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。

$\Leftrightarrow$ クルル次元が 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. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}\,(p:\text{素数}), \mathbb{Q}_p\,(p\text{ 進体})$

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。つまり、以下の図が可換であるということ。

定義 1.7. 体の準同型とは環としての準同型のこと。

Note 1.8. 体の準同型は全て単射。

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

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

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

定義 1.9. $[L : K] := \dim_K(L)$ と書きこれを L/K の 拡大次数 (extension degree)という。この値により拡

大は有限次拡大、無限次拡大に分けられる。

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

$K[x]/(f)$ で $f = a_0 + a_1 x + \cdots + a_n x^n$ で既約とすると $a_n = 1$ とできて、$x^n \equiv -(a_0 + \cdots + a_{n-1}x^{n-1}), (\mod (f))$ 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。

定義 1.11. 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。

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 1.12. 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 1.13. 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 1.14. $H_1 \subset H_2 \subset \mathrm{Aut}(L) \Longrightarrow L^{H_1} \supset L^{H_2}$ 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 1.15. $L/M/K$ のとき $[L : K] = [L : M][M : K]$ が成り立つ。何れかが無限次元であれば成立する。

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

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

2　Galois 理論の基本定理

2.1　Dedekind の補題

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

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

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

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

Galois 理論の基本定理を示すために準備を行う。

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

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

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

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

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

となる。これと $\sigma_n(x_0)$ を式にかけたものは

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

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

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

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

□

補題 2.4. Dedekind の補題

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

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

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

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。 □

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

2.2 Artin の定理

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

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

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

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

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

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

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

今、有限次拡大であるので M の基底を (m_i)、その双対空間 $\mathrm{Hom}_K(M,K)$ の基底つまり双対基底を (f_i)、L の基底を (l_j) とできる。よって $z \in \mathrm{Hom}_K(M,K) \otimes_K L$ は $z = \sum_{ij} a_i j(f_i \otimes l_j), a_{ij} \in K$ と書ける。そし

て定義から $\theta(z)(m) = \sum_{ij} a_i j(f_i(m) l_j)$ となる。$m = m_i$ とすると双対基底からクロネッカーのデルタから $f_i(m_j) = \delta_{ij}$ となるので $\theta(z)(m_i) = \sum_j a_i j l_j$ である。$\theta(z) = 0$ になるとき、全ての (m_i) において 0 になるので (l_j) が基底より一次独立を考えれば $^\forall i, \sum_j a_i j l_j = 0 \Leftrightarrow a_i j = 0$ 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 $\phi : K^n \otimes_K L \longrightarrow L^n, (k_1, \ldots, k_n) \otimes l \longmapsto (k_1 l, \ldots, k_n l)$ とする。これは $(k_1 l, \ldots, k_n l) = (k_1' l', \ldots, k_n' l') \Leftrightarrow {}^\forall i, k_i l = k_i' l$ 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 phi は単射。そして、任意の $(l_1, \ldots, l_n) \in L^n$ に対して $k_i = l_i l^{-1}$ 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