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

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、**??**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。

$G = \{\sigma_1, \ldots, \sigma_m\}, L$ の K 上の基底を $(w_1, \ldots, w_n)$ とする。仮定より $m \leq n$ 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 $(c_1, \ldots, c_n) \in L^n$ 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 $c_i, (1 \leq i \leq r)$ 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 $r \leq 2$ 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 $|G| \geq [L:K]$ 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。

□