\in K[X^p]-K$ で $K^p:=\{x^p|x\in K\}$ (p 乗元の集合) とする。K が完全体なので Frobenius が全射だから $K=K^p$ なので $^\forall a_i\in K$ に対して $^\exists b_i\in K, a_i=b_i^p\in K^p=K$ である。したがって $\mathrm{char}(K)=p>0$ に注意すれば $f=\sum b_i^pX^{pi}=(\sum b_iX^i)^p$ より $\sum b_iX^i\in K[X]$ で分解できるから f は可約。

($\Leftarrow$) 対偶の K : 非完全 $\Rightarrow$ $^\exists f\in K[X^p]-K$ は既約 を示す。

K : 非完全とする。このとき $K^p\neq K$ から $^\exists a\in K^\times-K^p$ が取れる。ここで $f=X^p-a\in K[X]$ は既約になる。

b を f の根 ($b^p=a$) とし、g を b の K 上の最小多項式とする。最小性から $g\mid f$ で $\mathrm{char}(K)=p>0$ より $f=(X-b)^p$ となるから $g=(X-b)^d$ ($d^e=p$) と書ける。$f=g^e$ の形になり、 p が素数から $d=p$ または $d=1$ になる。$d=1$ とすると $g\in K[X]$ より $b\in K$ であり、 $a=b^p\in K^p$ から $a\in K^\times-K^p$ に矛盾する。

よって $d=p$ で $f=g$ となるから f は既約。これより既約な $f \in K[K^p]-K$ が存在するので対偶が示された。 □

9.2 元の分離性

定義 9.6. L/K : 拡大としたとき、K 上代数的な元 $x \in L$ がK 上分離的とは体の拡大 $K(x)/K$ が分離的であること。そうでないとき非分離的という。

命題 9.7. $x \in L : K$ 上代数的な元、 $f : x$ の最小多項式とするとき、次は同値。

(1) x は K 上分離的。

(2) f は分離多項式。

(3) x は f の単根。

(4) $K[X]/(f)$ は K 上 etale ($\Leftrightarrow K$ 上分離的)

Proof. x が K 上代数的なので命題 (6.14) から $K(x)=K[X]/(f)$ となる。

x が K 上分離的なとき定義から $K(x)/K$ が分離的なので $K[X]/(f)$ が K 上分離的である。そして命題 (9.2) の (5) $\Leftrightarrow$ (4) より f の任意の根は単根より x は f の単根であり、f は分離多項式である。 □

系 9.8. $x \in L$ が ${}^{\exists}g \in K[X]$ の単根ならば x は K 上分離的。

Proof. x の最小多項式を f としたとき最小性から $f \mid g$ より $f=gh$ となる $h \in K[X]$ が存在する。このとき h が x を根として持っているとすると f の最小性に矛盾するから $h(x) \neq 0$ である。したがって $f=gh$ は x を単根としてもつので命題 (9.7) から x は K 上分離的。 □

系 9.9. $x \in L$ が K 上分離的ならば L/K の任意の中間体 M でも分離的。

Proof. x の M 上の最小多項式を f_M とし、K 上の最小多項式を f_K とする。このとき $K[X] \subset M[X]$ から $M[X]$ 上で $f_M \mid f_K$ となる。x は K 上分離的なので f_K の単根であるから系 (9.8) で $g=f_K \in M[X]$ と見れば x は M 上分離的である。 □

命題 9.10. 拡大 L/K について以下は同値。

(1) L は K 上代数的かつ分離的。

(2) L の任意の元 x は K 上代数的かつ分離的。

(3) L は K 上代数的かつ分離的な元のある部分集合 $S(\subset L)$ によって K 上生成される。($L=K(S)$ となる)

Proof. (1) $\Rightarrow$ (2) L/K が代数的なので L の任意の元は K 上代数的。分離的であることから、 L/K の任意の有限次部分拡大が分離的である。${}^{\forall}x \in L$ は代数的元なので命題 (6.14) より $K(x)/K$ は有限次部分拡大。したがって $K(x)/K$ が分離的だから定義より x は分離的。

(2) $\Rightarrow$ (3) 仮定より L の任意の元は K 上代数的かつ分離的なので $S=L$ ととれて、 $K(L)=L$ より成立する。

(3) $\Rightarrow$ (1) 任意の $x \in L$ は S のある有限部分集合 S' によって $x \in K(S')$ となり、 $K(S')$ は有限次拡大より x は K 上代数的。よって L は K 上代数的。$S'=\{\alpha_1,\ldots,\alpha_n\}$ となっている時を考えれば良い。$L'=K(S')(=K(\alpha_1,\ldots,\alpha_n))$ とおくと $\alpha_i \in L$ は K 上代数的なので命題 (6.14) から L'/K は有限次拡大よ

り代数的である。$K_0 := K, K_n := L'$ として、 $K_{i+1} := K_i(\alpha_{i+1}), 0 \leq i \leq n-1$ と定めると拡大の列

$$K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$$

が作られる。α_{i+1} は K 上分離的なので系 (9.9) から K_n/K_0 の中間体である K_i 上分離的になる。よって定義から $K_i(\alpha_i)/K_i = K_{i+1}/K_i$ は分離的であるので $[K_{i+1} : K_i]_s = [K_{i+1} : K_i]$ となり、L'/K が有限次より $[K_{i+1} : K_i]$ も有限だから命題 (8.20) の (3) を繰り返し用いれば

$$\begin{aligned}[L' : K] = [K_n : K_0] &= \prod_{i=0}^{n-1}[K_{i+1} : K_i] \\ &= \prod_{i=0}^{n-1}[K_{i+1} : K_i]_s = [K_n : K_0]_s = [L' : K]_s\end{aligned}$$

となり L'/K は分離的である。 □

系 9.11. 代数拡大 L/K において次は同値。
(1) L/K は分離的。
(2) ${}^\forall x \in L$ は K 上の最小多項式の単根。 ($\Leftrightarrow$ 最小多項式が分離的)

Proof. 命題 (9.10) の (1) $\Leftrightarrow$ (2) から成立する。 □

命題 9.12. (1) L/K がある集合 S によって $L = K(S)$ とするとき

$$S \text{ の任意の元が } K \text{ 上代数的かつ分離的} \Rightarrow L/K \text{ は分離的}$$

(2) 代数拡大 $L_1/K, L_2/K$ $(\subset {}^\exists L)$ に対して L_1, L_2 の合成体を L_1L_2 とすると、

$$L_1L_2/K \text{ が分離的} \Leftrightarrow L_1/K, L_2/K \text{ がともに分離的}$$

(3) $L/M/K$ で L/K : 代数拡大のとき

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

(4) $L/K, K'/K$ とその合成体 $L' := LK' = K'(L)$ について L/K が代数的であるとき

$$L/K \text{ が分離的} \Rightarrow L'/K' \text{が分離的}$$

Proof. (1)
S の元は代数的かつ分離的で L は K 上 S で生成されるから命題 (9.10) の (3) $\Leftrightarrow$ (1) から成立。
(2)
($\Rightarrow$) 定義より $L_1, L_2 \subset L_1L_2$ から明らか。
($\Leftarrow$) (4) で $L = L_1, K' = L_2, L' = L_1L_2$ とおけば L_1/K が分離的より L_1L_2/L_2 が分離的になる。(3) から $L_1L_2/L_2, L_2/K$ が分離的より L_1L_2/K が分離的より示された。
(3)
($\Rightarrow$) L/K が分離的より、 ${}^\forall x \in L$ は K 上分離的。したがって ${}^\forall x \in M \subset L$ も K 上分離的であるから M は K 上分離的。また、系 (9.9) より ${}^\forall x \in L$ は M 上分離的でもあるので L は M 上分離的。
($\Leftarrow$) まず、命題 (6.17) より、 $L/M, M/K$ は代数拡大。${}^\forall x \in L$ をとると M 上代数的かつ分離的より最小多項式 $f = \sum_{i=0}^{n} a_iX^i \in M[X]$ があり、これは分離多項式である。$M' := K(a_1, \ldots, a_n)$ とすると

$f \in M'[X]$ であり、 x の最小多項式のままである。$L' := M'(x)(= K(x, a_1, \ldots, a_n))$ とすると、命題 (6.14) と $f \in M'[X]$ から、$L' = M'[X]/(f)$ は有限次拡大で、x は最小多項式 f の単根だから命題 (9.7) より、L' は M' 上分離的。また、 M'/K は M/K が分離的より定義から分離的。よって $L'/M, M'/K$ が有限次拡大かつ分離的であることから系 (8.23) の (3) から $[L' : K] = [L' : M'][M' : K] = [L' : M']_s[M' : K]_s = [L' : K]_s$ となるので L'/K も分離的。したがって $x \in L'$ は K 上分離的であるから元の任意性より L は K 上分離的。

(4)

L/K が代数的より、 ${}^\forall x \in L$ は K 上代数的であるが、$K \subset K'$ より K' 上代数的でもある。また、 x の K 上の最小多項式を f とすると $f \in K[X] \subset K'[X]$ で、 L/K が分離的から x は f の単根なので系 (9.8) より x は K' 上分離的。したがって L は K' 上分離的かつ代数的な元の集合なので命題 (9.10) の (3) $\Leftrightarrow$ (1) から $L' = K'(L)$ は K' 上代数的かつ分離的。 □

9.3 原始元

定義 9.13. L/K : 拡大で、 $x \in L$ が L/K の原始元 (primitive element)とは $L = K[x](= K[X]/(f) = K(x))$ となること。ただし f は x の K 上の最小多項式である。定理 (6.14) から L/K が原始元を持つためには有限次拡大であることが必要である。

定理 9.14. L/K について次は同値。

(1) L/K は原始元をもつ

(2) L/K は中間体を有限個しか持たない。

さらに、 L/K が有限次分離拡大ならこれらが成立する。

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

原始元を $x \in L$ とし、その最小多項式を $f \in K[X]$ とする。f を L 上で割り切ることができる monic 多項式 $g \in L[X]$ に対して、その係数で生成される K 上の体を E_g とする。この $\deg(f) = n$ のとき、 L で f は高々 n 個の既約多項式の積に表すことができる。この既約多項式の積の組み合わせが g になりうるので g の個数は高々 2^n 個であるのでこのような体 E_g は有限個である。L の中間体が全て E_g でかければ有限個だけであることがわかるのでそれを示す。

M をある中間体とすると $K \subset M, L = K[x]$ より $M[x] = L$ となる。ここで x の M 上の最小多項式を f_M とすると $[L : M] = \deg(f_M)$ である。$K[X] \subset M[X]$ より $f_M | f$ であるので f_M は M 上、したがって L 上で f を割り切る。$f_M \in M[X]$ より f_M の係数はすべて M に含まれているから $E_{f_M} \subset M$ である。また、$E_{f_M}[x] = L$ より、 $f_M \in E_{f_M}[X], f_M(x) = 0$ から $[L : E_{f_M}] \leq \deg(f_M) = [L : M]$ となるので $M \subset E_{f_M}$ である。したがって $M = E_{f_M}$ となり E_g の形で書けるから中間体は高々 2^n 個の有限個しか持たない。

(2) $\Rightarrow$ (1)

まず原始元の最小多項式の存在性のため、L/K が代数拡大であることを背理法により示す。L/K が超越元 x を持つと仮定する。このとき命題 (6.2) の (3) $\Leftrightarrow$ (1) の否定から $1, x, x^2, \cdots$ は一次独立である。したがってその部分集合 $1, x^2, (x^2)^2, \cdots$ も一次独立より x^2 も K 上超越元である。ここで $K(x) = K(x^2)$ と仮定すると、$x = f(x^2)/g(x^2)$ となる $f(X), g(X)(\neq 0) \in K[X]$ が存在するから、 x が $Xg(X^2) - f(X^2) \in K[X]$ の根になる。$Xg(X^2)$ は奇数次、 $f(X^2)$ は偶数次より $Xg(X^2) - f(X^2)$ となるからこれは x を根にもつ 0 でない K 上多項式になるため x の超越性に矛盾する。よって $K(x) \neq K(x^2)$ であるから $K(x^2) \subsetneq K(x)$ で

ある。これを繰り返せば

$$K \subset \cdots \subsetneq K(x^3) \subsetneq K(x^2) \subsetneq K(x) \subset L$$

となり無限個の中間体が存在してしまうのでこれは仮定に矛盾するから L/K は超越元を持たないから代数拡大である。

さらに、 L/K は有限生成であることを背理法により示す。有限生成でないとすると $\alpha_i \in L$ により

$$K \subsetneq K(\alpha_1) \subsetneq K(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq K(\alpha_1, \ldots, \alpha_n) \subsetneq \cdots \subset L$$

として無限個の中間体が存在してしまうので仮定に矛盾するから L/K は有限生成。以上より L/K は有限次元代数拡大である。

単拡大であることを示す。

・ K が有限体のとき

系 (4.6) からある素数 p と正整数 $f = [K : F_p]$ があり、 $q = p^f$ として、$K \cong F_q$(位数 $q = p^f$の有限体) となる。L/K は有限次拡大より拡大次数を e とすると、$L \cong F_{q^e}$ とできる。F_{q^e} の乗法群 $F_{q^e}^\times$ は位数 $q^e - 1$ の巡回群になるので $F_{q^e}^\times$ は位数 $q^e - 1$ の元 $\zeta \in F_{q^e}^\times$ を持つ。したがって $F_{q^e}^\times = \{1, \zeta, \ldots, \zeta^{q^e-2}\}$ から、$F_{q^e} = \{0, 1, \zeta, \ldots, \zeta^{q^e-2}\}$ となる。よって $F_{q^e} \subset F_q(\zeta) \subset F_{q^e}$ から $L = F_{q^e} = F_q(\zeta) = K(\zeta)$ より原始元 ζ が存在する。

・ K が無限体のとき

$^\forall\alpha \in L$ について有限次拡大より $[K(\alpha) : K] \leq [L : K] \leq \infty$ なので $\{[K(\alpha) : K] | \alpha \in L\}$ は正整数の有界集合。したがってある $\alpha_0 \in L$ が存在して、$^\forall\alpha \in L$ で $[K(\alpha) : K] \leq [K(\alpha_0) : K]$ となる。ここで任意に $\beta \in L$ を一つ定める。$^\forall c \in K$ について $M_c := K(c\alpha_0 + \beta)$ とする。これは L/K の中間体より有限個しかないが K が無限体より、 c は無限個とれるのである異なる $c_1, c_2 \in K$ で $M := M_{c_1} = M_{c_2}$ となる。このとき $c_1, c_2 \in K \subset M$ から $c_1 - c_2 \in M, c_1 - c_2 \neq 0$ より $(c_1 - c_2)^{-1} \in M$ が存在する。また、 $(c_1\alpha_0 + \beta) - (c_2\alpha_0 + \beta) = (c_1 - c_2)\alpha_0 \in M$ なので $(c_1 - c_2)^{-1}$ をかけても M に含まれているので $\alpha_0 \in M$ となる。そして $c_1\alpha_0 \in M$ にもなるので $\beta = (c_1\alpha_0 + \beta) - c_1\alpha_0 \in M$ である。これより、 $K(\alpha_0) \subset M = K(c_1\alpha_0 + \beta)$ で $[K(\alpha_0) : K] \leq [K(c_1\alpha_0 + \beta) : K]$ となるが α_0 の定義から $[K(\alpha_0) : K] = [K(c_1\alpha_0 + \beta) : K]$ で $K(\alpha_0) = K(c_1\alpha_0 + \beta) = M$ である。そして任意にとった $\beta \in L$ が $M = K(\alpha_0)$ に含まれるので $L = K(\alpha_0)$ となるから L/K は原始元 α_0 をもつ。 □

例 9.15. $L := F_p(X, Y), K := F_p(X^p, Y^p)$ とする。この中間体として $K(f_i), f_i := X + g_iY, g_i \in F_p(X, Y)$ をとると、$g_i \neq g_j \Rightarrow K(f_i) \neq K(f_j)$ となり、g_i のとり方は無限個あるので L/K の中間体は無限個あるから L/K に原始元は存在しない。

例 9.16. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ は $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$ ともできるので原始元が存在するから中間体は有限個。

9.4 分離閉体、分離閉包

定義 9.17. L/K に対して K の L の中での相対的分離 (代数) 閉包 (relative separable (algebraic) closure) L_s とは

$$L_s := \{x \in L | x \text{ は } K \text{ 上分離的 }\}$$

となるもの。これは命題 (9.10) の (2) ⇔ (1) より K 上代数的かつ分離的な拡大で L に含まれる代数的かつ分離的な拡大のうち最大のもの。

定義 9.18. L/K が代数拡大とする。$L_s = K$ となるときこの拡大を純非分離拡大という。

定義 9.19. 体 Ω が分離閉体 (separably closed) とはその分離的代数拡大は Ω のみであること。

定義 9.20. Ω が体 K の分離閉包 (separable closure)とは K の代数拡大で分離閉体であること。K 上分離閉な拡大ともいう。

命題 9.21. $\Omega : K$ 上代数閉な拡大とするとき
(1) Ω_s は K の分離閉包。
(2) K の分離閉包は K 上の同型を除き一意的

Proof. (1) L を Ω_s の分離的代数拡大とする。Ω_s は K 上代数的な元の集合でもあるので Ω が K 上の代数閉包より 拡大 Ω/Ω_s がつくれる。L/Ω_s は代数拡大で Ω は代数閉体なので命題 (7.5) から Ω_s- 準同型 $u : L \longrightarrow \Omega$ が存在し、Ω の中に L を $u(L)$ として埋め込める。このとき Ω の中で $u(L)/\Omega_s, \Omega_s/K$ はともに分離的なので命題 (9.12) の (3) より $u(L)/K$ は分離的で u は Ω_s- 準同型から $K-$ 準同型でもあるので構造を保存するから $u(L)/K$ は代数拡大。したがって $u(L)/K$ は代数的かつ分離的な拡大であり $\Omega_s \subset u(L)$ なので相対的分離閉包の最大性から $\Omega_s = u(L)$ となる。これより u の終域を制限して Ω_s- 準同型 $u : L \longrightarrow \Omega_s$ とできる。これは体の準同型から単射であり、 $u(L) = \Omega_s$ より全射なので同型なので $L \cong \Omega_s$ となる。そして、 L は Ω_s の拡大なので $\Omega_s \subset L$ から $L = \Omega_s$ となる。Ω_s の任意の分離的代数拡大は Ω_s だけであることが示されたので Ω_s は分離閉体である。相対的分離閉包の定義から K の代数拡大でもあるので K の分離閉包である。

(2) E を K の分離閉包とする。E は K の代数拡大より Ω が K の代数閉包より定理 (7.5) から $K-$ 準同型 $v : E \longrightarrow \Omega$ が存在して E を Ω に $v(E)$ として埋め込める。v は構造を保存するから $v(E)$ は K の分離閉包なので分離的代数拡大になっているから Ω_s の最大性より $v(E) \subset \Omega_s$ であり、$v(E)$ は Ω_s/K の中間体となっている。Ω_s/K が分離的より命題 (9.12) の (3) から $\Omega_s/v(E)$ は分離的。$v(E)$ が K の分離閉包より分離閉体だから $v(E)$ の分離拡大はそれ自身だけなので $v(E) = \Omega_s$ である。$E \subset \Omega_s$ は一般に言えていないので $E = \Omega_s$ とはならない。これより、 v の終域を制限した $K-$ 準同型 $v : E \longrightarrow \Omega_s$ は同型写像になるので任意の K の分離閉包は Ω_s と同型になるから同型を除いて一意的に定まる。 □

系 9.22. L/K : 分離的代数拡大、 E/K : 分離閉な拡大としたときある $K-$ 準同型 $\phi : L \longrightarrow E$ が存在する。(任意の分離的代数拡大は分離閉体 E に埋め込める)
定理 (7.5) の代数閉体のときと同じである。

Proof. Ω を E の代数閉包とすると K の Ω の中での相対的分離閉包 Ω_s は K 上分離的な元の集合なので $\Omega_s \subset E$ である。Ω は K 上代数閉でもあるので命題 (9.21) の (1) より Ω_s は K の分離閉包となるから (2) と $\Omega_s \subset E$ から同型より更に、$\Omega_s = E$ となる。また、 Ω は K の代数閉包であるから L/K が代数拡大より定理 (7.5) から $K-$ 準同型 $v : L \longrightarrow \Omega$ が存在する。v は構造を保存するから $v(L)$ は K 上分離的かつ代数的であるから、$v(L) \subset \Omega_s = E$ である。したがって $K-$ 準同型 $v : L \longrightarrow E$ が存在する。 □

9.5 非分離次数

定義 9.23. L/K とその K の L の中での相対的分離閉包 L_s について $[L : K]_i := [L : L_s]$ を L/K の非分離次数 (inseparable degree)という。

補題 9.24. 有限次拡大 L/K とその相対的分離閉包 L_s について $x \in L - L_s$ の L_s 上の最小多項式 $f \in L_s[X]$ はある素数 p と正整数 e と $y = x^{p^e} \in L_s$ で $f = X^{p^e} - y$ と書ける。

Proof. L/K が有限次拡大より代数拡大である。$\mathrm{char}(K) = 0$ のとき K は完全体より系 (9.5) の (1) $\Leftrightarrow$ (3) からその任意の代数拡大 L/K は分離的なので $L = L_s$ となる。したがって $L - L_s = \emptyset$ より補題は成立する。

$\mathrm{char}(K) = p > 0$ のときのみを考える。f の根 x は K 上分離的な元の集合の L_s に含まれないので非分離的な元である。したがって f は非分離的なので命題 (9.4) の (1) $\Leftrightarrow$ (4) から $\mathrm{char}(K) = p > 0$ で考えていることに注意すれば $f \in L_s[X^p]$ である。よって $f = g_1(X^p), g_1 \in L_s[X]$ となる g_1 が存在する。もし g_1 が非分離的であるとまた f と同様に $g_1 \in L_s[X^p]$ となるから $g_1 = g_2(X^p), g_2 \in L_s[X]$ となる g_2 が存在し、$f = g_2(X^{p^2})$ となる。これを g_n と g_{n+1} に帰納的に繰り返せば f, g_i が有限次よりあるところで分離的な多項式になり止まるのでこれを $g_e = g$ とおくと $f = g(X^{p^e}), g \in L_s[X], e \in \mathbb{Z}$ と書ける。$f \in L_s[X^p]$ より $\deg(f) = p^{e'}$ とおけるので $p^e \cdot \deg(g) = \deg(f) = p^{e'}$ が成り立つ。

f は x を根として持つので $f(x) = g(x^{p^e}) = 0$ より g の根でもある。この g の根を y とすると y は L_s 上分離的で $y = x^{p^e} \in L$ である。L_s 上分離的な元なので定義より $L_s(y)/L_s$ が分離的となるが L_s は命題 (9.21) の (1) より分離閉体なので $L_s(y) = L_s$ とならなくてはならない。したがって $y \in L_s$ である。ここで $h(X) = X^{p^e} - y$ とすると $h(X) \in L_s[X]$ であり、$\mathrm{char}(K) = p > 0$ より $(X - x)^{p^e} = X^{p^e} - x^{p^e} = X^{p^e} - y = h(X)$ から $h(X)$ は x を根にもつ L_s 上の多項式となる。

このとき $\deg(g) > 1$ と仮定すると $p^e \cdot \deg(g) = p^{e'}$ の等式より $p^{e'-e} = \deg(g) > 1$ から $e' > e$ となるから $\deg(h) = p^e < p^{e'} = \deg(f)$ となる。しかしこれは f の最小性に矛盾するから $\deg(g) = 1$ である。したがって $g(X) = X - y$ より $f(X) = g(X^{p^e}) = X^{p^e} - y$ となるので $x \in L - L_s$ の最小多項式は $x^{p^e} = y$ となる $y \in L_s$ によって $X^{p^e} - y$ とかける。

$\square$

命題 9.25. 有限次拡大 L/K について

$$[L : K]_s = [L_s : K]$$

がなりたつ。

Proof. Ω を K の代数閉包とする。L_s/K は命題 (9.10) の (2) $\Leftrightarrow$ (1) より分離的なので $[L_s : K]_s = [L_s : K] = |\operatorname{Hom}_K(L_s, \Omega)|$ となる。そして、$[L : K]_s = |\operatorname{Hom}_K(L, \Omega)|$ であるから定義域を制限する写像 $\operatorname{Hom}_K(L_s, \Omega) \longrightarrow \operatorname{Hom}_K(L, \Omega)$ が全単射であることを示せば $[L : K]_s = [L_s : K]$ となることが示される。

・全射性

${}^\forall \phi \in \operatorname{Hom}_K(L_s, \Omega)$ の L への拡張を $\tilde{\phi} \in \operatorname{Hom}_K(L, \Omega)$ とする。補題 (9.24) から $x \in L - L_s$ の L_s 上の最小多項式がある素数 p と $n \in \mathbb{Z}$ と $a \in L_s$ で $X^{p^n} - a$ の形になる。よって $\tilde{\phi}(x)^{p^n} = \tilde{\phi}(x^{p^n}) = \tilde{\phi}(a) = \phi(a)$ より $\tilde{\phi}(x) = \phi(a)^{1/p^n}$ と定まる。この $\tilde{\phi}$ をとればいいので全射

・単射性

$\phi \in \operatorname{Hom}_K(L_s, \Omega)$ の $\tilde{\phi} \in \operatorname{Hom}_K(L, \Omega)$ への延長は $\tilde{\phi}(x) = \phi(a)^{1/p^n}$ より ϕ に依るので一意的なので単射。 $\square$

10　ノルムとトレース

10.1　ノルムとトレース

定義 10.1. A : 有限次 $K-alg$ とする。$x \in A$ に対して x 倍写像

$$\begin{aligned} T_x : A &\longrightarrow A \\ a &\longmapsto xa \end{aligned}$$

は A が $K-alg$ より $K-$ 線形写像になる。よって $\dim_K(A) = n$ のときある A の基底 $\{e_1, \ldots, e_n\}$ により、 $T_x = (t_{ij})_{i,j=1,\ldots,n}$ とおいたとき行列表示は

$$T_x(e_j) = xe_j = \sum_{i=1}^{n} t_{ij} e_i$$

を満たすような $t_{ij} \in K$ で作られてこれにより行列 $T_x : K^n \longrightarrow K^n$ にできて行列の記法で

$$x(e_1, \cdots, e_n) = (e_1, \cdots, e_n)T_x$$

と書くことができる。

この行列 T_x について x のトレース (trace) $\mathrm{Tr}_{A/K}(x)$ と x のノルム (norm) $\mathrm{N}_{A/K}(x)$ を

$$\begin{aligned} \mathrm{Tr}_{A/K}(x) &:= \mathrm{Tr}(T_x) \\ \mathrm{N}_{A/K}(x) &:= \det(T_x) \end{aligned}$$

とするとこの値は K の元であるから

$$\begin{aligned} \mathrm{Tr}_{A/K} &: A \longrightarrow K \\ \mathrm{N}_{A/K} &: A \longrightarrow K \end{aligned}$$

という写像になっていて $\mathrm{Tr}_{A/K}$ は $K-$ 線形写像、 $\mathrm{N}_{A/K}$ は乗法的 $(\mathrm{N}(xy) = \mathrm{N}(x)\,\mathrm{N}(y))$ である。とくに、定義域を乗法群 $A^\times$ に制限すれば

$$\mathrm{N}_{A/K}|_{A^\times} : A^\times \longrightarrow K$$

は群準同型になる。

例 10.2. $x \in K$ のとき $n := [A : K]$ として、A の基底を $\{e_1, \ldots, e_n\}$ とする。$T_x = (t_{ij})_{i,j=1,\ldots,n}$ とおいたとき行列表示は

$$T_x(e_j) = \sum_{i=1}^{n} t_{ij} e_i$$

とできて $T_x(e_j) = xe_j$ で基底の一次独立性から $t_{jj} = x, t_{ij} = 0 \ (i \neq j)$ となるので

$$T_x = \begin{pmatrix} x & & \\ & \ddots & \\ & & x \end{pmatrix}$$

と書ける。したがって $\mathrm{Tr}_{A/K}(x) = nx, \mathrm{N}_{A/K}(x) = x^n$ となる。

例 10.3. $A := K[X]/(f)$ で $f = X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$ とする。$x := X + (f) \in A$ についてその x 倍写像 T_x は

$$T_x = \begin{pmatrix} 0 & & & -a_n \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \vdots \\ & & 1 & -a_1 \end{pmatrix}$$

と書けるから $\mathrm{Tr}_{A/K}(x) = -a_1, \mathrm{N}_{A/K}(x) = (-1)^n a_n$ となる。

Proof. $x \in A$ はその定義から f の根になっている。命題 (6.7) の (2) より $\{1, x, \ldots, x^{n-1}\}$ は A の基底になっているのでこの基底を用いて T_x を行列表示にする。$T_x := (t_{ij})_{i,j=1,\ldots,n}$ は x の指数を考えれば

$$T_x(x^j) = \sum_{i=0}^{n-1} t_{i+1j+1} x^i \ (0 \leq j \leq n-1)$$

とできる。$T_x(x^j) = x^{j+1}$ $(0 \leq j \leq n-1)$ より $1 \leq j+1 \leq n-1$ のとき

$$t_{i+1j+1} = \begin{cases} 1 & (j+1 = i) \\ 0 & (j+1 \neq i) \end{cases}$$

$j+1 = n$ のとき $x \cdot x^{n-1} = x^n = X^n + (f) = -a_1X^{n-1} - \cdots - a_n + (f) = -a_1x^{n-1} - \cdots - a_n$ であるので

$$\begin{aligned} T_x(x^{n-1}) &= x^n = -a_1x^{n-1} - a_2x^{n-2} - \cdots - a_n \\ &= \sum_{i=0}^{n-1} t_{i+1n} x^i = t_{nn}x^{n-1} + t_{n-1n}x^{n-2} + \cdots + t_{1n} \end{aligned}$$

より $t_{n-kn} = -a_{k+1}$ となる。よって T_x は上記の形になる。

$\mathrm{Tr}_{A/K}(x) = \mathrm{Tr}(T_x) = -a_1$ は明らか。$\mathrm{N}_{A/K}(x) = \det(T_x)$ は n 列をとなりの列と順番に入れ替えていけば入れ替えるごとに -1 倍されて 1 列まで移動させれば行列式の性質より $\det(T_x) = (-1)^{n-1}(-a_n)\det(E_n) = (-1)^n a_n$ となる。 □

Fact 10.4. $L/M/K$ に対し、 Tr, N は推移的。つまり、

$$\begin{aligned} \mathrm{Tr}_{L/K} &= \mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} \\ \mathrm{N}_{L/K} &= \mathrm{N}_{M/K} \circ \mathrm{N}_{L/M} \end{aligned}$$

が成り立つ。

10.2 正則表現

命題 10.5. 体拡大 L/K について x 倍写像を作る対応 T を L の K 上の基底 $\{e_1, \ldots, e_n\}$ によって $T_x \in M_n(K)$ で考えると

$$\begin{aligned} T : L &\longrightarrow M_n(K) \\ x &\longmapsto T_x \end{aligned}$$

は T_x の成分の定まり方より写像であり、単射環準同型になる。この K 上の写像 T を基底 $\{e_1, \ldots, e_n\}$ に関する A/K の正則表現という。

Proof. $T_x, T_y, T_{x+y}, T_{cx}, T_{xy} \in M_n(K)$ $(x, y \in A\ c \in K)$ についてこれはそれぞれ

$$\begin{aligned}
x(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_x \\
y(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_y \\
(x+y)(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_{x+y} \\
cx(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_{cx} \\
xy(e_1, \cdots, e_n) &= (e_1, \cdots, e_n)T_{xy}
\end{aligned}$$

を満たしている。それぞれ演算結果が等しくなることを考えれば

$$\begin{aligned}
T_{x+y} &= T_x + T_y \\
T_{cx} &= cT_x \\
T_{xy} &= T_xT_y
\end{aligned}$$

を満たすので $T : L \longrightarrow M_n(K)$ は環準同型である。

また、 e_j が基底なので $T(x) = T_x = 0 \Leftrightarrow t_ij = 0({}^\forall i, j) \Leftrightarrow xe_j = 0({}^\forall j) \Leftrightarrow x = 0$ が成り立つから $\ker(T) = \{0\}$ より T は単射。 □

10.3 分離拡大のノルムとトレース

命題 10.6. $L/K : n$ 次分離拡大、 $\Omega : K$ の代数閉包、 $\sigma_i \in \mathrm{Hom}_K(L, \Omega), (1 \leq i \leq n = [L : K] = [L : K]_s($分離拡大より$))$ とする。このとき L の n 個の元 $e_1, \ldots, e_n$ について次は同値。

(1) $e_1, \ldots, e_n$ は L/K の基底。

(2)

$$\det(\sigma_i(e_j)) = \begin{vmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \sigma_2(e_1) & \cdots & \sigma_2(e_n) \\ \vdots & & \vdots \\ \sigma_n(e_1) & \cdots & \sigma_n(e_n) \end{vmatrix} \neq 0$$

Proof. (1) ⇒ (2)

$\det(\sigma_i(e_j)) = 0$ と仮定すると $X = (\sigma_i(e_j))$ とおいたとき $\vec{x}X = 0$ は非自明解 $(c_1, \ldots, c_n) \in \Omega^n$ をもつ。つまり $\sum_{i=1}^n c_i\sigma_i(e_j) = 0$ $(1 \leq j \leq n)$ となるものが存在している。このとき任意の元 $\alpha \in L$ に対して、基底であることより $\alpha = \sum_{i=1}^n a_ie_i$ となる $a_i \in K$ が存在する。このとき σ_i は K を動かさないので

$$\begin{aligned}
\sum_{i=1}^n c_i\sigma_i(\alpha) &= \sum_{i=1}^n c_i\sigma_i\left(\sum_{i=1}^n a_ie_i\right) \\
&= \sum_{i=1}^n c_i \sum_{j=1}^n a_j\sigma_i(e_j) \\
&= \sum_{j=1}^n a_j \sum_{i=1}^n c_i\sigma_i(e_j) \\
&= \sum_{j=1}^n a_j \cdot 0 \\
&= 0
\end{aligned}$$

となるが c_i は全ては 0 で無いので Dedekind の補題 (2.6) に矛盾する。よって $\det(\sigma_i(e_j)) \neq 0$

(2) $\Rightarrow$ (1)

(2) を満たすような $e_1, \ldots, e_n$ が一次独立であることを示す。$c_1e_1 + \cdots + c_ne_n = 0$ となる $c_i \in K$ をとる。全体に σ_j をかけると $\sum_{i=1}^n c_i\sigma_j(e_i) = 0$ であるから

$$\begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \vdots & & \vdots \\ \sigma_n(e_1) & \cdots & \sigma_n(e_n) \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

となる。ここで仮定より $\det(\sigma_i(e_j)) \neq 0$ なのでこの連立方程式は自明解のみをもつから $c_1 = \cdots = c_n = 0$ であるので $e_1, \cdots, e_n$ は一次独立。L/K は n 次拡大なので基底の個数は n 個だからこの $e_1, \cdots, e_n$ が基底になる。 □

命題 10.7. $L/K : n$ 次分離拡大、 Ω を K の代数閉包、$\sigma_i : L \longrightarrow \Omega, \alpha \longmapsto \alpha^{\sigma_i} (= \alpha^{(i)}) := \sigma_i(\alpha), \sigma_i \in \mathrm{Hom}_K(L, \Omega)$ としたとき $\alpha \in L$ について

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \alpha^{(i)} = \sum_{i=1}^n \alpha^{\sigma_i}$$
$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^n \alpha^{(i)} = \prod_{i=1}^n \alpha^{\sigma_i}$$

となる。

Proof. L/K の基底を $e_1, \ldots, e_n$ とする。任意の $\alpha \in L$ についてこの基底による正則表現 $T : L \longrightarrow M_n(K), \alpha \longmapsto T_\alpha$ は $\alpha(e_1, \cdots, e_n) = (e_1, \cdots, e_n)T_\alpha$ を満たす。これに σ_i をかけると $\sigma_i(T_\alpha) = T_\alpha$ であり、$\alpha^{(i)}(e_1^{(i)}, \cdots, e_n^{(i)}) = (e_1^{(i)}, \cdots, e_n^{(i)})T_\alpha$ となる。これは

$$T_\alpha^\circ := \begin{pmatrix} \alpha^{(1)} & & \\ & \ddots & \\ & & \alpha^{(n)} \end{pmatrix}$$

と $M := (e_j^{(i)})_{i,j=1,\ldots,n}$ によって $T_\alpha^\circ M = MT_\alpha$ となる。命題 (10.6) の (1) $\Rightarrow$ (2) より $\det(M) \neq 0$ なので正則行列より M^{-1} が存在するから $T_\alpha = M^{-1}T_\alpha^\circ M$ とできる。したがって Tr と det の性質から

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(T_\alpha) = \mathrm{Tr}(M^{-1}T_\alpha^\circ M) = \mathrm{Tr}(T_\alpha^\circ) = \sum_{i=1}^n \alpha^{(i)} = \sum_{i=1}^n \alpha^{\sigma_i}$$
$$\mathrm{N}_{L/K}(\alpha) = \det(T_\alpha) = \det(M^{-1}T_\alpha^\circ M) = \det(T_\alpha^\circ) = \prod_{i=1}^n \alpha^{(i)} = \prod_{i=1}^n \alpha^{\alpha_i}$$

が成り立つ。 □

系 10.8. L/K が有限次分離拡大なら $\mathrm{Tr}_{L/K}(\alpha) \neq 0$ となる $\alpha \in L$ が存在する。

Proof. 任意の $\alpha \in L$ について命題 (10.7) から $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \alpha^{(i)}$ であり、これが 0 に等しいとすると命題 (2.6) に矛盾するからある $\alpha \in L$ で $\mathrm{Tr}_{L/K}(\alpha) \neq 0$ となる。 □

補題 10.9. L/K を標数 $p > 0$ の有限次純非分離拡大とする。このとき $\alpha \in L$ について以下が成立する。

$$\begin{aligned}\mathrm{Tr}_{L/K}(\alpha) &= [L:K]\alpha \\ \mathrm{N}_{L/K}(\alpha) &= \alpha^{[L:K]}\end{aligned}$$

とくに $[L:K] > 1$ のとき $\mathrm{Tr}_{L/K}(\alpha) = 0$ である。

Proof. 標数 $p > 0$ の体の有限次拡大なので $[L:K] = p^e, [L:K(\alpha)] = p^f, [K(\alpha):K] = p^g, f+g = e$ とする。$\mathrm{char}(K) = p > 0$ の純非分離拡大なので $K = L_s$ から、補題 (9.24) より α の最小多項式 $f(X) \in K[X]$ が存在して命題 (6.14) より次数は $p^g = [K(\alpha):K]$ なので $f = X^{p^g} - \alpha^{p^g} = (X-\alpha)^{p^g}$ とかける。Tr と N の推移律から

$$\begin{aligned}\mathrm{Tr}_{L/K}(\alpha) &= \mathrm{Tr}_{K(\alpha)/K}(\mathrm{Tr}_{L/K(\alpha)}(\alpha)) \\ \mathrm{N}_{L/K}(\alpha) &= \mathrm{N}_{K(\alpha)/K}(\mathrm{N}_{L/K(\alpha)}(\alpha))\end{aligned}$$

である。$\alpha \in K(\alpha)$ より例 (10.2) から $\mathrm{Tr}_{L/K(\alpha)}(\alpha) = [L:K(\alpha)](\alpha), \mathrm{N}_{L/K(\alpha)}(\alpha) = \alpha^{[L:K(\alpha)]}$ であることと Tr が準同型で N が乗法的であることより

$$\begin{aligned}\mathrm{Tr}_{L/K}(\alpha) &= \mathrm{Tr}_{K(\alpha)/K}([L:K(\alpha)]\alpha) = [L:K(\alpha)]\,\mathrm{Tr}_{K(\alpha)/K}(\alpha) = p^f\,\mathrm{Tr}_{K(\alpha)/K}(\alpha) \\ \mathrm{N}_{L/K}(\alpha) &= \mathrm{N}_{K(\alpha)/K}(\alpha^{[L:K(\alpha)]}) = (\mathrm{N}_{K(\alpha)/K}(\alpha))^{[L:K(\alpha)]} = \mathrm{N}_{K(\alpha)/K}(\alpha)^{p^f}\end{aligned}$$

となる。また、 $K(\alpha) = K[X]/(f)$ より例 (10.3) から $f = X^n + a_1X^{n-1} + \cdots + a_n$ のとき $\mathrm{Tr}_{K(\alpha)/K}(\alpha) = -a_1, \mathrm{N}_{K(\alpha)/K}(\alpha) = (-1)^n a_n$ である。二項定理より $f = (X-\alpha)^{p^g} = X^{p^g} - p^g X^{n-1}\alpha + \cdots + (-\alpha)^{p^g}$ なので $a_1 = -p^g\alpha, a_n = (-\alpha)^{p^g}$ であるのでこれを代入すれば

$$\begin{aligned}\mathrm{Tr}_{L/K}(\alpha) &= p^f \cdot -(-p^g\alpha) = p^{f+g}\alpha = p^e\alpha = [L:K]\alpha \\ \mathrm{N}_{L/K}(\alpha) &= ((-1)^{p^g}(-\alpha)^{p^g})^{p^f} = ((-1)^{2p^g}\alpha^{p^g})^{p^f} = \alpha^{p^e} = \alpha^{[L:K]}\end{aligned}$$

となり、示された。$[L:K] = p^e$ より $[L:K] > 1$ では p の冪なので $\mathrm{char}(K) = p > 0$ より $\mathrm{Tr}_{L/K}(\alpha) = 0$ である。 □

補題 10.10. 有限次拡大 L/K に対して、K の代数閉包を Ω とし $\sigma_i \in \mathrm{Hom}_K(L,\Omega), 1 \le i \le s := [L:K]_s$ とする。このとき ${}^\forall\alpha \in L$ に対して

$$\begin{aligned}\mathrm{Tr}_{L/K}(\alpha) &= [L:K]_i \sum_{i=1}^{s} \alpha^{\sigma_i} \\ \mathrm{N}_{L/K}(\alpha) &= \left(\prod_{i=1}^{s} \alpha^{\sigma_i}\right)^{[L:K]_i}\end{aligned}$$

となる。(命題 (10.7) では有限次分離拡大であったがより一般に有限次拡大で述べている)

Proof. 定義より $[L:K]_i = [L:L_s], s = [L:K]_s = |\mathrm{Hom}_K(L,\Omega)|$ である。命題 (9.25) から $s = [L:K]_s = [L_s:K]$ となっていてその証明から $\mathrm{Hom}_K(L_s,\Omega)$ と $\mathrm{Hom}_K(L,\Omega)$ の間の定義域を制限する写像が全単射であるから $\sigma_i \in \mathrm{Hom}_K(L,\Omega)$ に対して $\sigma_i|_{L_s} \in \mathrm{Hom}_K(L_s,\Omega)$ が全部で s 個ある。このとき ${}^\forall\alpha \in L$ に対して L/L_s は定義から純非分離拡大なので命題 (10.9) から

$$\begin{aligned}\mathrm{Tr}_{L/L_s}(\alpha) &= [L:L_s]\alpha = [L:K]_i\alpha \\ \mathrm{N}_{L/L_s}(\alpha) &= \alpha^{[L:L_s]} = \alpha^{[L:K]_i}\end{aligned}$$

となる。$\mathrm{Tr}_{L/L_s}, \mathrm{N}_{L/L_s}$ はともに $L \longrightarrow L_s$ の写像なので $[L:K]_i\alpha, \alpha^{[L:K]_i} \in L_s$ である。

命題 (10.7) から $\mathrm{Tr}_{L_s/K}, \mathrm{N}_{L_s/K}$ について $\sigma_i|_{L_s} : L_s \longrightarrow \Omega, 1 \leq i \leq s$ より

$$\mathrm{Tr}_{L_s/K}(\beta) = \sum_{i=1}^{s} \beta^{\sigma_i|_{L_s}} = \sum_{i=1}^{s} \beta^{\sigma_i}$$
$$\mathrm{N}_{L_s/K}(\gamma) = \prod_{i=1}^{s} \gamma^{\sigma_i|_{L_s}} = \prod_{i=1}^{s} \gamma^{\sigma_i}$$

となる。$\beta := [L:K]_i\alpha, \gamma := \alpha^{[L:K]_i}$ とすれば推移律より

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{L_s/K}(\mathrm{Tr}_{L/L_s}(\alpha)) = \mathrm{Tr}_{L_s/K}(\beta) = \sum_{i=1}^{s} \beta^{\sigma} = \sum_{i=1}^{s} [L:K]_i \alpha^{\sigma_i} = [L:K]_i \sum_{i=1}^{s} \alpha^{\sigma_i}$$
$$\mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{L_s/K}(\mathrm{N}_{L/L_s}(\alpha)) = \mathrm{N}_{L_s/K}(\gamma) = \prod_{i=1}^{s} \gamma^{\sigma_i} = \prod_{i=1}^{s} \left(\alpha^{[L:K]_i}\right)^{\sigma_i} = \left(\prod_{i=1}^{s} \alpha^{\sigma_i}\right)^{[L:K]_i}$$

となり成立する。 □

系 10.11. L/K を有限次非分離拡大で $[L:K] > 1$ とすれば任意の $\alpha \in L$ について $\mathrm{Tr}_{L/K}(\alpha) = 0$ となる。

(補題 (10.9) は純非分離拡大のみだったが一般の非分離拡大で成り立つことを述べている)

Proof. $\mathrm{char}(K) = 0$ は分離拡大なので $\mathrm{char}(K) = p > 0$ とする。このとき $[L:K] > 1$ から $[L:K] = p^e$ $(e \in \mathbb{Z}^+)$ であるから $[L:K]_i = [L:L_s] = p^f$ $(f \in \mathbb{Z}^+)$ となる。補題 (10.10) より任意の $\alpha \in L$ で $\mathrm{Tr}_{L/K}(\alpha) = [L:K]_i \sum_{i=1}^{s} \alpha^{\sigma_i} = p^f \sum_{i=1}^{s} \alpha^{\sigma_i}$ となる。これは $\mathrm{char}(K) = p > 0$ より 0 になるので示された。 □

命題 10.12. 有限次拡大 L/K について以下は同値

(1) L/K は分離拡大。

(2) $\mathrm{Tr}_{L/K}(\alpha) \neq 0$ となる $\alpha \in L$ が存在する。

Proof. (1) ⇒ (2)

系 (10.8) で示した。

(2) ⇒ (1)

$[L:K] > 1$ のとき系 (10.11) の対偶をとればよい。$[L:K] = 1$ のとき L_s は $K \subset L_s \subset L$ であり、$L = K$ から $L_s = L$ なので $L/K = L_s/K$ は分離拡大。 □

11　正規拡大 (準 Galois 拡大)

11.1　共役

定義 11.1. $\Omega := \overline{K}$: K の代数閉包とする。$L/K, M/K (L, M \subset \Omega)$ が K 上共役 (conjugate)とはある $\sigma \in \mathrm{Aut}_K(\Omega)$ があって $\sigma(L) = M$ となること。

$x, y \in \Omega$ が K 上共役 (conjugate)とはある $\sigma \in \mathrm{Aut}_K(\Omega)$ があって $\sigma(x) = y$ となること。

例 11.2. $z, \overline{z} \in \mathbb{C}$ は $\mathbb{R}$ の代数閉包であり、$G = \mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) := \{\mathrm{Id}_{\mathbb{R}}, \sigma\}, \sigma(z) = \overline{z}$ とする。このとき G の固定体 $\mathbb{R}^G = \mathbb{R}$ となるので $\mathbb{C}/\mathbb{R}$ は Galois である。この σ は複素共役をとる写像であるが $\sigma(z) = \overline{z}$ より一般の共役の定義にも適している。

命題 11.3. K の代数閉包 Ω とし、$x, y \in \Omega$ をとる。このとき次は同値。

(1) x と y は K 上共役。

(2) $K-$ 同型写像 $v : K(x) \longrightarrow K(y)$ で $v(x) = y$ となるものが存在する。

(3) x と y の K 上の最小多項式は同じ。

Proof. (1) $\Rightarrow$ (3)

x の最小多項式を $f \in K[X]$ とする。x と y は共役なのである $\sigma \in \mathrm{Aut}_K(\Omega)$ が存在して $\sigma(x) = y$ となる。σ は $K-$ 自己準同型より K の元を動かさないので f の係数を動かさない。よって $f(y) = f(\sigma(x)) = \sigma(f(x)) = \sigma(0) = 0$ より f は y を根にもつ。y の最小多項式を $g \in K[X]$ とする。$f \neq g$ と仮定すると $\deg(g)$ の最小性から $g|f$ より $f = gh$ となる $h \in K[X], \deg(h) > 0$ が存在する。このとき $f(x) = g(x)h(x) = 0$ となり f より次数の低い g または h が x を根にもつ。これは $\deg(f)$ の最小性に矛盾するから $f = g$ より x と y の最小多項式は一致する。

(3) $\Rightarrow$ (2)

x と y の最小多項式を $f \in K[X]$ とする。このとき命題 (6.14) より $K(x) \cong K[X]/(f) \cong K(y)$ であり、

$$\begin{aligned} K(x) &\longrightarrow K[X]/(f) \longrightarrow K(y) \\ x &\longmapsto X + (f) \longmapsto y \end{aligned}$$

となる同型写像が作れる。したがって $v : K(x) \longrightarrow K(y), x \longmapsto v(y)$ となる $K-$ 同型写像が存在する。

(2) $\Rightarrow$ (1)

Ω は $K(x), K(y)$ の代数閉包でもあるので系 (7.11) から $K-$ 同型 $v : K(x) \longrightarrow K(y)$ を $\tilde{v} : \Omega \longrightarrow \Omega$ に延長できる。これは $K-$ 自己準同型なので $\tilde{v} \in \mathrm{Aut}_K(\Omega)$ で $\tilde{v}(x) = v(x) = y$ より定義から x と y は K 上共役。 □

系 11.4. $x \in K$ の最小多項式 $f \in K[X]$ で $\sigma \in \mathrm{Aut}_K(\Omega)$ とする。このとき

$$g(X) := \prod_{\sigma \in \mathrm{Aut}_K(\Omega)} (X - \sigma(x))$$

は Ω において f を割る。

Proof. 命題 (11.3) の (1) $\Leftrightarrow$ (3) より f は x の共役元を根としてすべて含むので Ω において f が一次因子の積に分解できることより g は f を割る。 □

11.2 正規

定義 11.5. 代数拡大 L/K が正規 (normal)もしくは準 Galois (quasi − galois)であるとは任意の既約多項式 $f \in K[X]$ が根を L 内に一つもてば d は $L[X]$ において一次因子の積に分解することができる。(すべて同じ体の中に根をもつ)

$\Leftrightarrow$ ${}^{\forall}x \in L$ に対してその最小多項式 $f \in K[X]$ は $L[X]$ において一次因子の積に分解できる。

とくに代数閉包 Ω/K は代数閉体の同値条件の命題 (7.1) の (AC1) から正規拡大である。

命題 11.6. 代数拡大 L/K と代数閉包 Ω/K について次は同値。

(1) L/K は正規。

(2) ${}^{\forall}x \in L$ に対してその任意の共役は L に含まれる。

(3) ${}^{\forall}\sigma \in \mathrm{Aut}_K(\Omega), \sigma(L) = L$ となる。

(4) ${}^{\forall}\phi \in \mathrm{Hom}_K(L, \Omega), \phi(L) = L$ となる。

(5) L はある K 上の多項式族 $(f_i)_{i \in I}$ の最小分解体。

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

$x \in L$ の最小多項式 $f \in K[X]$ をとる。L/K が正規で x が L での f の根なので f は $L[X]$ 上で一次因子の積に分解できる。よって f の根はすべて L に含まれている。ここで命題 (11.3) の (1) $\Leftrightarrow$ (3) より x の任意の共役元も最小多項式は f なので f の根であるからそれは L に含まれる。

(2) $\Rightarrow$ (1)

${}^{\forall}x \in L$ について L/K が代数拡大より最小多項式 $f \in K[X]$ がある。f の他の根 $a_i \in \Omega/K, 1 \leq i \leq n := \deg(f)$ も f を最小多項式として持っているから命題 (11.3) の (1) $\Leftrightarrow$ (3) より a_i は x の共役元である。したがって $a_i \in L$ であるから f は $L[X]$ で $f = \prod_{i=1}^{n}(X - a_i)$ と一次因子の積に分解できるので L/K は正規拡大。

(1) $\Rightarrow$ (5)

${}^{\forall}x \in L$ の K 上の最小多項式の族 $(f_i)_{i \in I}$ をとり、この最小分解体を M とする。このとき $M[X]$ では f_i はすべて一次因子の積に分解できるから $M \subset L$ であり、 $x \in M$ でもあるので $M = L$ より L は $(f_i)_{i \in I}$ の最小分解体である。

(5) $\Rightarrow$ (3)

L が $(f_i)_{i \in I}$ の最小分解体であるとする。f_i の根を $\alpha_{ij} \in \Omega/K, 1 \leq j \leq n := \deg(f_i)$ とする。この根の集合を R_i とおくとき最小分解体の定義から $L = K(\cup_{i \in I} R_i)$ とかける。${}^{\forall}\sigma \in \mathrm{Aut}_K(\Omega)$ をとったときこれは K を動かさない。また、 α_{ij} の最小多項式はすべて f_i なのでそれぞれ共役であり体の準同型から単射なので $\sigma(R_i) = R_i$ となる。したがって $\sigma(L) = \sigma(K(\cup_{i \in I} R_i)) = K(\cup_{i \in I} R_i) = L$ より成立。

(3) $\Rightarrow$ (2)

${}^{\forall}x \in L$ に対してその共役は任意の $\sigma \in \mathrm{Aut}_K(\Omega)$ による $\sigma(x)$ であるが仮定より $\sigma(L) = L$ より $\sigma(x) \in L$ となる。したがって任意の元のすべての共役は L に含まれるので成立。

(4) $\Rightarrow$ (3)

${}^{\forall}\sigma \in \mathrm{Aut}_K(\Omega)$ をとる。このとき $\sigma|_L \in \mathrm{Hom}_K(L, \Omega)$ なので仮定より $\sigma|_L(L) = L$ で $\sigma|_L(L) = \sigma(L)$ より成立。

(3) $\Rightarrow$ (4)

$\phi \in \mathrm{Hom}_K(L,\Omega)$ にたいして $L, \phi(L)$ は K の代数拡大なので定理 (7.5) から代数閉包 Ω に埋め込めるので Ω はこれらの代数閉包でもある。ϕ は体の準同型より単射なので $\phi : L \longrightarrow \phi(L)$ は全単射となっているから $L \cong \phi(L)$ になっていて系 (7.11) よりこれを延長する $\sigma : \Omega \longrightarrow \Omega$ が存在する。したがって仮定より $\sigma(L) = L$ であり、 $\sigma|_L = \phi$ なので $\phi(L) = \sigma|_L(L) = \sigma(L) = L$ より成立。 □

系 11.7. L/K : 有限次拡大のとき

$$L/K : \text{正規} \Leftrightarrow [L:K]_s = h_L(L)(:= |\mathrm{Hom}_K(L,L)|)$$

が成り立つ。

Proof. 系 (8.3) より $[L:K]_s \leq [L:K]$ より L/K が有限次拡大なので $[L:K]_s$ も有限。$L \subset \Omega$ から一般に $\mathrm{Aut}_K(L) \subset \mathrm{Hom}_K(L,\Omega)$ である。体の準同型は単射なので $\mathrm{Hom}_K(L,L) = \mathrm{Aut}_K(L)$ とも書ける

($\Rightarrow$)

命題 (11.6) の (1) $\Leftrightarrow$ (4) から ${}^\forall\sigma \in \mathrm{Hom}_K(L,\Omega)$ をとると $\sigma(L) = L$ となっているので $\sigma \in \mathrm{Aut}_K(L)$ である。よって $\mathrm{Hom}_K(L,\Omega) \subset \mathrm{Aut}_K(L)$ であるので、一般に $\mathrm{Aut}_K(L) \subset \mathrm{Hom}_K(L,\Omega)$ が成り立つことを考えれば $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L,\Omega)$ だから $h_L(L) = [L:K]_s$ である。

($\Leftarrow$)

$h_L(L) = [L:K]_s$ が有限で成り立っていて $\mathrm{Aut}_K(L) \subset \mathrm{Hom}_K(L,\Omega)$ より $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L,\Omega)$ である。${}^\forall\sigma \in \mathrm{Hom}_K(L,\Omega)$ をとると $\sigma \in \mathrm{Aut}_K(L)$ なので $\sigma(L) = L$ を満たすから命題 (11.6) の (1) $\Leftrightarrow$ (4) から L/K は正規。 □

12　Galois 拡大再論

12.1　Galois 拡大

命題 12.1. 代数拡大 L/K について次は同値

(1) L/K は Galois

(2) L/K は正規かつ分離的

(2)$'$ $^\forall x \in L$ に対し、その最小多項式は分離的かつ $L[X]$ において一次因子の積に分解される。

(3) L/K はある分離多項式族 $(f_i)_{i\in I}$ の最小分解体

さらに、 L/K が有限次なら次も同値

(4) $[L:K] = h_L(L)(:= |\operatorname{Aut}_K(L)|)$

Proof. Ω を K の代数閉包とする。

(2) $\Leftrightarrow$ (2)$'$ は正規の定義 (11.5) と系 (9.11) と多項式の分離性の定義 (9.2) から明らか。

(1) $\Rightarrow$ (2)

$^\forall x \in L$ とその最小多項式 $f \in K[X]$ をとる。また、$Y_x := \{\sigma(x) | \sigma \in \operatorname{Aut}_K(L)\}$ と定めるとこれは x の Ω における共役元の集合の部分集合になり、$\sigma \in \operatorname{Aut}_K(L)$ から $Y \subset L$ である。命題 (11.3) の (1) $\Leftrightarrow$ (3) から x の共役元はすべて f の根なので高々 $\deg(f)$ 個しかないので Y_x は有限集合。$g := \prod_{y\in Y_x}(X-y), n := \deg(g)$ とする。y はすべて異なるから単根なので g は分離的である。また、 y は x の共役元より f の根でもあるから g のすべての根は f の根より $g|f$ となる。

$y \in Y_x \subset L$ よりその元から作られる基本対称式は L に含まれるので $g = \sum_{i=1}^n a_i X^i, a_i \in L$ と書ける。$\sigma g = \sum_{i=1}^n \sigma(a_i) X^i$ とすると係数だけに σ をかけているから $(\sigma g)(X) = \prod_{y\in Y_x}(X - \sigma(y))$ となる。ここで $y \in Y_x$ より $y = \tau(x), \tau \in \operatorname{Aut}_K(L)$ となるものが存在する。$\operatorname{Aut}_K(L)$ は自己同型写像であるから $\sigma \circ \tau \in \operatorname{Aut}_K(L)$ より $\sigma(y) = \sigma \circ \tau(x) \in Y_x$ となる。ここで Y_x は有限集合であることと σ は体の準同型より単射なのでそれぞれの y は σ によりそれぞれ異なる Y_x の元に行く。したがって $(\sigma g)(X) = \prod_{y\in Y_x}(X-y) = g(X)$ となるから a_i は $^\forall \sigma \in \operatorname{Aut}_K(L)$ によって動かされない。L/K が Galois より $L^{\operatorname{Aut}_K(L)} = K$ より $a_i \in K$ であるから $g \in K[X]$ である。

$g, f \in K[X]$ で $g|f$ より f の最小性から $f = g$ なので任意の $x \in L$ の最小多項式は $f = \prod_{y\in Y_x}(X-y)$ と $L[X]$ 上で一次因子の積に分解されるので L/K は正規。また、 $g(=f)$ は分離的でもあったので任意の最小多項式が分離的より系 (9.11) より L/K は分離的であるので L/K は正規かつ分離的。

(2) $\Rightarrow$ (1)

$L = K$ のとき $L^{\operatorname{Aut}_K(L)} = K^{\operatorname{Aut}_K(K)} = K$ で成立。$L \neq K$ のとき $L \supsetneq K$ であるから $^\forall x \in L - K$ をとる。これがある $\sigma \in \operatorname{Aut}_K(L)$ で $\sigma(x) \neq x$ となればよい。

x の最小多項式を $f \in K[X]$ とすると $x \in L - K$ より $\deg(f) > 1$ であり、仮定から L/K が分離的より系 (9.11) から f が単根を持つので定義より分離的だから $f(y) = 0$ で $y \neq x$ であるような元 $y \in \Omega$ が存在する。y の K 上の最小多項式も f なので命題 (11.3) の (2) $\Leftrightarrow$ (3) から $\sigma(x) = y$ となるような $\sigma \in \operatorname{Aut}_K(\Omega)$ が存在する。仮定から L/K は正規なので命題 (11.6) の (1) $\Leftrightarrow$ (3) から $\sigma(L) = L$ より $\sigma|_L \in \operatorname{Aut}_K(L)$ となる。この σ により $\sigma(x) = y \neq x$ なので x は固定されないから固定されるのは K の元のみなので $L^{\operatorname{Aut}_K(L)} = K$ となり定義より L/K は Galois である。

(2) $\Leftrightarrow$ (3)

命題 (11.6) の (1) $\Leftrightarrow$ (5) より「規 $\Leftrightarrow$ ある多項式族 $(f_i)_{i\in I}$ の最小分解体」が言えている。その多項式族は $^\forall x \in L$ の最小多項式の族であったので系 (9.11) より「分離的 $\Leftrightarrow$ 多項式族のすべての多項式が分離的」が言えている。

(2) $\Leftrightarrow$ (4)

有限次拡大のとき系 (11.7) から「正規 $\Leftrightarrow [L:K]_s = h_L(L)$」が言えている。定義より「分離的 $\Leftrightarrow [L:K] = [L:K]_s$」なので「正規かつ分離的 $\Leftrightarrow [L:K] = [L:K]_s = h_L(L)$」となり示された。 □

12.2 多項式の Galois 群

定義 12.2. K : 体、 $f \in K[X] - K$: 分離多項式、 L_f : f の K 上の最小分解体とするときその根をすべて添加しているので命題 (6.14) から L_f/K は有限次だから命題 (12.1) の (1) $\Leftrightarrow$ (3) から L_f/K は有限次 Galois 拡大である。このとき $\mathrm{Gal}(L_f/K)$ をf の K 上の Galois 群という。

命題 12.3. 分離多項式 $f \in K[X] - K$ にたいしてその最小分解体 L_f を考える。Ω を K の代数閉包で L_f を含むもの、$W := \{x \in \Omega | f \text{ の根 }\}$ とする。f は分離多項式なので $|W| = n := \deg(f)$ となる。このとき $\mathrm{Gal}(L_f/K)$ は W に作用し、根の置換を引き起こす。したがって W の自己同型写像の群、つまり W の置換群を $\mathfrak{S}_W$ とするとき $|W| = n$ から n 次対称群 $\mathfrak{S}_n$ でもあり、

$$\begin{aligned} \mathrm{Gal}(L_f/K) &\longrightarrow \mathfrak{S}_W (= \mathfrak{S}_n) \\ \sigma &\longmapsto \sigma|_W \end{aligned}$$

という単射群準同型が存在する。 ($\mathfrak{S}_W$に $\mathrm{Gal}(L_f/K)$ は埋め込める)

とくに $|\mathrm{Gal}(L_f/K)| = [L_f : K] \le n!$ である。

Proof. $^\forall \sigma \in \mathrm{Gal}(L_f/K) = \mathrm{Aut}_K(L_f)$ は $f(\sigma(x)) = \sigma(f(x)) = 0$ より $\sigma(x) \in W$ だから $\sigma(W) \subset W$ なので

$$\begin{aligned} \sigma|_W : W &\longrightarrow W \\ x &\longmapsto \sigma(x) \end{aligned}$$

となり σ は体の準同型より単射であって $|W| = n$ で有限集合なのでこれは全単射である。したがって $\sigma|_W$ は W 上の全単射写像の群である $\mathfrak{S}_W$ の元となる。$\sigma = \tau \in \mathrm{Gal}(L_f/K)$ のとき、 $\sigma|_W = \tau|_W$ であるので $\mathrm{Gal}(L_f/K) \longrightarrow \mathfrak{S}_W, \sigma \longmapsto \sigma|_W$ は写像になっている。また、 $\sigma|_W = \tau|_W$ のとき、$\mathrm{Aut}_K(L_f)$ の元としての σ, τ は K を動かさないので最小分解体の定義から $L_f = K(W)$ なので W の動かし方で定まるから $\sigma = \tau$ である。したがって制限写像 $\mathrm{Gal}(L_f/K) \longrightarrow \mathfrak{S}_W$ は単射である。

L_f/K は定義 (12.2) から有限次 Galois なので命題 (12.1) の (1) $\Leftrightarrow$ (4) から $[L_f : K] = h_{L_f}(L_f) = |\mathrm{Aut}_K(L_f)| = |\mathrm{Gal}(L_f/K)|$ である。ここで上述のことから $\mathrm{Gal}(L_f/K)$ は $\mathfrak{S}_W = \mathfrak{S}_n$ に埋め込めるから $|\mathrm{Gal}(L_f/K)| = [L_f : K] \le |\mathfrak{S}_n| = n!$ より示された。 □

系 12.4. 一般の n 次多項式 $f \in K[X]$ の最小分解体 L の拡大次数は $n!$ 以下である。

Proof. 命題 (12.3) で f は分離多項式とは限らないので $|W| \le n$ であるから $|\mathfrak{S}_W| \le |\mathfrak{S}_n|$ である。埋め込むことは同様にできるから $\mathrm{Gal}(L_f/K)$ を $\mathrm{Aut}_K(L)$ として $|\mathrm{Aut}_K(L)| \le |\mathfrak{S}_W| \le |\mathfrak{S}_n| = n!$ より成立。 □

命題 12.5. 分離多項式 $f \in K[X] - K$ の根の集合 W とその元 $x, y \in W$ に対して以下は同値。

(1) x と y は K 上共役。

(2) x と y は同じ $\mathrm{Gal}(L_f/K)-$ 軌道上に属する。

(3) x と y は f の同じ既約成分の根。

とくに f が既約であるためには $W \neq \emptyset$ かつ $\mathrm{Gal}(L_f/K)$ が W に推移的に作用することが必要十分である。(群 G が集合 X に推移的に作用するとは $G-$ 軌道 $G(x) := \{\sigma(x) | \sigma \in G\}$ とするとき $G(x) = X$ となること)

Proof. Ω を K の代数閉包とする。

$(1) \Leftrightarrow (2)$

f が分離的なので L_f/K は有限次 Galois 拡大であるから正規なので $\sigma \in \mathrm{Aut}_K(\Omega), \sigma(L_f) = L_f$ を満たすから $\sigma|_{L_f} \in \mathrm{Aut}_K(L_f) = \mathrm{Gal}(L_f/K)$ となる。また、 $\sigma \in \mathrm{Gal}(L_f/K)$ は系 (7.11) より $\tilde{\sigma} \in \mathrm{Aut}_K(\Omega)$ に拡張できる。これより

$$
\begin{aligned}
x \text{ と } y \text{ が } K \text{ 上共役} &\Leftrightarrow {}^{\exists}\sigma \in \mathrm{Aut}_K(\Omega), x = \sigma(y) \\
&\Leftrightarrow y \in \{\sigma(x) | \sigma \in \mathrm{Gal}(L_f/K)\} \\
&\Leftrightarrow y \text{ は } x \text{ の } \mathrm{Gal}(L_f/K) - \text{軌道に含まれる}
\end{aligned}
$$

となる。

$(1) \Leftrightarrow (3)$

命題 (11.3) の $(1) \Leftrightarrow (3)$ より x と y が K 上共役 $\Leftrightarrow$ x と y の K 上の最小多項式は同じなのでその最小多項式を $g \in K[X] - K$ とすれば g は f の既約成分であるので示された。

もし $\mathrm{Gal}(L_f/K)$ が $W(\neq \emptyset)$ に推移的に作用するとすると、ある f の根 x に対してその $\mathrm{Gal}(L_f/K)-$ 軌道は W に一致するので任意の f の根は $(2) \Leftrightarrow (3)$ から f の同じ既約成分の根になる。したがって f の根はすべて f の既約成分の根になるから f は既約。f が既約であるとき $(2) \Leftrightarrow (3)$ からすべての根はある f の根 x と同じ $\mathrm{Gal}(L_f/K)-$ 軌道上に属するから $W \subset \mathrm{Gal}(L_f/K)-$ 軌道である。また、 x の軌道はすべて f の根になるから $W \supset \mathrm{Gal}(L_f/K)-$ 軌道より $W = \mathrm{Gal}(L_f/K)-$ 軌道となり推移的である。 □

例 12.6. K : 体、 $L := K(T_1, \ldots, T_n)$: n 変数の有理関数体とする。$G := \mathfrak{S}_n$ として T_i の添字の置換とする。つまり、 $\sigma \in G$ と $f = f(T_1, \ldots, T_n) \in L$ に対して、$\sigma f := f(T_{\sigma(1)}, \ldots, T_{\sigma(n)})$ と作用させることとする。このとき、 G の元は T_i を写し、 K の元は動かさないので L の体の自己同型とみなせるので $G \subset \mathrm{Aut}_{体}(L)$ となる。

$M := L^G$ とおくとこれは $T_1, \ldots, T_n$ の対称有理式の集合になる。このとき L/M が Galois となって、$G = \mathrm{Gal}(L/M)$ を満たす。とくに $[L : M] = n!$ となる。

Proof. $s_i := (T_1, \ldots, T_n$の i 次基本対称式$)$ とすると $s_i \in L$ である。つまり、 $s_1 = T_1 + \cdots + T_n, s_2 = T_1T_2 + T_1T_3 + \cdots + T_{n-1}T_n, \cdots, s_n = T_1 \cdots T_n$ となっている。$M_0 := K(s_1, \ldots, s_n)$ とおくと基本対称式は文字を置換しても同じままなので M_0 は G で固定される。よって $M_0 \subset M$ である。

ここで $T_1, \ldots, T_n$ は解と係数の関係から $X^n - s_1X^{n-1} + \cdots + (-1)^n s_n \in M_0[X]$ の根になる。$T_1, \ldots, T_n$ はそれぞれ異なるから命題 (9.2) からこの多項式は分離的である。L はこの多項式の最小分解体なので定義 (12.2) から L/M_0 は有限次 Galois 拡大になる。命題 (12.3) から $[L : M_0] \leq n!$ である。また、L/M は Artin の定理 (2.9) から Galois 拡大で $G = \mathfrak{S}_n = \mathrm{Aut}_M(L)$ であり、Rem (2.11) から $[L : M] = |\mathrm{Aut}_M(L)| = |\mathfrak{S}_n| = n!$ となる。よって $M_0 \subset M$ と $[L : M_0] \leq n! = [L : M]$ より $M_0 = M$ となる。以上より M は $T_1, \ldots, T_n$ の対称有理式の集合になり、$G = \mathfrak{S}_n = \mathrm{Gal}(L/M)$ で、 $[L : M] = n!$ となる。 □

Fact 12.7. $n \geq 5$ ならば n 次交代群 $\mathfrak{A}_n$ は非アーベル単純群なので非自明な正規部分群を持たない。命題 (3.4) より可解群となるための可解列に出てくる交換子群は正規部分群であるので $\mathfrak{A}_n$ は可解群にならない。よって $\mathfrak{A}_n$ を含む $\mathfrak{S}_n$ は $n \geq 5$ で非可解群。任意の n 次分離多項式 $(\in \mathbb{Q}[X])$ の Galois 群は命題 (12.3) より $\mathfrak{S}_n$ の部分群に同型である。これより定理 3.8 から 5 次以上の一般代数方程式は解の公式を持たないことがわかる。

12.3 IGP (Inverse Galois Problem)

Galois の逆問題 (IGP Inverse Galois Problem) とは K : 体、G : 有限群が与えられたとき、$\mathrm{Gal}(L/K) \cong G$ となる Galois 拡大 L/K は作れるかというもの

Fact 12.8. Hilbert の既約性定理

$X^n - s_1X^{n-1} + \cdots + (-1)^n s_n$ はほとんどの (有限個の例外を除き) $(s_1, \ldots, s_n) \in \mathbb{Q}^n$ に対し既約でその Galois 群は $\mathfrak{S}_n$ と同型。

12.4 無限次 Galois 拡大

L/K が無限次 (かもしれない)Galois 拡大のとき $\mathrm{Gal}(L/K)$ は profinite(副有限、射影有限) 群 (有限群の射影極限になっている群) である。つまり、 $L'/K, L''/K (L' \subset L'')$ を L に含まれる任意の有限次 Galois 拡大とし、制限写像 $\mathrm{Gal}(L''/K) \longrightarrow \mathrm{Gal}(L'/K), \sigma \longmapsto \sigma|_{L'}$ による射影極限

$$\mathrm{Gal}(L/K) = \varprojlim_{L'/K} \mathrm{Gal}(L'/K) \subset \prod_{L'/K} \mathrm{Gal}(L'/K)$$

で定義される。$\mathrm{Gal}(L'/K)$ は離散位相によって位相群になるので $\mathrm{Gal}(L/K)$ にはその直積位相が入り、これを Krull 位相という。

定理 12.9. Galois 理論の基本定理の無限次版

L/K :Galois 拡大、 $G := \mathrm{Gal}(L/K)$ とすると次の一対一対応がある。

$$\begin{aligned}
\{L/K \text{ の部分体 }\} &\overset{1:1}{\longleftrightarrow} \{G \text{ の閉部分群 }\} \\
M &\longmapsto \mathrm{Aut}_M(L) = \mathrm{Gal}(L/M) \\
L^H &\longleftarrow H \\
\{L/K \text{ の部分体で } K \text{ 上有限次のもの }\} &\overset{1:1}{\longleftrightarrow} \{G \text{ の開部分群 (指数有限の部分群)}\} \\
\{L/K \text{ の部分体で } K \text{ 上有限次のものでかつ } K \text{ 上 Galois になるもの }\} &\overset{1:1}{\longleftrightarrow} \{G \text{ の開正規部分群 }\}
\end{aligned}$$

他の性質は有限次のとき (2.13) と同じ。

定義 12.10. K : 体、 K^{sep} : K の分離閉包とするとき、命題 (9.21) から K の代数閉包の相対的分離閉包が K^{sep} になるから $^\forall x \in K^{\mathrm{sep}}$ は K 上代数的かつ分離的なので K^{sep}/K は Galois であり、$G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ を K の<u>絶対 Galois 群</u>という。絶対 Galois 群は適切な位相を導入することで位相群になる。

すると、 L'/K を K^{sep}/K に含まれる有限次 Galois 拡大とするとき $G_K = \varprojlim_{L'/K} \mathrm{Gal}(L'/K)$ となり、とく

に $\forall L'/K$ に対し $G_K \overset{sur}{\longrightarrow} \mathrm{Gal}(L'/K)$ があるから $\forall L'/K$ に G_K が作用していると考えられる。
逆に G_K から K を作ることも考えられる。

定理 12.11. Neukirch − 内田 (−Pop) の定理
K_1, K_2 : 素体上有限生成な体。

$$G_{K_1} \cong G_{K_2} \Rightarrow K_1 \cong K_2$$
(位相群として同型)　(体として同型)

が成り立つ。これの一般化である Grothendieck 予想もある。

12.5 有限体の Galois 拡大

以下では K : 有限体、 $\mathrm{char}(K) = p > 0$ で $[K : F_p] = f, |K| = p^f = q$ とする。

定義 12.12. 群 G の冪数とはそれが存在するなら G の元の位数の最小公倍数のことである。

補題 12.13. 体 F の乗法群 $F^\times$ の有限部分群は巡回群。

Proof. G を $F^\times$ の有限部分群、 N を G の冪数とする。このとき正整数 $n_1|n_2|\cdots|n_r$ によって $G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \mathbb{Z}/n_r\mathbb{Z}$ で $N = \mathrm{LCM}(n_1, \ldots, n_r) = n_r$ となる。このとき $\forall x \in G, x^N = 1$ より G の元は $X^N - 1$ の根であり、この多項式は F に高々 N 個しか根を持たないので $|G| \leq N$ となる。そして、$|\mathbb{Z}/n_r\mathbb{Z}| = n_r = N$ より $G = \mathbb{Z}/n_r\mathbb{Z}$ となるしかなく、したがって G は巡回群になる。 □

系 12.14. K が q 元体ならば $K^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$ で位数 $q-1$ の巡回群となる。

Proof. $K^\times$ は 0 を除いた $q-1$ 個の元の有限群なので成立。 □

系 12.15. 位数 q の有限体 K は同型を除き一意に定まる。これを $\mathbb{F}_q$ と書く。

Proof. 有限体 K は素体として $\mathbb{F}_p$ と同型な体を含む。Ω を $\mathbb{F}_p$ の代数閉包とすると $K/\mathbb{F}_p$ が有限次拡大より代数拡大なので定理 (7.5) から Ω に K を埋め込める。K の元は系 (12.14) より $X^{q-1} - 1$ の根と 0 ですべて出しつくされるので $K = \{x \in \Omega | x^q = x\}$ と書ける。Ω に埋め込めばすべてこの形に書けるので同型を除き一意に定まる。 □

系 12.16. 各 $n \in \mathbb{Z}^+$ に対し $\mathbb{F}_q$ の n 次拡大は同型を除きただ一つ存在しそれは $\mathbb{F}_{q^n}$ である。とくに $\mathbb{F}_p$ の代数閉包 Ω の中では唯一つである。

Proof. $\mathbb{F}_q$ の n 次拡大は $\mathbb{F}_p$ の q^n 次拡大なので系 (12.15) を q^n について適用すれば良い。Ω の中では $\mathbb{F}_{q^n} = \{x \in \Omega | x^{q^n} = x\}$ として書けるので唯一つに定まる。 □

命題 12.17. $\mathbb{F}_{q^n}/\mathbb{F}_q$ は Galois 拡大であり

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ 1 &\longmapsto \phi_q \end{aligned}$$

で定める準同型写像は同型写像になる。ただし、 ϕ_q は

$$\begin{aligned}\phi_q : \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n} \\ x &\longmapsto x^q\end{aligned}$$

とする。

Proof. $\mathbb{F}_q$ の任意の n 次拡大体 L は系 (12.16) より $L \cong \mathbb{F}_{q^n}$ となるので $L = \mathbb{F}_{q^n}$ とする。定義から $\phi_q \in \mathrm{Aut}(\mathbb{F}_{q^n})$ である。${}^{\forall}x \in \mathbb{F}_q$ に対しては $\mathbb{F}_q = \{x \in \Omega | x^q = x\}$ より $\phi_q(x) = x^q = x$ なので $\mathbb{F}_q$ 上恒等的だから $\phi_q \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ となる。

また、 ϕ_q は位数 n になることを示す。つまり、 ϕ_q^i が $i = 1, \ldots, n-1$ で $\phi_q^i \neq \mathrm{Id}$ となり、$i = n$ で $\phi_q^i = \mathrm{Id}$ となればよい。$\phi_q^i : x \longmapsto \phi_q^i(x) = x^{q^i}$ であるからもしこれが恒等であるとすると ${}^{\forall}x \in \mathbb{F}_{q^n}, x^{q^i} = x$ であるので $\mathbb{F}_{q^n}$ は系 (12.16) の証明における $\{x \in \Omega | x^{q^i} = x\} = \mathbb{F}_{q^i}$ の部分集合になるから元の個数を考えれば $i = n$ でそのようになることがわかる。したがって ϕ_q は位数 n である。

$G := \langle \phi_q \rangle \subset \mathrm{Aut}(\mathbb{F}_{q^n})$ とする。ϕ_q の位数が n より $\langle \phi_q \rangle \cong \mathbb{Z}/n\mathbb{Z}$ となる。L/L^G は Artin の定理 (2.9) より Galois 拡大で $[L : L^G] = |G| = n$ となる。また、 $L = \mathbb{F}_{q^n}$ より $[L : \mathbb{F}_q] = n$ なので $[L : \mathbb{F}_q] = [L : L^G]$ と $\mathbb{F}_q, L^G \subset L$ より $\mathbb{F}_q = L^G$ となるから $\mathbb{F}_{q^n} / \mathbb{F}_q$ は Galois 拡大でその Galois 群は $\mathbb{Z}/n\mathbb{Z}$ と同型。 □

系 12.18. $\mathbb{F}_q$ の代数閉包を $\overline{\mathbb{F}_q}$ とすると $\mathbb{F}_q$ の絶対 Galois 群 $G_{\mathbb{F}_q} := \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ であり、このとき $G_{\mathbb{F}_q} \cong \hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ となる。また、 $\mathbb{Z}_l := \varprojlim_m \mathbb{Z}/l^m\mathbb{Z}$ とするとき $\hat{\mathbb{Z}}$ は $\prod_{l:\text{素数}} \mathbb{Z}_l$ とも書ける。

例 12.19. 形式的冪級数体 $K := \mathbb{C}((X))$ の絶対 Galois 群は $G_K \cong \hat{\mathbb{Z}}$ である。

12.6 円分拡大

定義 12.20. K : 体、 $n \in \mathbb{Z}^+$ とする。

$X^n - 1 \in K[X]$ の K 上の最小分解体を K の<u>n 分拡大 (n − th cyclotomic extension)</u>といい、ある n に対する n 分拡大を<u>円分拡大 (cyclotomic extension)</u>という。とくに $K = \mathbb{Q}$ のとき n 分体、円分体という。

$p \mid n$ のとき、 $n = p^e m$ かつ $p \nmid m$ となる $e, m \in \mathbb{Z}^+$ が存在して、 $X^n - 1 = X^{p^e m} - 1 = (X^m - 1)^{p^e}$ となるので $X^n - 1$ の最小分解体と $X^m - 1$ の最小分解体は一致するから以降は $p \nmid n$ で考える。

$X^n - 1 \in K[X]$ が分離的であるときは定義 (12.2) より有限次 Galois 拡大である。

補題 12.21. $\mathrm{char}(K) = p > 0$ であるとき $X^n - 1 \in K[X]$ について以下は同値。

(1) $p \nmid n$

(2) $X^n - 1$ は分離的。

Proof. 命題 (9.4) の (1) ⇔ (4) より $X^n - 1$ は分離的 ⇔ $X^n - 1 \notin K[X^p]$ ⇔ $p \nmid n$ なので成立。 □

Rem 12.22. 補題 (12.21) の同値からいま $p \nmid m$ で考えてるので $X^n - 1$ は分離的だから円分拡大は Galois 拡大になる。

定義 12.23. K の元 ζ が 1 の n 乗根とはある $n \in \mathbb{Z}^+$ に対して $\zeta^n = 1$ となることである。原始 n 乗根とは ζ の位数が n であることである。つまり原始 n 乗根は n 乗して初めて 1 になる K の元のこと。

補題 12.24. K の代数閉包を Ω とし、それに含まれる $1(\in K)$ の n 乗根全体の集合を $\mu_n(:= \{1$ の n 乗

根 $\in \Omega\}$) とする。このとき μ_n は K の積で群を成す。これは原始 n 乗根をもち、それの冪乗で任意の μ_n の元を表せる。

Proof. 結合法則は K より成り立つ。$\zeta_i, \zeta_j \in \mu_n$ に対して $(\zeta_i\zeta_j)^n = \zeta_i^n\zeta_j^n = 1 \cdot 1 = 1$ より $\zeta_i, \zeta_j \in \mu_n$ なので積で閉じている。単位元は $1 \in K$ が $1^n = 1$ より存在している。$\zeta_i\zeta_i^{n-1} = \zeta_i^n = 1$ から $\zeta_i^{-1} = \zeta_i^{n-1}$ から逆元が存在するので μ_n は群。

とくにこれは $K^\times$ の有限部分群なので補題 (12.13) から巡回群になるので生成元 $\zeta \in \mu_n$ が存在する。これは位数 n なので定義 (12.23) から原始 n 乗根である。したがって $|\mu_n| \le n$ と ζ の位数が n より $|\mu_n| = n$ で $^\forall x \in \mu_n$ に対して $x = \zeta^i$ となる $j \in \mathbb{Z}, 1 \le i \le n$ が存在する。 □

補題 12.25. 補題 (12.24) の文字を用いて $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ が成り立つ。

Proof. ζ は μ_n の生成元なので $\zeta_i := \zeta^i$ とする。このとき

$$\begin{aligned} \phi : \mu_n &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \zeta_i = \zeta^i &\longmapsto i \end{aligned}$$

とすると $\zeta^i = \zeta^j$ のとき $\zeta^i\zeta^{n-i} = \zeta^j\zeta^{n-i} \Leftrightarrow 1 = \zeta^{n+j-i} \Leftrightarrow 1 = \zeta^{j-i}$ より $j - i \in n\mathbb{Z}$ から $j = i \in \mathbb{Z}/n\mathbb{Z}$ なので写像になっている。$i = j$ のとき $\zeta^i = \zeta^j$ より単射で $^\forall i \in \mathbb{Z}/n\mathbb{Z}$ で $1 \le i \le n$ だから $\zeta^i \in \mu_n$ を取ればいいから全射。また、 $\phi(\zeta^i\zeta^j) = \phi(\zeta^{i+j}) = i + j, \phi(\zeta^i) + \phi(\zeta^j) = i + j$ より群準同型になっているため $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ である。 □

補題 12.26. 補題 (12.24) の文字を用いて $\mathrm{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$ が成り立つ。

Proof. μ_n 上で

$$\begin{aligned} \phi : \mu_n &\longrightarrow \mu_n \\ \zeta(:= \zeta_1) &\longmapsto \phi(\zeta) \\ \zeta_i &\longmapsto \phi(\zeta_i) = \phi(\zeta)^i (1 \le i \le n) \end{aligned}$$

とすると μ_n の元は ζ の冪で全て表せるので ϕ が一意に定まり、準同型になる。もし $\phi(\zeta)$ が μ_n の原始 n 乗根でないとするとある $1 \le j \le n$ で $\phi(\zeta)^j = 1$ となる。しかし、 ϕ が準同型より $\phi(\zeta^j) = 1$ から $\zeta^j = 1$ となりこれは ζ が原始 n 乗根であることに矛盾するので $\phi(\zeta)$ も原始 n 乗根である。$\phi(\zeta) \in \mu_n$ より $\phi(\zeta) = \zeta^a$ となる $a \in \mathbb{Z}^+, 1 \le a \le n$ が存在している。$a = 1$ となると a と n は互いに素であるから $a \in (\mathbb{Z}/n\mathbb{Z})^*$ である。$a \ne 1$ のとき $a \mid m$ であるとすると $ak = n$ となる $k \in \mathbb{Z}^+, 1 \le k < n$ があり $a = n/k$ となる。$\phi(\zeta)^k = (\zeta^{n/k})^k = \zeta^n = 1$ となり、これは $\phi(\zeta)$ が原始 n 乗根であることに矛盾するから $a \nmid m$ なので $a \in (\mathbb{Z}/n\mathbb{Z})^*$ この $a_\phi := a$ を取れば

$$\begin{aligned} \mathrm{Aut}(\mu_n) &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \phi &\longmapsto a_\phi \end{aligned}$$

とできてこの a で ϕ が一意に定まるから全単射である。$\phi \circ \varphi(\zeta) = \phi(\zeta^{a_\varphi}) = (\zeta^{a_\varphi})^{a_\phi} = \zeta^{a_\varphi + a_\phi}$ と $\phi(\zeta) = \zeta^{a_\phi}, \varphi(\zeta) = \zeta^{a_\varphi}$ より準同型になるので $\mathrm{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$ が成立する。 □

命題 12.27. K_n を K の n 分拡大とすると Rem (12.22) から K_n/K は Galois なので $G_n := \mathrm{Aut}_K(K_n) =$

$\mathrm{Gal}(K_n/K)$ とする。ζ を原始 n 乗根とし、$\sigma \in G_n$ に対して $\sigma(\zeta) = \zeta^{a_\sigma}$ となる $a_\sigma \in \mathbb{Z}^+$ をとる。このとき

$$\begin{aligned} \chi_n : G_n &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^*(\cong \mathrm{Aut}(\mu_n)) \\ \sigma &\longmapsto a_\sigma \end{aligned}$$

は単射群準同型となる。この χ_n を<u>n 次円分指標 (cyclotomic character)</u>といい Galois 表現の一種である。

Proof. $\sigma \in G_n$ に対して補題 (12.26) と同様に $\sigma(\zeta) = \zeta^{a_\sigma}$ で一意に定まるから χ_n は単射群準同型である。$^\forall a \in (\mathbb{Z}/n\mathbb{Z})^*$ に対して $\phi(\zeta) = \zeta^a$ は K を固定するとは限らないので全射にはならない。 □

定義 12.28. $K = \mathbb{Q}$ のとき、その代数閉包を $\overline{\mathbb{Q}}$ としてその中で考える。

$$\begin{aligned} \Phi_n(X) &:= \prod_{\zeta:1 \text{ の原始 } n \text{ 乗根}} (X - \zeta) \\ &= (\zeta \text{の } \mathbb{Q} \text{ 上の最小多項式}) \\ &= (X^n - 1 \text{ の既約成分で} \zeta \text{を根に持つもの}) \end{aligned}$$

としてこの $\Phi_n(X)$ を<u>第 n 次円分多項式 (cyclotomic polynomial)</u>という。このとき $X^n - 1 = \prod_{d|n} \Phi_d(X)$ と $\deg(\Phi_n = \varphi(n)$ が成り立つ。ただしここで $\varphi(n)$ は Euler の関数であって $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ を満たす。

定理 12.29. (Gauss)
n 次円分多項式 Φ_n と n 次円分指標 χ_n で次が成り立つ。
(1) Φ_n は $\mathbb{Q}[X]$ において既約。
(2) $\chi_n : \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ は同型でとくに $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \phi(n)(= |(\mathbb{Z}/n\mathbb{Z})^*|)$ となる。

Rem 12.30. $\mathbb{Q}(\mu_\infty) := \mathbb{Q}(1$ の任意の冪根$)$ を<u>全円分体</u>という。このとき

$$\mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^* \cong \hat{\mathbb{Z}}^\times$$

となる。

Rem 12.31. Kronecker-weber の定理
$\mathbb{Q}$ の任意の Abel 拡大は $\mathbb{Q}(\mu_\infty)$ に含まれる。つまり、$\mathbb{Q}(\mu_\infty)$ は $\mathbb{Q}$ の最大 Abel 拡大であり $\mathbb{Q}^{\mathrm{ab}}$ とも書く。
$K = \mathbb{Q}(\sqrt{-m})$ の場合の最大 Abel 拡大は Kronecker の青春の夢と呼ばれていてそれ以外の場合は Hilbert の 12th problem として上がっている。

12.7 Kummer 拡大

以下では $n \in \mathbb{Z}^+$ と K : 体とする。ただし K は K の代数閉包におけるある 1 の原始 n 乗根 ζ を含んでいるとする。とくに $\mathrm{char}(K) = p > 0$ のときは $p \nmid n$ とする。

定義 12.32. 群 G が<u>n で零化される (annihilated by n)</u>とは $^\forall g \in G, g^n = e$ となること。

定義 12.33. 拡大 L/K が<u>冪数 (定義 (12.12)) が n を割り切る Abel 拡大 (abelian of exponent dividing n)</u>とはこの拡大が Abel 拡大でその Galois 群 $\mathrm{Gal}(L/K)$ が n で零化されること。冪数は元の位数の最小公倍数であったので任意の元は冪数乗すると単位元になるため n で零化されるときその冪数は文字通り n を割り切っている。

命題 12.34. $a \in K^\times$ に対して $X^n - a$ の K の代数閉包に入っているある根を $x := \sqrt[n]{a}$ とする。このとき他の根は $x\zeta^i$ $(1 \leq i \leq n-1)$ であり、$L = K(x)$ は $X^n - a$ の最小分解体で L/K が冪数が n を割り切る Abel 拡大となる。このような拡大 L/K を Kummer 拡大という。

Proof. 仮定より $\zeta \in K$ なので $X^n - a$ のすべての根は $L = K(x)$ に含まれるので $X^n - a$ の最小分解体になっている。$X^n - a$ のすべての根は $x\zeta^i$ で書かれるので重根を持たないから $X^n - a$ は分離多項式である。したがって定義 (12.2) より L/K は有限次 Galois 拡大である。

冪数が n を割り切ることを示す。${}^\forall\sigma \in G := \mathrm{Gal}(L/K)$ をとる。σ は準同型であることと $\sigma|_K = \mathrm{id}_K$ であり、$a \in K^\times$ から $\sigma(x)^n = \sigma(x^n) = \sigma(a) = a$ となる。したがって $\sigma(x)$ も $X^n - a$ の根だから $\sigma(x) = x\zeta^i$ となる整数 $1 \leq i \leq n$ が存在する。よって合成写像 σ^n を考えると $\zeta \in K$ より $\zeta^i \in K$ だから

$$\begin{aligned}\sigma^n(x) &= \sigma^{n-1} \circ \sigma(x) \\ &= \sigma^{n-1}(x\zeta^i) \\ &= \sigma^{n-1}(x)\dot{\sigma}^{n-1}(\zeta^i) \\ &= \zeta^i \sigma^{n-1}(x) \\ &\vdots \\ &= (\zeta^i)^n x = x\end{aligned}$$

なので $\sigma^n(x) = x$ である。$\sigma|_K = \mathrm{id}_K$ だから $\sigma^n|_K = \mathrm{id}_K$ なので $\sigma^n = \mathrm{id}_L$ より定義 (12.32) から G は n で零化される。

G が Abel であることを示す。$\sigma, \sigma' \in G$ をとる。上記と同様に $\sigma(x) = x\zeta^i, \sigma'(x) = x\zeta^j$ となる i, j が存在する。K 上ではともに恒等写像だから $\sigma\sigma'|_K = \sigma'\sigma|_K$ である。また、 $\sigma\sigma'(x) = \sigma(x\zeta^j) = \sigma(x)\sigma(\zeta^j) = x\zeta^i\zeta^j = x\zeta^{i+j}$ と $\sigma'\sigma(x) = \sigma'(x\zeta^i) = \sigma'(x)\sigma'(\zeta^i) = x\zeta^j\zeta^i = x\zeta^{j+i} = x\zeta^{i+j}$ より $\sigma\sigma'(x) = \sigma'\sigma(x)$ より $\sigma\sigma' = \sigma'\sigma$ なので Abel である。 □

命題 12.35. 命題 (12.34) の記号を用いる。$\mu_n := \{1 \text{ の } n \text{ 乗根} \in \overline{K}\}$ としたとき

$$\begin{aligned}\chi_a : G &\longrightarrow \mu_n \\ \sigma &\longmapsto \zeta^i\end{aligned}$$

は単射群準同型である。ただし $\sigma(x) = \zeta^i x$ を満たしている。よって補題 (12.25) から G は $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ の部分群に同型である。

Proof. $\sigma = \tau$ のとき写像として同じなので $\sigma(x) = x\zeta^i = \tau(x)$ より χ_a は写像になっている。$\chi_a(\sigma) = 1 = \zeta^0$ のとき $\sigma(x) = x\dot{1} = x$ より $\sigma = \mathrm{id}_K$ なので χ_a は単射。$\sigma, \tau \in G$ について $\sigma(x) = x\zeta^i, \tau(x) = x\zeta^j$ とすると $\zeta \in K$ から $\sigma\tau(x) = \sigma(x\zeta^j) = \sigma(x)\sigma(\zeta^j) = x\zeta^i\zeta^j = x\zeta^{i+j}$ より $\chi_a(\sigma\tau) = \zeta^{i+j}$ と $\chi_a(\sigma)\chi_n(\tau) = \zeta^i\zeta^j = \zeta^{i+j}$ より χ_a は単射準同型。 □

系 12.36. a が $K^\times$ で n の任意の約数 d において d 乗元でないとする。つまり剰余体 $K^\times/(K^\times)^n$ において a の像の位数が n であるとする。このとき $\chi_a : G \longrightarrow \mu_n$ は同型になる。

Proof. 命題 (12.35) より χ_a は単射準同型なのである μ_n の部分群と同型である。$\mathrm{Im}(\chi_a) \subset \mu_n$ で μ_n の部分群は Lagrange の定理から n のある約数 m を位数で持つから $\chi_a \cong \mu_m$ となる。$f := \prod_{\gamma\in\mu_m}(X - \gamma x) \in L[X]$ に任意の $\sigma \in G$ を作用させると $\sigma f = \prod_{\gamma\in\mu_m}(X - \sigma(\gamma x))$ となって $\gamma \in K$ より $\sigma(x) = \gamma' x, \gamma' \in \mu_m$

に対して $\sigma(\gamma x)=\sigma(\gamma)\sigma(x)=\gamma\gamma' x$ となる。そして μ_m は有限群だから γ が全体を動くとき $\gamma\gamma'$ も全体を動くので $\sigma f=f$ となる。任意の G の元で固定されるから L/K が Galois より $f\in K[X]$ である。また、$(\gamma x)^m=\gamma^m x^m=x^m$ より γx は x^m の m 乗根である。また、ある原始 m 乗根の冪も μ_m に含まれるので $|\mu_m|=m$ から $\deg(f)=m$ だから X^m-x^m の K の代数閉包での根はすべて γx で書けるから $f=X^m-x^m$ となる。$f\in K[X]$ より $x^m\in K^\times$ である。$a^m=(x^n)^m=(x^m)^n\in(K^\times)^n$ だから a の $(K^\times)/(K^\times)^n$ への像の位数が n であることより $n\leq m$ を満たす。$m|n$ より $m\leq n$ でもあるから $n=m$ より $\mu_m=\mu_n$ である。したがって $G\cong\mu_m=\mu_n$ より χ_a は同型写像。 □

定理 12.37. Hilberts Satz 90

L/K が n 次巡回拡大のとき $\mathrm{Gal}(L/K)$ の生成元を σ とすると $\mathrm{N}_{L/K}(a)=1$ となる $a\in L$ について $a=\sigma(b)/b$ となる $b\in L$ が存在する。

定理 12.38. K の n 次巡回拡大 L はある $a\in(K^\times\cap(L^\times)^n)/(K^\times)^n$ により $L=K(\sqrt[n]{a})$ と書ける。

Proof. L/K は n 次巡回拡大なので $G:=\mathrm{Gal}(L/K)$ としたとき G は位数 n の巡回群だから $\chi:G\longrightarrow\mu_n$ が同型となる χ が存在する。G の生成元を σ とすると $\chi(\sigma)\in\mu_n\subset K$ だから例 (10.2) より $\mathrm{N}_{L/K}(\chi(\sigma))=(\chi(\sigma))^n=1$ なので Hilberts Satz 90 (12.37) より $\chi(\sigma)=\sigma(\theta)/\theta$ となる $\theta\in L^\times$ が存在する。$(\chi(\sigma))^n=1$ より $\sigma(\theta)^n/\theta^n=1$ なので $\sigma(\theta^n)=\theta^n$ より θ^n は G の生成元で固定されるため、G の任意の元で固定されるから L/K が Galois より $\theta^n\in K^\times$ となるから $a:=\theta^n$ とおく。$\theta\in L^\times$ より $a=\theta^n\in(L^\times)^n$ でもあるから $a\in K^\times\cap(L^\times)^n$ である。a は任意の θ^n の n 乗根をとっていいからそれをまとめて書くために $a\in K^\times\cap(L^\times)^n/(K^\times)^n$ として a を取り直す。

$f\in K[X]$ を θ の最小多項式とする。このとき $\chi(\sigma)\in\mu_n$ から $\chi(\sigma)=\zeta^j$ とおくと $1\leq i\leq n$ で $\sigma^i(\theta)=\sigma^{i-1}(\zeta^j\theta)=\cdots=(\zeta^j)^i\theta$ となる。$(\sigma^i(\theta))^n=(\zeta^{i+j}\theta)^n=\theta^n=a$ より $\sigma^i(\theta)$ も $X^n-a\in K[X]$ の根である。$\sigma^i\in G$ より $f(\sigma^i(\theta))=\sigma^i(f(\theta))=0$ だから $\sigma^i(\theta)$ は θ と同じ最小多項式を持つ。したがって θ を根にもつ X^n-a は $\zeta^{i+j}\theta$ の n 根をもち、これ以上次数が下がらないので $f=X^n-a$ である。そして $\theta\in L$ と $\zeta\in K$ なので $\zeta^{i+j}\theta\in L$ だから f は $L[X]$ で一次の積に分解されてその根はすべて異なるから分離的である。$[K(\theta):K]=\deg(f)=n=[L:K]$ で $K(\theta)\subset L$ より $L=K(\theta)=K(\sqrt[n]{a})$ なので示された。 □

Fact 12.39. より一般に L/K を K の冪数が n を割り切る最大 Abel 拡大とすると

$$\begin{aligned}\mathrm{Gal}(L/K)\times K^\times/(K^\times)^n&\longrightarrow\mu_n\\(\sigma,a)&\longmapsto\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\end{aligned}$$

は双線形で一意に定まる。これより $\mathrm{Gal}(L/K)\cong\mathrm{Hom}(K^\times/(K^\times)^n,\mu_n)$ も従う。

12.8 Artin-Schreier 拡大

以下では $\mathrm{char}(K)=p>0$ とする。$(\Leftrightarrow K\supset\mathbb{F}_p)$

命題 12.40. K の代数閉包 Ω 上で以下のように対応を定める。

$$\begin{aligned}\mathscr{P}:\Omega&\longrightarrow\Omega\\x&\longmapsto x^p-x\end{aligned}$$

するとこれは Ω の加法群の準同型になり、とくに $\mathscr{P}|_K$ は K の加法群の準同型になる。その核は $\mathbb{F}_p$ である。

Proof. $x=y$ のとき明らかに $x^p-x=y^p-y$ より $\mathscr{P}$ は写像。$\mathscr{P}(x+y)=(x+y)^p-(x+y)=x^p+y^p-x-y=(x^p-x)+(y^p-y)=\mathscr{P}(x)+\mathscr{P}(y)$ より加法群の準同型。また、 $\mathbb{F}_p\subset K\subset\Omega$ で系 (12.15) から Ω のなかで $\mathbb{F}_p=\{x\in\Omega|x^p=x\}$ と書けるから $\mathscr{P}(x)=0\Leftrightarrow x^p-x=0\Leftrightarrow x^p=x\Leftrightarrow x\in\mathbb{F}_p$ より $\ker(\mathscr{P})=\mathbb{F}_p$ となる。$\mathbb{F}_p\subset K$ なので $\ker(\mathscr{P}|_K)=\mathbb{F}_p$ にもなる。 □

補題 12.41. $a\in K$ に対して $f:=X^p-x-a\in K[X]$ とおいてそのある根を $x\in\Omega$ とおく。このとき f が K 上で可約であることと $a\in\mathscr{P}(K)$ は必要十分である。

Proof. $a\in\mathscr{P}(K)\Leftrightarrow{}^\exists\alpha\in K,\alpha^p-\alpha=a=x^p-x$ から $\mathrm{char}(K)=p>0$ より $(x-\alpha)^p=x-\alpha$ なので $\mathbb{F}_p=\{x\in\Omega|x^p=x\}$ から $x-\alpha\in\mathbb{F}_p\subset K$ である。$\alpha\in K$ より $(x-\alpha)+\alpha=x\in K$ となる。また、$x\in K$ のとき $x^p-x-a=0\Leftrightarrow a=x^p-x$ より $a\in\mathscr{P}(K)$ となる。したがって $a\in\mathscr{P}(K)\Leftrightarrow x\in K$ が成り立つので f が K 上可約 $\Leftrightarrow x\in K$ を示せば良い。

$g(X)\in K[X]$ を x の K 上の最小多項式とすると $f(x)=0$ と $\deg(g)$ の最小生から $g(X)|f(X)$ である。$f(X)=X^p-X-a$ はその形から $f(X)=f(X+1)$ なので $f(X)=f(X+1)=\cdots=f(X+i)=\cdots=f(X+(p-1)),i\in\mathbb{F}_p$ となっている。f が p 次であることと ${}^\forall i\in F_p$ に対して $0=f(x)=f(x+i)$ より $x+i$ も f の根になっているから f の根はすべて $x+i$ の形で書ける。

ここで $g(X)=g(X+1)$ のとき同様に $g(X)=g(X+1)=\cdots=g(X+i)=\cdots=g(X+(p-1))$ である。$g(X)$ は x を根に持っていたから $0=g(x)=g(x+i)$ より $x+i$ も $g(X)$ の根になるので少なくとも p 個の相異なる根を持っていて $g|f$ から $\deg(g)\le p$ なので $\deg(g)=p$ となり、$g(X)=\prod_{i=0}^{p-1}(X-(x+i))$ と書ける。f の根もすべて $x+i$ であるから $g=f$ となる。したがって g が最小多項式なので f は既約。対偶をとって f が可約 $\Rightarrow g(X)\neq g(X+1)$ が言えた。

$g(X)\neq g(X+1)$ のときある $k\in\mathbb{F}_p$ で $g(X)=g(X+k)$ となったとする。このとき $0\le l\le p-1$ で $g(X)=g(X+k)=g(X+2k)=\cdots=g(X+lk)=\cdots=g(X+(p-1)k)$ となる。lk は l によってそれぞれ異なり、それが p 個あるのである l で $g(X+1)=g(X+lk)$ となるものが存在する。これは $g(X)\neq g(X+1)(=g(X+lk))$ に矛盾するので $g(X),g(X+1),\ldots,g(X+(p-1))$ は相異なる。$g(X)|f(X)$ から任意の $i\in\mathbb{F}_p$ で $g(X+i)|f(X+i)=f(X)$ となるから $\prod_{i=0}^{p-1}g(X+i)|f(X)$ となり、 $g(X+i)$ がそれぞれ異なるから $f(X)$ は可約。したがって $g(X)\neq g(X+1)\Rightarrow f$ が可約が言えた。

とくにこのとき $\deg(f)=p$ なので $f=\prod_{i=0}^{p-1}g(X+i)$ で $g(X)$ は x の K 上の最小多項式であったから $\deg(g(X+i))\le 1$ だから $g(X+i)$ は一次式であり、$g(X)=X-x\in K[X]$ となる。よって $f=\prod_{i=0}^{p-1}(X-(x+i))$ と K 上で一次式の積に分解できて $x\in K$ となる。したがって $g(X)\neq g(X+1)\Rightarrow f$ が可約 $\Rightarrow f=\prod_{i=0}^{p-1}(X-(x+i))$ と分解できる $\Rightarrow x\in K$ が言えた。

$x\in K$ のとき $x+i\in K$ だから f は K 上で $f=\prod_{i=0}^{p-1}(X-(x+i))$ と分解できて x の最小多項式 $g\in K[X]$ は $g(X)=X-x$ となるから $g(X)\neq g(X+1)$ である。したがって逆も言えて f が可約 $\Leftrightarrow x\in K$ となるので $x\in K\Leftrightarrow a\in\mathscr{P}(K)$ より示された。 □

命題 12.42. ある $a\in K$ に対して $\mathscr{P}(x)=a$ となる $x\in\Omega$ をとる。このとき $L:=K(x)$ とすると L/K は冪数が n を割り切る Abel 拡大であり、$G:=\mathrm{Gal}(L/K)$ とおいたとき加法群としての $\mathbb{F}_p$ に対して

$$\begin{aligned}\chi_a: G&\longrightarrow\mathbb{F}_p\\ \sigma&\longmapsto\sigma(x)-x\end{aligned}$$

という単射群準同型が存在する。とくに $a\in K-\mathscr{P}(K)=K-\mathrm{Im}(\mathscr{P})$ を取ったときは χ_a は全射になり、L/K は p 次巡回拡大になる。このような拡大 L/K を Artin-Shreier 拡大という。

Proof. $\mathscr{P}(x)=a$ となる x は $\mathscr{P}(x)=x^p-x=a$ より $f:=X^p-X-a\in K[X]$ の根になっている。ここで $x+i, i\in\mathbb{F}_p$ は $\mathbb{F}_p=\{x\in\Omega|x^p=x\}$ と $\mathrm{char}(K)=p>0$ なので $(x+i)^p-(x+i)-a=x^p+i^p-x-i-a=x^p-x-a=0$ より f の根になる。$1\leq i\leq p$ だから f の根はこれで全てなので $\mathbb{F}_p\subset K$ より L は f の最小分解体であり、全て根が異なるから分離多項式なので L/K は p 次 Galois 拡大となる。

$f(\sigma(x))=(\sigma(x))^p-\sigma(x)-a=\sigma(x^p-x-a)=0$ だから $\sigma(x)$ も f の根であるのである $i_\sigma\in\mathbb{F}_p$ で $\sigma(x)=x+i_\sigma$ となるから $\sigma(x)-x=i_\sigma\in\mathbb{F}_p$ となる。したがって χ_a の終域は確かに $\mathbb{F}_p$ になる。$\sigma=\tau\in G$ のとき $\sigma(x)-x=\tau(x)-x$ より χ_a は写像になっている。また、$\chi_a(\sigma)=0$ のとき $\sigma(x)-x=0\Leftrightarrow\sigma(x)=x$ より $\sigma=\mathrm{id}_L$ より χ_a は単射。$\chi_a(\sigma\circ\tau)=\sigma\circ\tau(x)-x=\sigma(x+i_\tau)-x=(x+i_\sigma)+i_\tau-x=i_\sigma+i_\tau$ であり、$\chi_a(\sigma)+\chi_a(\tau)=(\sigma(x)-x)+(\tau(x)-x)=i_\sigma+i_\tau$ より $\chi_a(\sigma\circ\tau)=\chi_a(\sigma)+\chi_a(\tau)$ だから χ_a は群準同型になる。

${}^\forall\sigma\in G$ に対して $\mathrm{char}(K)=p>0$ から $\sigma^p(x)=\sigma^{p-1}(x+i)=\sigma^{p-1}(x)+\sigma^{p-1}(i)=\sigma^{p-1}(x)+i=\cdots=x+pi=x$ より $\sigma^p(x)=x$ となる。したがって $\sigma^n=\mathrm{id}_L$ より p で零化される。$\sigma\circ\tau(x)=\sigma(x+i_\tau)=x+i_\sigma+i_\tau$ と $\tau\circ\sigma(x)=\tau(x+i_\sigma)=x+i_\tau+i_\sigma$ で $i_\sigma+i_\tau=i_\tau+i_\sigma$ より $\sigma\circ\tau=\tau\circ\sigma$ なので G は可換だから L/K は冪数が p を割り切る Abel 拡大。p が素数より冪数が 1 か p だから G は単位元のみの位数 1 の群になるか位数 p の元を持つ巡回群になるかである。

$a\in K-\mathscr{P}(K)$ を取ったとき補題 (12.41) の否定から $f=X^p-X-a$ は既約で f は x の最小多項式である。L/K は Galois より $|G|=[L:K]=\deg(f)=p=|\,\mathbb{F}_p\,|$ である。χ_a が単射なので $|G|=|\,\mathbb{F}_p\,|$ より全射になるから χ_a は同型になる。$\mathbb{F}_p$ は加法群として巡回群なので L/K は p 次の巡回拡大になる。 □

定理 12.43. $\mathbb{F}_p$ を含む体 K の p 次巡回拡大はすべて命題 (12.42) のようにして作られる。

Fact 12.44. $\mathbb{F}_p$ を含む体 K について $p\nmid n$ となる n 次巡回拡大は定理 (12.38) のようにして、p 次巡回拡大は定理 (12.43) のようにして作られる。p の冪次については K の加法群の代わりに Witt ベクトルの群を考える Artin-Shreier-Witt 理論を用いて作られる。

13 Galois 理論の基本定理の別の定式化

K : 体、 K^{sep} : K の分離閉包、 A :etale $K-alg$ に対して $\mathscr{S}(A) := \mathrm{Hom}_{K-alg}(A, K^{\mathrm{sep}})$ とおく。このとき K の絶対 Galois 群 $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ は $\mathscr{S}(A)$ に以下のように作用する。

$$\begin{aligned} G_K \times \mathscr{S}(A) &\longrightarrow \mathscr{S}(A) \\ (\sigma, f) &\longmapsto \sigma f \end{aligned}$$

ただし σf は

$$\begin{aligned} \sigma f : A &\longrightarrow K^{\mathrm{sep}} \\ x &\longmapsto (\sigma f)(x) := \sigma(f(x)) \end{aligned}$$

である。G_K は定義 (12.10) から位相群であり、この位相についてこの作用は連続になり、これは各 $f \in \mathscr{S}(A)$ の固定化群が開であることと同値になっている。

$A = K[X]/(f)$ のとき f のある根 α_i に対して $\alpha_i = X + (f)$ とすることで $\mathscr{S}(A)$ の写像が一つ定まるので $\mathscr{S}(A) \cong \{f \text{ の根 }\}$ が成り立ち、$\mathscr{S}(A)$ を多項式の根のように見ることができる。

逆に S を G_K が連続に作用する有限集合 (G_K- 集合) とすると $\mathscr{A}(S) := \mathrm{Map}_G(S, K^{\mathrm{sep}}) := \{f : S \longrightarrow K^{\mathrm{sep}} | f(\sigma(x)) = \sigma(f(x)), {}^{\forall}\sigma \in G_K\}$ とおいたとき $\mathscr{A}(S)$ は $K-alg$ でさらに有限次 etale でもある。

以上のことから以下の定理が成り立つ。

定理 13.1. 次の反圏同値がある。

$$\begin{aligned} (\text{etale}K-alg \text{ の圏}) \quad &\cong \quad (\text{有限 } G_K - \text{集合の圏}) \\ A &\longmapsto \mathscr{S}(A) \\ \mathscr{A}(S) &\longleftarrow S \\ K-alg \text{ hom} : A_1 \to A_2 &\longleftrightarrow G_K - \text{集合の射} : S_1 \leftarrow S_2 \\ \text{単射 hom} : A_1 \hookrightarrow A_2 &\longleftrightarrow \text{全射} : S_1 \twoheadleftarrow S_2 \\ \text{全射 hom} : A_1 \twoheadrightarrow A_2 &\longleftrightarrow \text{単射} : S_1 \hookleftarrow S_2 \\ A : \text{体} &\longleftrightarrow S \text{ は一つの orbit からなる} \\ A : K \text{ の Galois 拡大} &\longleftrightarrow \mathrm{Stab}_S := S \text{ の固定化群が } G_K \text{で正規} \\ A : K \text{ の Galois 拡大のとき } A/K \text{ の中間体} &\longleftrightarrow \text{全射} : (\text{一点}) \twoheadleftarrow S \text{ の中間集合} \end{aligned}$$

14 Galois cohomology

14.1 群の cohomology

定義 14.1. G : 群、 M : 加法 (Abel) 群で G は M に加群としての作用をしているとする。ここで以下のように G^n から M への写像全体の集合を $C^n(n \in \mathbb{Z}_{\geq 0})$ として定める。

$$C^n = C^n(G, M) := \{f : G^n \longrightarrow M\} = \mathrm{Map}(G^n, M)$$

ただし $G^0 = \{e\}$ と考えることで $C^0 := M$ と定める。この C^n の各元を n コチェイン (cochain)という。C^n 上へは $f, g \in C^n$ に対して $(f+g)(x) := f(x) + g(x)$ と演算を定めることで C^n は加法群となる。

定義 14.2. C^n から C^{n+1} への以下のように定まる写像 ∂ を考える。

$$\begin{aligned} \partial = \partial^n : C^n &\longrightarrow C^{n+1} \\ f &\longmapsto \partial f \end{aligned}$$

ここで $\partial f : G^{n+1} \longrightarrow M$ は G が M へ作用していることに注意して

$$\begin{aligned} \partial f(g_1, \ldots, g_{n+1}) &= g_1 f(g_2, \ldots, g_{n+1}) \\ &+ \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \ldots, g_n) \end{aligned}$$

と定める。このときこの $\partial(= \partial^n) : C^n(G, M) \longrightarrow C^{n+1}(G, M)$ は加法群の準同型になり、これを n 次のコバウンダリー (双対境界) 作用素 (coboundary operator)とよぶ。

命題 14.3. コバウンダリー作用素 ∂ に対して $\partial^{n+1} \circ \partial^n = 0$ が成り立つ。

Proof. $4 \leq n$ でまず考える。

$(\partial^{n+1} \circ \partial^n)(f)(g_1, \ldots, g_{n+2}) = \partial^{n+1}(\partial^n f)(g_1, \ldots, g_{n+2})$ なので $f' := \partial^n f$ として $\partial^{n+1} f'(g_1, \ldots, g_{n+2})$ は

$$\begin{aligned} \partial^{n+1} f'(g_1, \ldots, g_{n+2}) &= g_1 f'(g_2, \ldots, g_{n+2}) \\ &+ \sum_{i=1}^{n+1} (-1)^i f'(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+2}) \\ &+ (-1)^{n+1} f'(g_1, \ldots, g_{n+1}) \end{aligned}$$

である。$f'(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+2}) = \partial^n f(g_1, \ldots g_i g_{i+1}, \ldots, g_{n+2})$ を i の値によって計算する。

・ $i = 1$ のとき

$$\begin{aligned} \partial^n f(g_1 g_2, \ldots, g_{n+2}) &= g_1 g_2 f(g_3, \ldots, g_{n+2}) \\ &+ (-1)^1 f((g_1 g_2) g_3, g_4, \ldots, g_{n+2}) \\ &+ \sum_{k=3}^{n+1} (-1)^{k-1} f(g_1 g_2, g_3, \ldots, g_i g_{i+1}, \ldots, g_{n+2}) \\ &+ (-1)^{n+1} f(g_1 g_2, g_3, \ldots, g_n) \end{aligned}$$

・ $i=2$ のとき

$$\begin{aligned}\partial^n f(g_1, g_2g_3, g_4, \ldots, g_{n+2}) &= g_1 f(g_2g_3, g_4, \ldots, g_{n+2}) \\ &\quad + (-1)^1 f(g_1(g_2g_3), g_4, \ldots, g_{n+2}) \\ &\quad + (-1)^2 f(g_1, (g_2g_3)g_4, g_5, \ldots, g_{n+2}) \\ &\quad + \sum_{k=4}^{n+1} (-1)^{k-1} f(g_1, g_2g_3, g_4, \ldots, g_ig_{i+1}, \ldots, g_{n+2}) \\ &\quad + (-1)^{n+1} f(g_1, g_2g_3, g_4, \ldots, g_{n+1})\end{aligned}$$

・ $3 \leq i \leq n-1$ のとき

$$\begin{aligned}\partial^n f(g_1, \ldots, g_ig_{i+1}, \ldots, g_{n+2}) &= g_1 f(g_2, \ldots, g_ig_{i+1}, \ldots, g_{n+2}) \\ &\quad + \sum_{k=1}^{i-2} (-1)^k f(g_1, \ldots, g_kg_{k+1}, \ldots, g_ig_{i+1}, \ldots, g_{n+2}) \\ &\quad + (-1)^{i-1} f(g_1, \ldots, g_{i-2}, g_{i-1}(g_ig_{i+1}), g_{i+2}, \ldots, g_{n+2}) \\ &\quad + (-1)^i f(g_1, \ldots, g_{i-1}, (g_ig_{i+1})g_{i+2}, g_{i+3}, \ldots, g_{n+2}) \\ &\quad + \sum_{k=i+2}^{n+1} (-1)^{k-1} f(g_1, \ldots, g_ig_{i+1}, \ldots, g_kg_{k+1}, \ldots, g_{n+2}) \\ &\quad + (-1)^{n+1} f(g_1, \ldots, g_ig_{i+1}, \ldots, g_{n+1})\end{aligned}$$

・ $i=n$ のとき

$$\begin{aligned}\partial^n f(g_1, \ldots, g_ng_{n+1}, g_{n+2}) &= g_1 f(g_2, \ldots, g_ng_{n+1}, g_{n+2}) \\ &\quad + \sum_{k=1}^{n-2} (-1)^k f(g_1, \ldots, g_kg_{k+1}, \ldots, g_ng_{n+1}, g_{n+2}) \\ &\quad + (-1)^{n-1} f(g_1, \ldots, g_{n-1}(g_ng_{n+1}), g_{n+2}) \\ &\quad + (-1)^n f(g_1, \ldots, g_{n-1}, (g_ng_{n+1})g_{n+2}) \\ &\quad + (-1)^{n+1} f(g_1, \ldots, g_{n-1}, g_ng_{n+1})\end{aligned}$$

・ $i=n+1$ のとき

$$\begin{aligned}\partial^n f(g_1, \ldots, g_{n+1}g_{n+2}) &= g_1 f(g_2, \ldots, g_{n+1}g_{n+2}) \\ &\quad + \sum_{k=1}^{n-1} (-1)^k f(g_1, \ldots, g_kg_{k+1}, \ldots, g_n, g_{n+1}g_{n+2}) \\ &\quad + (-1)^n f(g_1, \ldots, g_{n-1}, g_n(g_{n+1}g_{n+2})) \\ &\quad + (-1)^{n+1} f(g_1, \ldots, g_n)\end{aligned}$$

となる。

また、 $g_1 f'(g_2, \ldots, g_{n+2})$ と $(-1)^{n+2} f'(g_1, \ldots, g_{n+1})$ は以下のようになる。

$$
\begin{aligned}
g_1 \partial^n f(g_2, \ldots, g_{n+2}) &= g_1 (g_2 f(g_3, \ldots, g_{n+2}) \\
&\quad + \sum_{i=2}^{n+1} (-1)^{i-1} f(g_2, \ldots, g_i g_{i+1}, \ldots, g_{n+2}) \\
&\quad + (-1)^{n+1} f(g_2, \ldots, g_{n+1})) \\
(-1)^{n+2} \partial^n f(g_1, \ldots, g_{n+1}) &= (-1)^{n+2} (g_1 f(g_2, \ldots, g_{n+1}) \\
&\quad + \sum_{i=1}^{n} (-1)^{i} f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\
&\quad + (-1)^{n+1} f(g_1, \ldots, g_n))
\end{aligned}
$$

これを $\partial^{n+1}(\partial^n f)(g_1,\dots,g_{n+2})$ の式に代入すると

$$
\begin{aligned}
\partial^{n+1}(\partial^n f)(g_1,\dots,g_{n+2} = &\{g_1g_2f(g_3,\dots,g_{n+2})\\
&+\sum_{i=2}^{n+1}(-1)^{i-1}g_1f(g_2,\dots,g_ig_{i+1},\dots,g_{n+2})\\
&+(-1)^{n+1}g_1f(g_2,\dots,g_{n+1})\}\\
&+(-1)^1\{g_1g_2f(g_3,\dots,g_{n+2})\\
&+(-1)^1f((g_1g_2)g_3,g_4,\dots,g_{n+2})\\
&+\sum_{k=3}^{n+1}(-1)^{k-1}f(g_1g_2,g_3,\dots,g_ig_{i+1},\dots,g_{n+2})\\
&+(-1)^{n+1}f(g_1g_2,g_3,\dots,g_n)\}\\
&+(-1)^2\{g_1f(g_2g_3,g_4,\dots,g_{n+2})\\
&+(-1)^1f(g_1(g_2g_3),g_4,\dots,g_{n+2})\\
&+(-1)^2f(g_1,(g_2g_3)g_4,g_5,\dots,g_{n+2})\\
&+\sum_{k=4}^{n+1}(-1)^{k-1}f(g_1,g_2g_3,g_4,\dots,g_ig_{i+1},\dots,g_{n+2})\\
&+(-1)^{n+1}f(g_1,g_2g_3,g_4,\dots,g_{n+1})\}\\
&+\sum_{i=3}^{n-1}(-1)^i\{g_1f(g_2,\dots,g_ig_{i+1},\dots,g_{n+2})\\
&+\sum_{k=1}^{i-2}(-1)^kf(g_1,\dots,g_kg_{k+1},\dots,g_ig_{i+1},\dots,g_{n+2})\\
&+(-1)^{i-1}f(g_1,\dots,g_{i-2},g_{i-1}(g_ig_{i+1}),g_{i+2},\dots,g_{n+2})\\
&+(-1)^if(g_1,\dots,g_{i-1},(g_ig_{i+1})g_{i+2},g_{i+3},\dots,g_{n+2})\\
&+\sum_{k=i+2}^{n+1}(-1)^{k-1}f(g_1,\dots,g_ig_{i+1},\dots,g_kg_{k+1},\dots,g_{n+2})\\
&+(-1)^{n+1}f(g_1,\dots,g_ig_{i+1},\dots,g_{n+1})\}\\
&+\{g_1f(g_2,\dots,g_ng_{n+1},g_{n+2})\\
&+\sum_{k=1}^{n-2}(-1)^kf(g_1,\dots,g_kg_{k+1},\dots,g_ng_{n+1},g_{n+2})\\
&+(-1)^{n-1}f(g_1,\dots,g_{n-1}(g_ng_{n+1}),g_{n+2})\\
&+(-1)^nf(g_1,\dots,g_{n-1},(g_ng_{n+1})g_{n+2})\\
&+(-1)^{n+1}f(g_1,\dots,g_{n-1},g_ng_{n+1})\}\\
&+\{g_1f(g_2,\dots,g_{n+1}g_{n+2})\\
&+\sum_{k=1}^{n-1}(-1)^kf(g_1,\dots,g_kg_{k+1},\dots,g_n,g_{n+1}g_{n+2})\\
&+(-1)^nf(g_1,\dots,g_{n-1},g_n(g_{n+1}g_{n+2}))\\
&+(-1)^{n+1}f(g_1,\dots,g_n)\}\\
&+\{(-1)^{n+2}(g_1f(g_2,\dots,g_{n+1})\\
&+\sum_{i=1}^{n}(-1)^if(g_1,\dots,g_ig_{i+1},\dots,g_{n+1})\\
&+(-1)^{n+1}f(g_1,\dots,g_n))\}
\end{aligned}
$$

□

定義 14.4. 以下のように $n \in \mathbb{Z}_{\geq 0}$ に対して定める Z^n をn-th (次) コサイクル (双対輪体)といい、B^n をn-th (次) コバウンダリー (境界輪体)という。

$$Z^n = Z^n(G, M) := \ker(\partial^n)$$
$$B^n = B^n(G, M) := \mathrm{Im}(\partial^{n-1})$$

ただし $B^0 := 0$ とする。このとき命題 (14.3) から $\partial^n \circ \partial^{n-1} = 0$ なので $\partial^n(\mathrm{Im}(\partial^{n-1})) = 0$ より $B^n \subset Z^n$ が成り立っている。よって剰余群 Z^n/B^n が定義できて

$$H^n = H^n(G, M) := Z^n(G, M)/B^n(G, M)$$

を G の M 係数のn-th (次) コホモロジー群 (cohomology)という。

例 14.5. $n = 0$ のときのコホモロジー群を考える。$Z^0 = \ker(\partial^0)$ であり、定義から $\partial^0 : C^0(= M) \longrightarrow C^1, x \longmapsto \partial^0 x$ と、$\partial^0 x(g) = gx - x$ なので $Z^0 = \{gx - x = 0 \Leftrightarrow gx = x | x \in M, {}^\forall g \in G\}$ となる。gx は M の元への G の作用でありそれがどんな $g \in G$ でも x になるから M の中で G によって固定されるので $Z^0 = M^G$ である。$B^0 := 0$ だったのでコホモロジー群 H^0 は $H^0 = Z^0/B^0 = M^G$ である。

例 14.6. $n = 1$ のときのコホモロジー群を考える。$Z^1 = \ker(\partial^1)$ で $\partial^1 : C^1 \longrightarrow C^2, f \longmapsto \partial^1 f$ となって $\partial^1 f(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1)$ となるから $Z^1 = \{f \in C^1 | g_1 f(g_2) - f(g_1 g_2) + f(g_1) = 0 \Leftrightarrow f(g_1 g_2) = g_1 f(g_2) + f(g_1), {}^\forall g_1, g_2 \in G\}$ となる。$B^1 = \mathrm{Im}(\partial^0) = \{\partial^0 x | x \in M, \partial^0 x(g) = gx - x\}$ となっている。いま作用が $G \times M \longrightarrow M, (g, x) \longmapsto gx = x$ として自明なものであるときを考えると $Z^1 = \{f \in C^1 | f(g_1 g_2) = f(g_1) + f(g_2), {}^\forall g_1, g_2 \in G\}$ でこれは G から M への群準同型なので $Z^1 = \mathrm{Hom}_{群}(G, M)$ となる。$B^1 = \{\partial^0 x | x \in M, \partial^0 x(g) = gx - x = x - x = 0\} = 0$ となるから $n = 1$ のときのコホモロジー群 H^1 は $H^1 = \mathrm{Hom}_{群}(G, M)$ となる。

命題 14.7. G 加群 M_1, M_2, M_3 に対して、$C_i^n := C^n(G, M_i), Z_i^n := Z^n(G, M_i), B_i^n := B^n(G, M_i), H_i^n := H^n(G, M_i)$ と書くことにする。また、 n 次コバウンダリー作用素 $\partial^n : C_i^n \longrightarrow C_i^{n+1}$ を ∂_i^n と書くことにする。ここで以下のような行が完全列になっていてそれぞれ写像が可換な図を考える。

$$\begin{tikzcd}
0 \arrow[r, "f_{01}^{n-1}"] & C_1^{n-1} \arrow[r, "f_{12}^{n-1}"] \arrow[d, "\partial_1^{n-1}"] & C_2^{n-1} \arrow[r, "f_{23}^{n-1}"] \arrow[d, "\partial_2^{n-1}"] & C_3^{n-1} \arrow[r, "f_{30}^{n-1}"] \arrow[d, "\partial_3^{n-1}"] & 0 \\
0 \arrow[r, "f_{01}^{n}"] & C_1^{n} \arrow[r, "f_{12}^{n}"] \arrow[d, "\partial_1^{n}"] & C_2^{n} \arrow[r, "f_{23}^{n}"] \arrow[d, "\partial_2^{n}"] & C_3^{n} \arrow[r, "f_{30}^{n}"] \arrow[d, "\partial_3^{n}"] & 0 \\
0 \arrow[r, "f_{01}^{n+1}"] & C_1^{n+1} \arrow[r, "f_{12}^{n+1}"] \arrow[d, "\partial_1^{n+1}"] & C_2^{n+1} \arrow[r, "f_{23}^{n+1}"] \arrow[d, "\partial_2^{n+1}"] & C_3^{n+1} \arrow[r, "f_{30}^{n+1}"] \arrow[d, "\partial_3^{n+1}"] & 0 \\
& {} & {} & {} &
\end{tikzcd}$$

完全列であることから f^i_{12} は単射で f^i_{23} は全射である。このとき

$$\begin{aligned} \partial^* : H^n_3 &\longrightarrow H^{n+1}_1 \\ \overline{z} = z + B^n_3 &\longmapsto \overline{x} = x + B^{n+1}_1 := \partial^*(\overline{z}) \end{aligned}$$

で定まる準同型写像が存在することを示す。

Proof. (1) ∼ (4) に分けて示す。ただし、より一般の完全列に対して (1) ∼ (3) は蛇の補題から $\partial^* : \ker(\partial^n_3) = Z^n_3 \longrightarrow \mathrm{Coker}(\partial^{n+1}_1) = C^{n+1}_1/B^{n+1}_1$ が境界準同型写像の存在性から示される。(1) では終域が C^{n+1}_1 よりさらに Z^{n+1}_1 に狭まることを、(4) ではとくに $H^n_3 \longrightarrow H^{n+1}_1$ で定義できるようになることがさらに示される。

(1) 以下のような対応 ∂^*_1 が存在すること

$$\begin{aligned} \partial^*_1 : Z^n_3 &\longrightarrow Z^{n+1}_1 \\ z &\longrightarrow x \end{aligned}$$

証明では以下のように元を取っていく。

$$\begin{tikzcd} & y := (f^n_{23})^{-1}(z) \arrow[r, "f^n_{23}"] \arrow[d, "\partial^n_2"] & z \arrow[d, "\partial^n_3"] \\ x := (f^{n+1}_{12})^{-1} \circ \partial^n_2(y) \arrow[r, "f^{n+1}_{12}"] \arrow[d, "\partial^{n+1}_1"] & \partial^n_2(y) \arrow[r, "f^{n+1}_{23}"] & 0 \\ 0 & & \end{tikzcd}$$

$z \in Z^n_3 = \ker(\partial^n) \subset C^n_3$ をとる。このとき f^n_{23} は全射なので $f^n_{23}(y) = z$ となる $y \in C^n_2$ が少なくとも 1 つ存在する。このうちの一つを y としてとると $y = (f^n_{23})^{-1}(z)$ である。ここで図式が可換より $\partial^n_3 \circ f^n_{23} = f^{n+1}_{23} \circ \partial^n_2$ なので $z \in \ker(\partial^n_3)$ だから $\partial^n_3 \circ f^n_{23}(y) = \partial^n_3(z) = 0$ なので $f^{n+1}_{23} \circ \partial^n_2(y) = 0$ より $\partial^n_2(y) \in \ker(f^{n+1}_{23})$ である。完全列であることから $\ker(f^{n+1}_{23}) = \mathrm{Im}(f^{n+1}_{12})$ と f^{n+1}_{12} は単射だからあるただ一つの $x \in C^{n+1}_1$ が存在して $f^{n+1}_{12}(x) = \partial^n_2(y)$ となるからこの x により $\partial^*(z) := x = (f^{n+1}_{12})^{-1} \circ \partial^n_2 \circ (f^n_{23})^{-1}(z)$ として定めると $y = (f^n_{23})^{-1}(z)$ が一つに定まらないことより対応 $\partial^*_1 : Z^n_3 \longrightarrow C^{n+1}_1$ が作られる。

ここで $\partial^{n+1}_1(x) = \partial^{n+1}_1((f^{n+1}_{12})^{-1} \circ \partial^n_2(y))$ である。図式が可換であることと f^i_{12} が単射だから $(f^{n+1}_{12})^{-1} \circ \partial^n_2 = \partial^n_1 \circ (f^n_{12})^{-1}$ より $\partial^{n+1} \circ \partial^n = 0$ に注意すれば $\partial^{n+1}_1(x) = \partial^{n+1}_1((f^{n+1}_{12})^{-1} \circ \partial^n_2(y)) = \partial^{n+1}_1(\partial^n_1 \circ (f^n_{12})^{-1}(y)) = (\partial^{n+1}_1 \circ \partial^n_1) \circ (f^n_{12})^{-1}(y) = 0$ となるから $x \in \ker(\partial^{n+1}_1) = Z^{n+1}_1$ となる。したがって対応 ∂^*_1 の終域は Z^{n+1}_1 となるので上記のような対応が作られる。

(2) 対応 ∂^*_1 から以下のような写像 ∂^*_2 が作られること

$$\begin{aligned} \partial^*_2 : Z^n_3 &\longrightarrow H^{n+1}_1 (:= Z^{n+1}_1/B^{n+1}_1) \\ z &\longrightarrow \overline{\partial^*_1(z)} = \overline{x} = x + B^{n+1}_1 \end{aligned}$$

いま ∂^*_1 によって $z = z' \in Z^n_3$ に対し、ある $y = (f^n_{23})^{-1}(z), y' = (f^n_{23})^{-1}(z')$ は $y \neq y'$ になる可能性がある。その y, y' に対しては ∂^n_2 が写像で f^n_{12} が単射よりただ一つの $x = (f^{n+1}_{12})^{-1} \circ \partial^n_2(y), x' = (f^{n+1}_{12})^{-1} \circ \partial^n_2(y')$ が存在する。このとき $x - x' \in B^{n+1}_1$ であれば $\overline{x} = \overline{x'}$ となるから ∂^*_2 が写像になる。したがって $x - x' \in B^{n+1}_1$ を示せばいい。

以下のような可換性を用いる。

$$\begin{tikzcd}
w := (f_{12}^n)^{-1}(y) - (f_{12}^n)^{-1}(y') \arrow[r, "f_{12}^n"] \arrow[d, "\partial_1^n"] & y - y' \arrow[d, "\partial_2^n"] \\
x - x' \arrow[r, "f_{12}^{n+1}"] & \partial_2^n(y) - \partial_2^n(y')
\end{tikzcd}$$

$x - x' = (f_{12}^{n+1})^{-1} \circ \partial_2^n(y) - (f_{12}^{n+1})^{-1} \circ \partial_2^n(y')$ である。f_{12}^i が単射で図式が可換より $(f_{12}^{n+1})^{-1} \circ \partial_2^n = \partial_1^n \circ (f_{12}^n)^{-1}$ となる。よって ∂_1^n が準同型だから $x - x' = \partial_1^n \circ (f_{12}^n)^{-1}(y) - \partial_1^n \circ (f_{12}^n)^{-1}(y') = \partial_1^n((f_{12}^n)^{-1}(y) - (f_{12}^n)^{-1}(y'))$ となる。ここで $w := (f_{12}^n)^{-1}(y) - (f_{12}^n)^{-1}(y') \in C_1^n$ より $x - x' = \partial_1^n(w) \in \mathrm{Im}(\partial_1^n) = B_1^{n+1}$ より示された。

とくに、以上のことから ∂_2^* は $y = (f_{23}^n)^{-1}(z)$ のとり方によらないので以下ではある一つを任意に取ることとする。

(3) 写像 ∂_2^* が準同型になること

$\partial_2^*(z) = \overline{x}, \partial_2^*(z') = \overline{x'}, x = (f_{12}^{n+1})^{-1} \circ \partial_2^n(y), x' = (f_{12}^{n+1})^{-1} \circ \partial_2^n(y')$ とする。ここで f_{23}^n が準同型より $f_{23}^n(y+y') = f_{23}^n(y) + f_{23}^n(y') = z + z'$ だから $y + y' = (f_{23}^n)^{-1}(z+z')$ となる。また、$f_{12}^{n+1}, \partial_2^n$ が準同型より $f_{12}^{n+1}(x+x') = f_{12}^{n+1}(x) + f_{12}^{n+1}(x') = \partial_2^n(y) + \partial_2^n(y') = \partial_2^n(y+y')$ なので $x + x' = (f_{12}^{n+1})^{-1} \circ \partial_2^n(y+y')$ とできる。以上より $\partial_2^*(z+z') = \overline{x+x'} = x + x' + B_1^{n+1} = (x + B_1^{n+1}) + (x' + B_1^{n+1}) = \overline{x} + \overline{x'} = \partial_2^*(z) + \partial_2^*(z')$ となるから ∂_2^* は準同型になる。

(4) 準同型写像 ∂_2^* から以下のような準同型写像 ∂^* が誘導されること。

$$\begin{aligned}
\partial^* : H_3^n &\longrightarrow H_1^{n+1} \\
\overline{z} = z + B_3^n &\longmapsto \partial_2^*(z) = \overline{x} = x + B_1^{n+1}
\end{aligned}$$

以下のような可換性を用いる。

$$\begin{tikzcd}
& u = (f_{23}^{n-1})^{-1}(w) \arrow[r, "f_{23}^{n-1}"] \arrow[d, "\partial_2^{n-1}"] & w \arrow[d, "\partial_3^{n-1}"] \\
& y = \partial_2^{n-1}(u) = (f_{23}^n)^{-1} \circ \partial_3^{n-1}(w) \arrow[r, "f_{23}^n"] \arrow[d, "\partial_2^n"] & \partial_3^{n-1}(w) \\
x \arrow[r, "f_{12}^{n+1}"] & 0 = \partial^n \circ \partial^{n-1}(u) &
\end{tikzcd}$$

∂_2^* はすでに準同型写像なので $\partial^*(\overline{z}) = \partial_2^*(z + B_3^n)$ より $\partial_2^*(B_3^n) = 0$ となれば $\partial^*(\overline{z}) = \partial_2^*(z) = \overline{x}$ とできて準同型写像が誘導される。したがって $\partial_2^*(B_3^n) = 0$ を示す。

$B_3^n = \mathrm{Im}(\partial_3^{n-1})$ より B_3^n の元は任意の $w \in C_3^{n-1}$ を用いて $\partial_3^{n-1}(w)$ で書かれる。$\partial^n \circ \partial^{n-1} = 0$ より $B_3^n \, \mathrm{Im}(\partial_3^{n-1}) \subset \ker(\partial_3^n) = Z_3^n$ なので ∂_2^* の定義域に即している。この $\partial_3^{n-1}(w)$ に対して今までと同様に $y = (f_{23}^n)^{-1}(\partial_3^{n-1}(w))$ と $x = (f_{12}^{n+1})^{-1} \circ \partial_2^n(y)$ が取れる。ここで f_{23}^{n-1} が全射なので $f_{23}^{n-1}(u) = w$ となる $u \in C_2^{n-1}$ が存在する。図式が可換より $\partial_3^{n-1} \circ f_{23}^{n-1}(u) = f_{23}^n \circ \partial_2^{n-1}(u)$ であるので $\partial_3^{n-1}(w) = f_{23}^n \circ \partial_2^{n-1}(u)$

から $\partial_2^{n-1}(u) = (f_{23}^n)^{-1} \circ \partial_3^{n-1}(w) = y$ となる。これより $\partial_2^n \circ \partial_2^{n-1} = 0$ に注意すれば $\partial_2^*(\partial_3^{n-1}(w)) = (f_{12}^{n+1})^{-1} \circ \partial_2^n(y) = (f_{12}^{n+1})^{-1} \circ (\partial_2^n \circ \partial_2^{n-1})(u) = 0$ となるので $\partial_3^{n-1}(w) \in \ker(\partial_2^*)$ より $\partial_2^*(B_3^n) = 0$ から適切に ∂^* が誘導される。

以上より準同型写像 $\partial^* : H_3^n \longrightarrow H_1^{n+1}, \overline{z} \longmapsto \overline{x}$ が存在することが示された。 □

Fact 14.8. G 加群 $M_i(1 \leq i \leq 3)$ に対して以下の加群の完全列が存在するとする。

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

このとき以下のような無限の長さの完全列が存在する。

$$\begin{aligned} 0 &\longrightarrow H^0(G, M_1) \longrightarrow H^0(G, M_2) \longrightarrow H^0(G, M_3) \\ &\longrightarrow H^1(G, M_1) \longrightarrow H^1(G, M_2) \longrightarrow H^1(G, M_3) \\ &\longrightarrow H^2(G, M_1) \longrightarrow \cdots \end{aligned}$$

14.2 Galois cohomology

定義 14.9. A を群 G が作用する Abel とは限らない群とする。このとき例 (14.5) より 0 次のコホモロジー群を $H^0(G, A) := A^G$ としても矛盾しないのでそのように定義する。

また、 $\alpha \in C^1(G, A)$ を

$$\begin{aligned} \alpha : G &\longrightarrow A \\ g &\longmapsto \alpha_g \end{aligned}$$

と定めると、 A の演算を非可換性を表すため積で書くことにすると

$$\begin{aligned} \partial^1(\alpha)(g, h) &= g\alpha_h \cdot \alpha_{gh}^{-1} \cdot \alpha_g \\ \alpha \in Z^1 = \ker(\partial^1) &\Leftrightarrow {}^\forall g, h \in G, g\alpha_h \cdot \alpha_{gh}^{-1} \cdot \alpha_g = 1 \\ &\Leftrightarrow \alpha_{gh}^{-1} \cdot \alpha_g = (g\alpha_h)^{-1} \\ &\Leftrightarrow \alpha_g(g\alpha_h) = \alpha_{gh} \end{aligned}$$

となるから例 (14.6) より 1 次のコサイクルは $Z^1 = \{\alpha \in C^1 | {}^\forall g, h \in G, \alpha_{gh} = \alpha_g \cdot g\alpha_h\}$ となるのでそのように定義する。

定義 14.10. 群 G とそれが作用する非可換群 A の 1 次コサイクル Z^1 について $\alpha, \beta \in Z^1$ がcohomologous ($\alpha \sim \beta$) とは

$${}^\exists a \in A \text{ s.t. } {}^\forall g \in G\ ,\ \beta_g = a^{-1} \cdot \alpha_g \cdot ga$$

となることであり、これは同値関係になる。G が恒等的な作用をするのであれば $ga = a$ よりこれは α_g と β_g が共役な関係になってることと同じになる。つまり共役から ga の分だけねじれているともみれる。

Proof. 同値関係になることをしめす。

まず、 ${}^\forall g \in G$ と ${}^\forall a \in A$ について $(ga)^{-1} = ga^{-1}, g(1) = 1$ が成り立つことを示す。定義から G が A に加群のように作用するので $g(1) = g(1 \cdot 1) = g(1) \cdot g(1)$ から $g(1) = g(1) \cdot g(1)^{-1} = 1$ より成立。これを用いれば $1 = g(1) = g(a \cdot a^{-1}) = ga \cdot ga^{-1} \Leftrightarrow (ga)^{-1} = ga^{-1}$ より成立。

・反射律

$a = 1 \in A$ としてとれば $\alpha_g = 1 \cdot \alpha_g \cdot 1 = 1^{-1} \cdot \alpha_g \cdot g(1)$ が任意の $g \in G$ で成り立つので $\alpha \sim \alpha$ より反射律が成り立つ。

・対称律

$\alpha \sim \beta$ のときある $a \in A$ で $\beta_g = a^{-1} \cdot \alpha_g \cdot ga$ となっているので逆元をそれぞれかけて $\alpha_g = a \cdot \beta_g \cdot (ga)^{-1}$ となっていて上で述べたことより $b := a^{-1} \in A$ を取る時 $(ga)^{-1} = ga^{-1} = gb$ から $\alpha_g = b^{-1} \cdot \beta_g \cdot gb$ となるので $\beta \sim \alpha$ より対称律がなりたつ。

・推移律

$\alpha \sim \beta, \beta \sim \gamma$ となっているとするときある $a, b \in A$ で $\beta_g = a^{-1} \cdot \alpha_g \cdot ga$ と $\gamma_g = b^{-1} \cdot \beta_g \cdot gb$ となっている。β_g に代入すると $\gamma_g = b^{-1} \cdot (a^{-1} \cdot \alpha_g \cdot ga) \cdot gb = (b^{-1}a^{-1}) \cdot \alpha_g \cdot (ga \cdot gb) = (ab)^{-1} \cdot \alpha_g \cdot g(ab)$ となり $ab \in A$ なので $\alpha \sim \gamma$ から推移律が成り立つ。 □

定義 14.11. Galois cohomology とは有限次 Galois 拡大 L/K があるとき $G := \mathrm{Gal}(L/K)$ としてこれが作用する群 M についてのコホモロジー群 $H^n(G, M)$ のことである。とくに M として $L, L^n, GL_n(L)$ 等を考える。ただし $GL_n(L)$ は L 成分の n 次正則行列全体の積による群であり、一般に L に作用する群を G としたとき $\sigma \in G$ は $X = (x_{ij}) \in M_n(L) := (n$ 次正方行列全体の集合$)$ に対して $\sigma(X) := (\sigma(x_{ij}))$ と定める。

命題 14.12. 体 L と有限群 $G \subset \mathrm{Aut}(L)$ について以下が成り立つ。

(1) $^\forall n \in \mathbb{Z}_{\geq 1}$ について $H^n(G, L) = 0$ となる。

(2) $^\forall n \in \mathbb{Z}_{\geq 1}$ について $H^1(G, GL_n(L)) = 1$ となる。とくに $H^1(G, L^\times) = 1$ となる。これは一つの成分だけの正則行列が $GL_1(L) = L^\times$ となることからすぐ導かれる。

Proof. (2)

一般に定義 (14.4) から $B^1 \subset Z^1$ だから $Z^1 \subset B^1$ を示せば $B^1 = Z^1$ から $H^1 = Z^1/B^1 = 1$ が示される。まず、 0 次コバウンダリー作用素 ∂^0 に対して $B^1 = \mathrm{Im}(\partial^0) = \{\partial^0 X | X \in GL_n(L)\}$ となっていて例 (14.6) の B^1 から $\partial^0 X$ は $GL_n(L)$ での演算は積であることに注意すれば

$$\begin{aligned} \partial^0 X : G &\longrightarrow GL_n(L) \\ g &\longmapsto \partial^0 X(g) = gX \cdot X^{-1} \end{aligned}$$

となっている。したがって $^\forall \alpha \in Z^1$ に対して $^\forall g \in G, \alpha_g = \partial^0 X(g) = gX \cdot X^{-1}$ となる $X \in GL_n(L)$ が存在すればよい。いま、ある $X \in GL_n(L)$ について

$$b := \sum_{h \in G} \alpha_h \cdot h(X)$$

と定義すると $b \in GL_n(L)$ である。$h \in G \subset \mathrm{Aut}(L)$ より Dedekind の補題 (2.4) から M を L とみればその対偶を取ることで $\alpha_h \in GL_n(L)$ はより任意の $h \in G$ で $\alpha_h \neq 0$ となるからある $x_{ij} \in L$ が存在して $\sum_{h \in G} \alpha_h \cdot hx_{ij} \neq 0$ となる。 □