Algebra III

1 体の拡大

定義 1.1 1. 体 K が、体 L の部分環であるとき、K は L の部分体、L は K の拡大体であると言い、$L:K$ と書く。

2. $L:K$ を体の拡大とし、$Y \subset L$ (部分集合) である時、$K \cup Y$ を含む L の部分体で最小のものを、K に Y を添加して得られた体と言い $K(Y)$ で表す。$Y = \{y_1, \ldots, y_n\}$ である時は、$K(Y)$ を $K(y_1, \ldots, y_n)$ とも書く。

3. ある L の元 α によって、$L = K(\alpha)$ と書けるとき、$L:K$ を単純拡大と言う。

定義 1.2 $L:K$ を体の拡大とし、$\alpha \in L$ とする。

1. 零でない多項式 $p(x) \in K[x]$ で、$p(\alpha) = 0$ となるものがあるとき、α を K 上代数的な元と呼び、そうでないとき、すなわち、$1, \alpha, \ldots, \alpha^n, \ldots$ が K 上で一次独立の時、α を K 上超越的な元と呼ぶ。

2. $\alpha \in L$ が K 上代数的であるとき、$m(\alpha) = 0$ となる零でない多項式 $m(x) \in K[x]$ で、次数最小、monic (最高次の係数が 1) なものを、α の最小多項式と呼ぶ。

命題 1.1 $L:K$ を体の拡大とし、α を K 上代数的な L の元、$m(x) \in K[x]$ を α の最小多項式とする。このとき、次が成立する。

(1) $m(x)$ は、既約。

(2) $f(x) \in K[x]$ が、$f(\alpha) = 0$ を満たせば、$m(x)$ は、$f(x)$ を割り切る。特に、最小多項式はただ一つであり、さらに、$f(x) \in K[x]$ が、既約な *monic* な多項式で、$f(\alpha) = 0$ ならば、$f(x) = m(x)$ すなわち、$f(x)$ は、最小多項式である。

(3) $K(\alpha) \simeq K[x]/(m(x))$。

(4) $K(\alpha) = K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \mid a_i \in K\}$ であり、$1, \alpha, \ldots, \alpha^{d-1}$ は、K 上一次独立である。ただし、$\deg m(x) = d$ とする。

命題 1.2 K を体、$m(x)$ を K 上既約な *monic* な多項式とする。このとき、拡大 $K(\alpha):K$ で、α の最小多項式が $m(x)$ となるものがある。

定義 1.3 $i: R_1 \longrightarrow R_2$ を環準同型とする。このとき、R_1、R_2 を係数とする多項式環の間の写像 $\hat{i}: R_1[x] \longrightarrow R_2[x]$ を次のように定義する。

$$a_0 + a_1x + \cdots + a_sx^s \mapsto i(a_0) + i(a_1)x + \cdots + i(a_s)x^s.$$

すると、$\hat{i}$ は、環準同型写像である。さらに、i が同型写像なら、$\hat{i}$ も 同型写像である。

次の定理は、この講義のあらゆる場面で、鍵となるものである。

定理 1.3 $i: K \to L$ を体同型、$K(\alpha):K$、$L(\beta):L$ を体の拡大とし、α を K 上代数的、β を L 上代数的とする。$m(x)$ が K 上 α の最小多項式とする。もし、$\hat{i}(m(x))$ が L 上 β の最小多項式ならば、体同型 $j: K(\alpha) \longrightarrow L(\beta)$ で、$j_{|K} = i$、$j(\alpha) = \beta$ となるものが存在する。

2 拡大の次数と作図問題

定義 2.1 $L:K$ を体の拡大とする。演算を次のように定義する。

$$\begin{aligned}(\lambda, u) &\mapsto \lambda u \ (\lambda \in K,\ u \in L),\\ (u, v) &\mapsto u + v \ (u, v \in L).\end{aligned}$$

すると、L は、K 上のベクトル空間になる。このときの次元 $\dim_K L$ を体の拡大 $L:K$ の次数と呼び、$[L:K]$ と書く。

定理 2.1 $M:L$、$L:K$ を体の拡大とする。このとき、次が成立する。

$$[M:K] = [M:L][L:K].$$

命題 2.2 $K(\alpha):K$ を単純拡大とする。このとき、次が成立する。

(1) α が K 上超越的ならば、$[K(\alpha):K] = \infty$。

(2) α が K 上代数的で、$m(x)$ をその最小多項式とする。すると、$[K(\alpha):K] = \deg m$。

定義 **2.2** $L:K$ を体の拡大とする。$[L:K]<\infty$ のとき、$L:K$ を有限次拡大であるという。また、L の各元が K 上代数的であるとき、代数拡大と呼ぶ。

命題 **2.3** $L:K$ を体の拡大とする。このとき、$[L:K]<\infty$ であることと、K 上代数的な元、$\alpha_1,\ldots,\alpha_t\in L$ で $L=K(\alpha_1,\ldots,\alpha_t)$ となるものがあることとは、同値である。さらにこのとき、$L:K$ は、代数拡大である。

以下作図問題について考える。

与えられた点集合 $\boldsymbol{R}^2\supset P$ から、定規によっては、P の 2 点を通る直線を引く。コンパスによっては、P の 2 点間の距離に等しい半径の円を P の点を中心に描くものとする。$\boldsymbol{R}^2\supset P_0$ を点の集合とする。P_0 からはじめて、上の操作を続けて行って得られる点の集合 P を P_0 から作図可能という。

- $P=P_0\cup\{r_1,r_2,\ldots,r_n\},\ r_i=(x_i,y_i)\ (i=1,\ldots,n)$,
- $P_0=\{p_1,p_2,\ldots,p_s\},\ p_j=(x'_j,y'_j)\ (j=1,\ldots,s)$,
- $K_0=\boldsymbol{Q}(x'_1,\ldots,x'_s,y'_1,\ldots,y'_s),\quad K_i=K_{i-1}(x_i,y_i),\ (i=1,\ldots,n)$

とする。

命題 **2.4** $[K_{i-1}(x_i):K_{i-1}]\le 2$ かつ、$[K_{i-1}(y_i):K_{i-1}]\le 2\ (i=1,\ldots,n)$。

定理 **2.5** 点 $r=(x,y)$ が、P_0 から作図可能ならば、$[K_0(x):K_0]$、$[K_0(y):K_0]$ は、ともに 2 べきである。

3 自己同型、不変体、分解体

定義 **3.1** $L:K$ を体の拡大とする。

1. L の自己同型 (環としての全単射) σ が、K-自己同型であるとは、$\sigma(k)=k$ がすべての $k\in K$ について、成り立つことである。
2. L の K-自己同型全体を、拡大 $L:K$ のガロア群 (Galois Group) といい、$\Gamma(L:K)$ とかく。$\Gamma(L:K)$ は、写像の合成に関して、群になる。

定義 **3.2** $L:K$ を体の拡大、$G=\Gamma(L:K)$ を拡大 $L:K$ のガロア群とする。

1. $K\subset M\subset L$ なる体 M を中間体 (intermidiate field) と言う。
2. M が拡大 $L:K$ の中間体のとき、$M^*=\Gamma(L:M)$ とする。$M^*\le K^*=G$ である。
3. $H\le G$ のとき、$H^+=\{a\in L\mid \sigma(a)=a \text{ for all } \sigma\in H\}$ は、拡大 $L:K$ の中間体である。これを、H の不変体という。

これによって、体の拡大 $L:K$ の中間体全体と、$G=\Gamma(L:K)$ の部分群全体との間に $*$ と $+$ により対応が定義できる。Galois は、拡大 $L:K$ がある性質（正規性・分離性）を満たすとき、この対応は、包含関係を逆にする全単射であることを示した。

定義 **3.3** K を体、$f(t)\in K[t]$ を多項式とする。

1. $f(t)$ が K 上で分解 (split) しているとは、K の元 $k,\alpha_1,\ldots,\alpha_n$ が存在して、$f(t)=k(t-\alpha_1)\cdots(t-\alpha_n)$ と書けること、すなわち、$f(t)$ が K の中で、一次因子に分解していることを言う。
2. 体 Σ が、f に対する K の分解体であるとは、以下の条件を満たすことである。
   (a) f は、Σ で分解している。
   (b) $K\subset\Sigma'\subset\Sigma$ で f が体 Σ' で分解していれば、$\Sigma'=\Sigma$。

   すなわち、Σ は、f が分解する極小の体ということである。上の 2 番目の条件は、次の条件にも置き換えることが出来る。

   (c) $\Sigma=K(\alpha_1,\ldots,\alpha_n)$、$\alpha_1,\ldots,\alpha_n$ は、f の Σ における根。

定理 **3.1** K を体 $f(t)\in K[t]$ とする。このとき、K 上 f の分解体が存在する。

命題 **3.2** $i:K\to K'$ を 体同型、$f\in K[t]$、Σ を K 上 f の分解体とする。また、L を $\hat{i}(f)$ が L で分解するような K' の拡大体とする。このとき、単射準同型 $j:\Sigma\to L$ で $j_{|K}=i$ すなわち、K 上では、i となっているものが存在する。

定理 **3.3** $i : K \to K'$ を体同型、$f \in K[t]$ とする。T を f の K 上の分解体、T' を $\hat{i}(f)$ の K' 上の分解体とする。このとき、同型写像 $j : T \to T'$ で、$j_{|K} = i$ となるものが存在する。

4 正規性と分離性

定義 **4.1** 体の拡大 $L : K$ が正規であるとは、L において、少なくとも一つの根を持つ K 上の既約多項式 f は、全て、L において分解している時を言う。

定理 **4.1** 体の拡大 $L : K$ が有限かつ正規であるという事と、L が、K 上ある多項式の分解体であることとは、同値である。

定義 **4.2** f を体 K 上の既約多項式とする。

1. f が、f の分解体において、重根を持たないとき、f を分離的または、分離多項式と言う。(分解体は、同型であるから、この定義は、分解体の取り方によらない。)
2. f が、分離的ではないとき、f を非分離的と言う。

定義 **4.3** K を体とし、$f(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t]$ とする。このとき、

$$Df = a_1 + 2a_2 t + \cdots + n a_n t^{n-1}$$

を f の形式的微分という。

形式的微分に関しては、次が成り立つ。

$$\begin{aligned} D(f+g) &= Df + Dg, \\ D(fg) &= Df \cdot g + f \cdot Dg, \\ D(\lambda g) &= \lambda Dg. \end{aligned}$$

命題 **4.2** K を体、$0 \neq f \in K[t]$ とする。f が、分解体において、多重根を持つと言うことと、$K[t]$ において、$(f, Df) \neq 1$ と言うこととは、同値である。

命題 **4.3** (1) $\mathrm{char}K = 0$ ならば、K 上の任意の既約多項式は、K 上分離的である。

(2) $\mathrm{char}K = p > 0$ ならば、K 上の既約多項式 f が非分離的だと言うことと、$f(t) \in K[t^p]$ となっていることとは、同値。すなわち、$f(t)$ は、以下のように書ける。

$$f(t) = a_0 + a_1 t^p + \cdots + a_r t^{rp},$$

$a_i \in K,\ i = 0, 1, \ldots, r.$

定義 **4.4** $L : K$ を体の拡大とする。

1. $f \in K[t]$ のすべての既約因子が、K 上分離的であるとき、f は、K 上分離的であると言う。
2. $\alpha \in L$ が、K 上代数的であって、かつ α の最小多項式が K 上分離的であるとき α は、K 上分離的であると言う。
3. L の元がすべて、K 上分離的であるとき、$L : K$ を分離拡大という。

命題 **4.4** $L : K$ を分離的な体の拡大とし、M をその中間体とする。このとき、$L : M$、$M : K$ は、共に分離的である。

5 次数と位数

命題 **5.1** K、L を体とするとき、K から L への相異なる単射準同型 $\lambda_1, \ldots, \lambda_n$ は、L 上で一次独立である。すなわち、$a_1, \ldots, a_n \in L$ に対して、

$$a_1\lambda_1(x) + \cdots + a_n\lambda_n(x) = 0 \ \textit{for all}\ x \in K$$

$$\Rightarrow a_1 = \cdots = a_n = 0.$$

以下、連立一次斉次方程式の定理を利用する。

命題 **5.2** 次の連立一次方程式は、$n > m$ のとき、すべては、零でない解を持つ。

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

定理 **5.3** K を体とし、G を $\mathrm{Aut}K$ の有限部分群とする。K_0 を G の不変体、

$$K_0 = \{k \in K \mid \sigma(k) = k,\ \ \textit{for every}\ \sigma \in G\}$$

とすると、$[K : K_0] = |G|$。

系 **5.4** $L:K$ を体の有限次拡大とする。$H \leq G = \Gamma(L:K)$ とすると、次の等式が成り立つ。

$$[L:K] = |H| \cdot [H^+ : K].$$

定理 **5.5** $L:K$ を体の有限正規拡大とし、M をその中間体とする。$\tau : M \to L$ が、K-単射準同型ならば、L の K-自己同型 $\sigma : L \to L$ で、$\sigma_{|M} = \tau$ となっているものが存在する。特に、$p(t) \in K[t]$ を既約な多項式とし、α, β をその根とすると、L の K-自己同型で、$\sigma(\alpha) = \beta$ となっているものが存在する。

6 ガロアの定理

$L:K$ を体の有限次拡大、$G = \Gamma(L:K)$ とする。$\mathcal{F}$ で、中間体全体を表し、$\mathcal{G}$ で、G の部分群全体を表すとする。

$M \in \mathcal{F}$、$H \in \mathcal{G}$ に対して、$M^* \in \mathcal{G}$, $H^+ \in \mathcal{F}$ をそれぞれ次の様に定義する。

$$\begin{aligned} M^* &= \{\sigma \in G \mid \sigma(m) = m, \ \text{ for all } m \in M\} \\ &= \Gamma(L:M) \\ H^+ &= \{a \in L \mid \sigma(a) = a, \ \text{ for all } \sigma \in H\} \end{aligned}$$

定理 **6.1** （ガロアの基本定理）$L:K$ を有限分離正規拡大、$[L:K] = n$、$G = \Gamma(L:K)$、$M \in \mathcal{F}$ とする。このとき、次が成立する。

(1) $|G| = n$。

(2) $*$ と、$+$ は、互いに逆写像で、包含関係を逆転させ、$\mathcal{F}$ と、$\mathcal{G}$ の間の一対一対応を与える。

(3) $[L:M] = |M^*|$、$[M:K] = |G|/|M^*|$。

(4) $M:K$ が正規拡大 $\Leftrightarrow M^* \lhd G$。

(5) $M:K$ が正規拡大 $\Rightarrow \Gamma(M:K) \simeq G/M^*$。

有限正規分離拡大のことを有限次ガロア拡大ともいう。この節の目標は、上の定理を証明することである。

定義 **6.1** $L:K$ を代数拡大、N が、$L:K$ の正規閉包であるとは、N が、L の拡大体で、次の条件を満たすものである時を言う。

1. $N:K$ は、正規拡大。
2. $L \subset M \subset N$ で、$M:K$ が正規ならば、$N = M$。

すなわち、正規閉包は、L を含む K の正規拡大の中で、最小のもの。

定理 **6.2** $L:K$ が有限拡大ならば、$L:K$ の正規閉包 N で、$N:K$ が有限拡大となるものがある。$M:K$ も、正規閉包ならば、$N:K$ と同型である。

補題 **6.3** $K \subset L \subset N \subset M$ を、体の拡大で、$[L:K] < \infty$、かつ N は、$L:K$ の正規閉包とする。$\tau : L \to M$ を K-単射準同型とすると、$\tau(L) \subset N$ である。

定理 **6.4** $L:K$ を有限拡大とすると、次は同値。

(1) $L:K$ は、正規拡大。

(2) L を含む K の正規拡大 M で次を満たすものがある。

$$\Gamma(L:K) = \{\sigma : L \to M \mid \sigma \ K\text{-単射準同型}\}$$

(3) L を含む K の任意の正規拡大 M は、次を満たす。

$$\Gamma(L:K) = \{\sigma : L \to M \mid \sigma \ K\text{-単射準同型}\}$$

定理 **6.5** $K \subset L \subset M$ を体の拡大の列とし、$M:K$ は、有限正規拡大とする。$[L:K] = n$ ならば、L から、M の中への単射準同型の数は、n 以下であり、それが、丁度 n となるのは、$L:K$ が分離拡大の時、しかもその時に限る。

定理 **6.6** $L:K$ を有限拡大とする。このとき、$L:K$ が正規かつ分離拡大ということと、K が、$\Gamma(L:K)$ の不変体であることとは、同値である。

7 べき根による解の存在

定義 **7.1** 体の拡大 $L:K$ がべき根による拡大であるとは、$L = K(\alpha_1, \ldots, \alpha_m)$ であり、各 $i = 1, 2, \ldots, m$ について、$\alpha_i^{n(i)} \in K(\alpha_1, \ldots, \alpha_{i-1})$ となる自然数 $n(i)$ があることである。

補題 **7.1** $L:K$ を有限拡大とする。M を $L:K$ の正規閉包とする。すると、K を含む M の部分体 $L_1, \ldots, L_s$ で、$M = L_1 \cdots L_s$、$L_i : K \simeq L : K$ となっているものが存在する。

補題 **7.2** $L:K$ べき根による拡大。M を $L:K$ の正規閉包とする。このとき、$M:K$ もべき根による拡大である。

補題 **7.3** K を標数 0 の体、L を t^p-1 の K 上の分解体、p を素数とする。このとき、$\Gamma(L:K)$ は、アーベル群である。

補題 **7.4** K を標数 0 の体で、t^n-1 は、K で、分解しているとする。$a\in K$ とし、L を t^n-a の K 上の分解体とすると、$\Gamma(L:K)$ は、アーベル群である。

定義 **7.2** 群 G が可解 (solvable) であるとは、G の部分群の列 $G_1,\ldots,G_{n-1}$ で、以下の条件を満たすものが存在することである。

$$1=G_0\lhd G_1\lhd\cdots\lhd G_{n-1}\lhd G_n=G,$$

G_{i+1}/G_i はアーベル群, $i=0,1,\ldots,n-1$.

定理 **7.5** G を群。$H\leq G$、$N\lhd G$ とする。このとき以下が成り立つ。

(1) G が可解ならば、H も可解。

(2) G が可解であることと、N と、G/N が共に可解であることとは、同値である。

注

1. アーベル群は、可解。
2. A_5 の正規部分群は、1 と A_5 のみで、かつ、A_5 は、アーベル群ではない。よって、A_5 は、可解ではない。定理 7.5 により、A_5 と同型な部分群を含む群 A_n、S_n $n\geq 5$ は、可解群ではない。

定義 **7.3** $f\in K[t]$、Σ を K 上 f の分解体とする。$\Gamma(\Sigma:K)$ を f の K 上のガロア群という。

注　定義 7.3 の記号のもとで、X を根全体とすると、$\phi:\Gamma(\Sigma:K)\to S^X$ を自然な写像とすると、これは、単射である。

定義 **7.4** K を標数 0 の体、$f\in K[t]$、Σ を K 上 f の分解体とする。このとき、f がべき根で解けるとは、Σ の拡大体 M で、$M:K$ がべき根による拡大となるものがある時を言う。

8　ガロア群の可解性

本節の目標は、次の定理を証明することである。

定理 **8.1** K を標数 0 の体とする。$f\in K[t]$、Σ を K 上 f の分解体とする。このとき次は、同値である。

(i) f は、べき根で解ける。

(ii) f の K 上のガロア群は、可解。

定理 **8.2** K を標数 0 の体とし、$K\subset L\subset M$ とする。$M:K$ がべき根による拡大ならば、$\Gamma(L:K)$ は、可解群である。

定義 **8.1** $L:K$ を有限ガロア拡大。$G=\Gamma(L:K)$ とする。$a\in L$ に対して、

$$N_{L/K}(a)=N(a)=\prod_{\tau\in G}\tau(a)$$

を a のノルムという。$\sigma\in G$ だから、

$$\sigma(N(a))=\prod_{\tau\in G}\sigma\tau(a)=\prod_{\tau'\in G}\tau'(a)=N(a)$$

これは、$N(a)\in K$ を意味する。

定理 **8.3** $L:K$ を有限ガロア拡大、$\Gamma(L:K)=<\tau>=G$ 巡回群、$a\in L$ とする。このとき、$N(a)=1$ となることと、L のある元 $b\neq 0$ について、$a=b/\tau(b)$ となることとは同値。

定理 **8.4** $L:K$ を有限ガロア拡大、$\Gamma(L:K)=G<\tau>\simeq \boldsymbol{Z}/p\boldsymbol{Z}$、$p$ を素数とする。K の標数は、0 または、p と素とする。t^p-1 が K 上で、分解しているとする。すると、L の元 α と、K の元 a で、$L=K(\alpha)$ となるものが存在する。ここで、α は、t^p-a の根である。

定理 **8.5** K を標数 0 の体。$\Gamma(L:K)=G$ を可解、$L:K$ を正規拡大とする。このとき、L の拡大 R で、$R:K$ がべき根による拡大となるものが存在する。

Suzuki, H.
International Christian University