Galois理論の証明

三枝 洋一

1 Galois理論

K を体とする．環 A に環準同型 $K \to A$ が定まっているものを K 代数という．K ベクトル空間として有限次元である K 代数を有限 K 代数という．

有限 K 代数 L が体であるとき，L は K の有限次拡大体であるという．準同型 $K \to L$ は単射なので，これによって K を L の部分集合とみなす．$\dim_K L$ を $[L : K]$ と書き，L の K 上の拡大次数という，

定義 1.1
K 代数 A が分解 K 代数であるとは，K 代数として $A \cong K^{\dim_K A}$ となることをいう．

補題 1.2

(i) A を整域である K 代数とし，合成 $K^n \xrightarrow{\mathrm{pr}_i} K \hookrightarrow A$（$\mathrm{pr}_i$ は第 i 成分への射影を表す）を ϕ_i と書くと，$\mathrm{Hom}_K(K^n, A) = \{\phi_1, \ldots, \phi_n\}$ である（Hom_K は K 代数の準同型全体の集合を表す）．特に $\mathrm{Hom}_K(K^n, K) = \{\mathrm{pr}_1, \ldots, \mathrm{pr}_n\}$ であり，$K \hookrightarrow A$ が誘導する単射 $\mathrm{Hom}_K(K^n, K) \hookrightarrow \mathrm{Hom}_K(K^n, A)$ は同型である．

(ii) A が分解 K 代数であるとし，B をその剰余 K 代数とする．このとき，B も分解 K 代数である．

証明 (i) を示す．$\phi \in \mathrm{Hom}_K(K^n, A)$ を任意にとる．$1 \le j \le n$ に対し，$e_j = (\delta_{ij})_i \in K^n$ とおく（δ_{ij} は Kronecker のデルタ）．このとき，$\phi(e_1 + \cdots + e_n) = \phi(1) = 1$ および $\phi(e_i)\phi(e_j) = \phi(e_i e_j) = 0$ $(i \ne j)$ より，$\phi(e_m) \ne 0$ となる m がただ一つ存在し，その m に対し $\phi(e_m) = 1$ となることが分かる．このとき，$a = (a_i) = \sum_{i=1}^n a_i e_i \in K^n$ に対し $\phi(a) = \sum_{i=1}^n \phi(a_i e_i) = a_m$ となるので，$\phi = \phi_m$ である．

(ii) を示す．$A = K^n$ としてよい．I を A のイデアルとすると，I は $\prod_{i=1}^n I_i$（I_i は K のイデアル）と直積分解する．各 I_i は K のイデアルであるから，0 か K である．$\Lambda = \{1 \le i \le n \mid I_i = 0\}$ とおくと $A/I = K^\Lambda$ となるので，剰余環 A/I も分解 K 代数である． ∎

定義 1.3
K の有限次拡大体 L が Galois 拡大であるとは，$L \otimes_K L$ が分解 L 代数であること，すなわち，$L \otimes_K L \cong L^{[L:K]}$ が成り立つことをいう．ここで，$L \otimes_K L$ は $a \mapsto a \otimes 1$ によって L 代数とみなす．

$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$（$L$ の K 自己同型全体）を L/K の Galois 群という．

以下では K の有限次 Galois 拡大体 L を固定し，$G = \mathrm{Gal}(L/K)$ とおく．

命題 1.4
$\delta \colon L \otimes_K L \to \prod_{g \in G} L;\ a \otimes b \mapsto (ag(b))_g$ は同型である．特に $\#\,\mathrm{Gal}(L/K) = [L : K]$ である．

証明 L 代数の同型 $\varepsilon \colon L \otimes_K L \cong L^n$ を固定する．$\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, L) = \mathrm{Hom}_L(L \otimes_K L, L) \cong \mathrm{Hom}_L(L^n, L)$ である．補題 1.2 (i) より $\mathrm{Hom}_L(L^n, L) = \{\mathrm{pr}_1, \ldots, \mathrm{pr}_n\}$ であり，pr_i に対応する $\mathrm{Aut}_K(L)$ の元を g_i と書くと，$b \in L$ に対し $g_i(b) = \mathrm{pr}_i(\varepsilon(1 \otimes b))$ が成り立つ．よって $ag_i(b) = a(\mathrm{pr}_i(\varepsilon(1 \otimes b))) =$

$\mathrm{pr}_i(\varepsilon(a\otimes b))$ であるから，$\varepsilon\colon L\otimes_K L\cong L^n$ による $a\otimes b$ の像は $(ag_i(b))_{1\le i\le n}$ となる．すなわち，$L\otimes_K L\to L^n;\ a\otimes b\mapsto (ag_i(b))$ は同型である．$\mathrm{Gal}(L/K)=\{g_1,\dots,g_n\}$ なので，主張が示された．∎

有限集合 S に対し，写像 $S\to L$ 全体のなす有限 L 代数を $L[S]$ と書く．これは直積 $\prod_{s\in S}L$ と同一視できるので，分解 L 代数である．

命題 1.5
H を G の部分群とし，$L^H=\{a\in L\mid ha=a\ (h\in H)\}$ とおく．これは $K\subset L$ の中間体（K を含む L の部分体）であり，L 代数の同型 $L\otimes_K L^H\cong L[G/H]$ がある．特に $[L^H:K]=\#(G/H)$ が成り立つ．

証明　L^H が $K\subset L$ の中間体であることは明らかである．$L\otimes_K L$ への H の作用を $h(a\otimes b)=a\otimes h(b)$ で定める．また, $L[G]$ への H の作用を $(hf)(g)=f(gh)$ で定める．このとき, 命題1.4の同型 $\delta\colon L\otimes_K L\xrightarrow{\cong}\prod_{g\in G}L=L[G]$ は H の作用と可換である．実際，$a\otimes b\overset{\delta}{\mapsto}f$, $a\otimes h(b)\overset{\delta}{\mapsto}f_h$ とすると，$(hf)(g)=f(gh)=a\cdot(gh)(b)=a\cdot g(h(b))=f_h(g)$ となる．よって $L\otimes_K L^H\cong(L\otimes_K L)^H\cong L[G]^H\cong L[G/H]$ となり，所望の同型が得られる．さらに両辺の L 上の次元を考えると，$[L^H:K]=\dim_L(L\otimes_K L^H)=\dim_L L[G/H]=\#(G/H)$ が従う．∎

命題 1.6
F を $K\subset L$ の中間体とすると，L は F の Galois 拡大である．$\mathrm{Gal}(L/F)$ は G の部分群であり，その位数は $[L:F]$ である．

証明　L 代数の自然な準同型 $L\otimes_K L\to L\otimes_F L$ は明らかに全射である．$L\otimes_K L$ は分解 L 代数であったから，補題1.2 (ii) より $L\otimes_F L$ も分解 L 代数であり，L が F の Galois 拡大であることが従う．$\mathrm{Gal}(L/F)$ は明らかに G の部分群であり，その位数は命題1.4より $[L:F]$ に等しい．∎

定理 1.7（Galois 理論）
G の部分群と $K\subset L$ の中間体は $H\mapsto L^H$, $F\mapsto\mathrm{Gal}(L/F)$ によって一対一に対応する．この対応は包含関係を逆転させる．

証明　H を G の部分群とする．明らかに $H\subset\mathrm{Gal}(L/L^H)$ である．$\#\mathrm{Gal}(L/L^H)\overset{(1)}{=}[L:L^H]=[L:K]/[L^H:K]\overset{(2)}{=}\#G/\#(G/H)=\#H$ であるから（(1) で命題1.6を，(2) で命題1.4と命題1.5を用いた），$H=\mathrm{Gal}(L/L^H)$ が従う．

次に F を $K\subset L$ の中間体とし，$H=\mathrm{Gal}(L/F)$ とおく．L/F および H に命題1.5を適用すると，$[L^H:F]=\#(H/H)=1$ となり $F=L^H=L^{\mathrm{Gal}(L/F)}$ が従う．

以上で $F\mapsto\mathrm{Gal}(L/F)$ と $H\mapsto L^H$ が互いに逆を与えることが分かった．これらが包含関係を逆転させることは明らかである．∎

系 1.8
F を $K\subset L$ の中間体とするとき，$L\otimes_K F$ は分解 L 代数である．

証明　F に対応する G の部分群を H とすると，$F=L^H$ である．命題1.5より $L\otimes_K F=L\otimes_K L^H\cong L[G/H]$ は分解 L 代数となるのでよい．∎

命題 1.9
F を $K \subset L$ の中間体とし，H を F に対応する G の部分群とする．F が K の Galois 拡大であることは H が G の正規部分群であることと同値である．さらにこのとき $\mathrm{Gal}(F/K) \cong G/H$ となる．

証明　まず, H が G の正規部分群であると仮定する．$L \otimes_K L^H$ への H の作用を $h(a \otimes b) = (ha) \otimes b$ で定め，$L[G/H]$ への H の作用を $(hf)(gH) = h(f(gH))$ で定める（これらは L^H 代数としての作用である）．このとき, 命題1.5 の同型 $L \otimes_K L^H \cong L[G/H]$ は H の作用と可換である．実際, $a \otimes b \mapsto f$, $(ha) \otimes b \mapsto f_h$ とすると，$(hf)(gH) = h(f(gH)) = h(a \cdot gb) = (ha)(hgb) = (ha)g(g^{-1}hgb) \overset{(*)}{=} (ha)(gb) = f_h(gH)$ である（$(*)$ では $g^{-1}hg \in g^{-1}Hg = H$ および b が H 不変であることを用いた）．よって，同型の両辺の H 固定部分をとることで L^H 代数の同型 $L^H \otimes_K L^H \cong L[G/H]^H$ が得られる．$L[G/H] = \prod_{x \in G/H} L$ への H の作用は成分ごとの作用 $h(a_x)_{x \in G/H} = (ha_x)_{x \in G/H}$ に他ならないので，$L[G/H]^H = \prod_{x \in G/H} L^H$ である．以上より $L^H \otimes_K L^H \cong L[G/H]^H$ は分解 L^H 代数となり，$F = L^H$ が K の Galois 拡大であることが分かる．

F が K の Galois 拡大であるとすると，$F \otimes_K F$ は分解 F 代数であるから，補題 1.2 (i) より，$F \subset L$ から誘導される単射 $\mathrm{Hom}_F(F \otimes_K F, F) \hookrightarrow \mathrm{Hom}_F(F \otimes_K F, L)$ は同型である．$\mathrm{Hom}_F(F \otimes_K F, F) \cong \mathrm{Hom}_K(F, F)$, $\mathrm{Hom}_F(F \otimes_K F, L) \cong \mathrm{Hom}_K(F, L)$ より，$\mathrm{Hom}_K(F, F) \hookrightarrow \mathrm{Hom}_K(F, L)$ も同型である．任意の $g \in G$ に対し，F への制限 $g|_F$ は $\mathrm{Hom}_K(F, L)$ の元を定めるが，上の同型より，これの像 $g(F)$ は F に含まれなくてはならない．同様に $g^{-1}(F) \subset F$ が分かるので，$g(F) = F$ となる．よって群準同型 $G \to \mathrm{Aut}_K(F)$; $g \mapsto g|_F$ が定まる．これの核は $\mathrm{Gal}(L/F) = H$ に等しいので，H は G の正規部分群である．さらに単射 $G/H \hookrightarrow \mathrm{Aut}_K(F) = \mathrm{Gal}(F/K)$ が誘導される．$\#\,\mathrm{Gal}(F/K) = [F : K] = [L : K]/[L : F] = \#(G/H)$ よりこれは全射であり，$G/H \cong \mathrm{Gal}(F/K)$ が従う．∎

2　Galois 拡大の判定条件

定義 1.3 は通常の Galois 拡大の定義と異なる可能性があるので，よく見る定義との同値性についてまとめておく．

命題 2.1
有限 K 代数 A が分解 K 代数であることは $\#\,\mathrm{Hom}_K(A, K) = \dim_K A$ であることと同値である．

証明　A が分解 K 代数ならば，補題 1.2 (i) より $\#\,\mathrm{Hom}_K(A, K) = \dim_K A$ である．

逆に $\#\,\mathrm{Hom}_K(A, K) = \dim_K A$ を仮定する．$\mathrm{Hom}_K(A, K) = \{\phi_1, \ldots, \phi_r\}$ $(r = \#\,\mathrm{Hom}_K(A, K))$ と書き，$1 \le i \le r$ に対し $\mathfrak{m}_i = \mathrm{Ker}\,\phi_i$ とおくと，準同型定理より $A/\mathfrak{m}_i \cong K$ なので，$\mathfrak{m}_i$ は A の極大イデアルである．さらに $A = K + \mathfrak{m}_i$ が成り立つ（$a \in A$ に対し，$a = \phi_i(a) + (a - \phi_i(a))$ と分解すればよい）．このことから，$i \neq j$ のとき $\mathfrak{m}_i \neq \mathfrak{m}_j$ であることが分かる．実際，$\mathfrak{m}_i = \mathfrak{m}_j$ とすると，$\phi_i, \phi_j \colon A \to K$ は $K \subset A$ および $\mathfrak{m}_i = \mathfrak{m}_j \subset A$ の上で一致するので，$A = K + \mathfrak{m}_i = K + \mathfrak{m}_j$ 上でも一致する．よって $i \neq j$ のとき $\mathfrak{m}_i + \mathfrak{m}_j = A$ なので, 中国剰余定理より，K 代数の同型 $A/\mathfrak{m}_1 \cdots \mathfrak{m}_r \xrightarrow{\cong} A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_r \cong K^r$ を得る．これと $A \to A/\mathfrak{m}_1 \cdots \mathfrak{m}_r$ を合成することで K 代数の全射準同型 $\phi \colon A \twoheadrightarrow K^r$ が得られるが，$\dim_K A = \#\,\mathrm{Hom}_K(A, K) = r = \dim_K K^r$ なので ϕ は同型である．よって A は分解 K 代数であることが示された．∎

命題 2.2
K の有限次拡大体 L が Galois 拡大であることは，$\#\,\mathrm{Hom}_K(L, L) = [L : K]$ と同値である．

証明　$\mathrm{Hom}_K(L,L) = \mathrm{Hom}_L(L \otimes_K L, L)$ である．命題 2.1 より，$L \otimes_K L$ が分解 L 代数であることはこの集合の元の個数が $[L:K]$ であることと同値であることが分かるのでよい．∎

K 係数多項式 $f(T) \in K[T]$ に対し，K の有限次拡大体 E で $f(T) \in E[T]$ が一次式の積に分解するようなものを $f(T)$ の分解体というのであった．分解体は必ず存在することが知られている．さらに，L を K の任意の有限次拡大体とするとき，$f(T)$ の分解体を L を含むようにとることができる（$f(T) \in L[T]$ の分解体をとればよい）．

命題 2.3

L を K の有限次拡大体とする．$a \in L$ に対し，その K 上の最小多項式を $f(T)$ とし，E を $f(T)$ の分解体とする．以下は同値である．

(i) $f(T)$ は E において重根を持たない．
(ii) $E \otimes_K K(a)$ は分解 E 代数である．
(iii) $E \otimes_K K(a)$ は被約である（0 でない冪零元を持たない）．

条件 (i) は明らかに E のとり方に依存しないので，(ii), (iii) もそうである．これらの条件を満たす $a \in L$ を K 上分離的な元という．

証明　$f(T)$ の $E[T]$ における因数分解を $f(T) = \prod_i (T-a_i)^{m_i}$（$m_i \geq 1$，$a_i$ は相異なる）とする．$K(a) \cong K[T]/(f(T))$ であるから，$E \otimes_K K(a) \cong E[T]/(f(T)) \cong \prod_i E[T]/((T-a_i)^{m_i})$ となる．

まず (i) すなわち $m_i = 1$ を仮定すると，$E[T]/(T-a_i) \cong E$ より $E \otimes_K K(a)$ は分解 E 代数となり (ii) が従う．(ii) ならば (iii) は明白である．(iii) を仮定すると $m_i = 1$ となり (i) が分かる．よって示された．∎

命題 2.4

K の有限次拡大体 L に対し，以下は同値である：

(i) L のある有限次拡大体 E が存在して，$E \otimes_K L$ は分解 E 代数となる．
(ii) 任意の $a \in L$ は K 上分離的である．
(iii) L の K 上の生成系 $a_1, \ldots, a_n$ で K 上分離的なものが存在する．

上記の 3 条件を満たす有限次拡大体を分離拡大という．

証明　(i) から (ii) を示す．$a \in L$ の K 上の最小多項式を $f(T)$ とおくと，$K(a) \cong K[T]/(f(T))$ は L の部分体である．L の拡大体 E を，(i) の条件を満たし，かつ $f(T)$ の分解体であるようにとる．$E \otimes_K K(a)$ は $E \otimes_K L$ の部分 E 代数であり，$E \otimes_K L$ は分解 E 代数なので被約であるから，$E \otimes_K K(a)$ も被約となる．したがって a の分離性が分かる．

(ii) から (iii) は明らか（例えば，L の K ベクトル空間としての基底をとればよい）．

(iii) から (i) を示す．a_i の K 上の最小多項式を $f_i(T)$ とし，$f_1(T) \cdots f_n(T)$ の分解体で L を含むものを E とする．$a_1, \ldots, a_n$ は L を生成するので，自然な準同型 $K(a_1) \otimes_K \cdots \otimes_K K(a_n) \to L$ は全射である．よって $(E \otimes_K K(a_1)) \otimes_E \cdots \otimes_E (E \otimes_K K(a_n)) \to E \otimes_K L$ も全射である．$E \otimes_K K(a_i)$ は分解 E 代数なので $(E \otimes_K K(a_1)) \otimes_E \cdots \otimes_E (E \otimes_K K(a_n))$ も分解 E 代数であり，したがって補題 1.2 (ii) より $E \otimes_K L$ も分解 E 代数である．以上で示された．∎

注意 2.5

(i) 命題 2.4 (i) の条件は「K のある有限次拡大体 E が存在して……」としても実は同じことである．
(ii) 定義より，Galois 拡大は分離拡大となる．

命題 2.6

K の有限次分離拡大体 L に対し，以下は同値である：

(i) L は K の Galois 拡大である．

(ii) L の任意の有限次拡大体 E に対し，$\mathrm{Hom}_K(L,L) \to \mathrm{Hom}_K(L,E)$ は全単射である．

(iii) L の任意の有限次拡大体 E および $K \subset L$ の任意の中間体 F に対し，$\mathrm{Hom}_K(F,L) \to \mathrm{Hom}_K(F,E)$ は全単射である．

(iv) 任意の $a \in L$ に対し，その K 上の最小多項式は $L[T]$ において一次式の積に分解する．

(v) L の K 上の生成系 $a_1, \ldots, a_n$ で，各 a_i の K 上の最小多項式が $L[T]$ において一次式の積に分解するようなものが存在する．

証明 (i) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) $\Longrightarrow$ (v) $\Longrightarrow$ (ii) $\Longrightarrow$ (i) の順で示す．

(i) から (iii) を示す．L を K の Galois 拡大とすると，系 1.8 より $L \otimes_K F$ は分解 L 代数である．よって補題 1.2 (i) より $\mathrm{Hom}_L(L \otimes_K F, L) \hookrightarrow \mathrm{Hom}_L(L \otimes_K F, E)$ は同型である．$\mathrm{Hom}_L(L \otimes_K F, E) \cong \mathrm{Hom}_K(F,E)$, $\mathrm{Hom}_L(L \otimes_K F, L) \cong \mathrm{Hom}_K(F,L)$ より，$\mathrm{Hom}_K(F,L) \hookrightarrow \mathrm{Hom}_K(F,E)$ も同型である．

(iii) から (iv) を示す．$a \in L$ の K 上の最小多項式を $f(T)$ とし，E をその分解体で L を含むものとする．$f(T)$ の E における根 b を任意にとり，$b \in L$ を示せばよい．$F = K(a) \cong K[T]/(f(T))$ とおくと，$T \mapsto b$ によって K 準同型 $F \to E$ が得られる．(iii) よりこれの像は L に含まれるので，$b \in L$ が従う．

(iv) から (v) は明らかである．

(v) から (ii) を示す．$\phi \in \mathrm{Hom}_K(L,E)$ をとる．a_i の K 上の最小多項式を $f_i(T)$ とおくと，$0 = \phi(f_i(a_i)) = f_i(\phi(a_i))$ より $\phi(a_i)$ も $f_i(T)$ の根であるから，$\phi(a_i) \in L$ が分かる．よって $\phi(L) \subset L$ となるので，$\phi \in \mathrm{Hom}_K(L,L)$ である．

(ii) から (i) を示す．L は K の分離拡大であるから，$E \otimes_K L$ が分解 E 代数となるような L の有限次拡大体 E が存在する．このとき，補題 1.2 (i) より $\mathrm{Hom}_K(L,E) = \mathrm{Hom}_E(E \otimes_K L, E) = \mathrm{Hom}_E(E^{[L:K]}, E)$ は $[L:K]$ 個の元からなる．よって $[L:K] = \#\mathrm{Hom}_K(L,E) = \#\mathrm{Hom}_K(L,L)$ となるので，命題 2.2 より L は K の Galois 拡大である． ∎

例 2.7

K の有限次拡大体 L が一つの元 $a \in L$ で生成されているとする．このとき，L が K の Galois 拡大であることは，a の K 上の最小多項式 $f(T)$ が $L[T]$ において相異なる $\deg f$ 個の根を持つことと同値である（命題 2.4，注意 2.5 (ii)，命題 2.6 より直ちに分かる）．

系 2.8

L を K の有限次拡大体とし，$G = \mathrm{Aut}_K(L)$ とおく．L が K の Galois 拡大であることは $L^G = K$ と同値である．

証明 L が G の Galois 拡大ならば，定理 1.7 より $L^G = L^{\mathrm{Gal}(L/K)} = K$ である．逆に $L^G = K$ と仮定して L が K の Galois 拡大であることを示す．まず，$a \in L$ に対し $H = \{g \in G \mid g(a) = a\}$ とおき，多項式 $f(T) = \prod_{g \in G/H}(T - g(a))$ を考えると，これは $L^G = K$ の元を係数に持つ多項式であり，その根は相異なる L の元である（実際，$g(a) = g'(a)$ ならば $g'^{-1}g \in H$ すなわち $gH = g'H$ となる）．a の最小多項式は $f(T)$ を割り切るので，$a \in L$ は分離的な元であり，命題 2.6 の条件 (iv) を満たすことが分かる．よって命題 2.6 から L は K の Galois 拡大である． ∎

命題 2.9

L を体とし，その自己同型群 $\mathrm{Aut}(L)$ の有限部分群 G を考える．このとき，L は L^G の有限次 Galois 拡大である．

証明　$K = L^G$ とおくと，$G \subset \mathrm{Aut}_K(L)$ である．L の有限部分集合 S で G 安定なもの，すなわち，任意の $g \in G$, $a \in S$ に対し $g(a) \in S$ となるもの全体を Λ とおく．$S \in \Lambda$ に対し，S で K 上生成される L の部分体 $K(S)$ を考える．$a \in S$ は $f(T) = \prod_{g\in G}(T - g(a)) \in K[T]$ の根なので K 上代数的であることに注意すると，$K(S)$ は K の有限次拡大であることが分かる．また，S が G 安定であることから，G の L への作用で $K(S)$ は保たれる．したがって，群準同型 $G \to \mathrm{Aut}(K(S)/K)$; $g \mapsto g|_{K(S)}$ が定まる．これの像を G_S とおくと，$K \subset K(S)^{\mathrm{Aut}(K(S)/K)} \subset K(S)^{G_S} \subset L^G = K$ なので，$K(S)^{\mathrm{Aut}(K(S)/K)} = K$ となり，系 2.8 より，$K(S)$ は K の Galois 拡大であることが分かる．さらに $K(S)^{\mathrm{Aut}(K(S)/K)} = K(S)^{G_S}$ と定理 1.7 より，$G_S = \mathrm{Aut}(K(S)/K) = \mathrm{Gal}(K(S)/K)$ を得る．特に，$[K(S) : K] = \#\,\mathrm{Gal}(K(S)/K) = \#G_S \leq \#G$ が従い（命題 1.4 を用いた），$\{[K(S) : K] \mid S \in \Lambda\}$ は最大値 d を持つことが分かる．$[K(S_0) : K] = d$ となる $S_0 \in \Lambda$ を一つとり固定する．このとき，$K(S_0) = L$ が成り立つ．実際，$a \in L \setminus K(S_0)$ が存在したとすると，$S_1 = S_0 \cup \{g(a) \mid g \in G\} \in \Lambda$ とすれば $K(S_0) \subset K(S_1)$ かつ $a \in K(S_1)$ なので $K(S_0) \subsetneq K(S_1)$ となり矛盾する．$K(S_0)$ は K の有限次 Galois 拡大であったから，主張が示された． ∎

A　補足

本稿を読むのに必要な予備知識について簡単に補足しておく．必要に応じて参照されたい．

A.1　K 代数のテンソル積

K を体とする．環 A に環準同型 $\iota_A \colon K \to A$ が定まっているものを K 代数という．通常，環準同型 ι_A は明示せず，「K 代数 A」という．また，$a \in K$ に対し，$\iota_A(a) \in A$ のことも単に a と書くことが多い．K 代数 L が特に体であるとき，L は K の拡大体であるという．このとき準同型 $\iota_L \colon K \to L$ は単射であるから，それによって K を L の部分集合とみなすことが多い．

A, B を K 代数とするとき，環準同型 $f \colon A \to B$ で $f \circ \iota_A = \iota_B$ を満たすものを K 代数の準同型あるいは単に K 準同型という．本稿では，A から B への K 代数の準同型全体を $\mathrm{Hom}_K(A, B)$ と表す．

K 代数 A は $a \cdot x = \iota_A(a)x$ $(a \in K, x \in A)$ によって K ベクトル空間ともみなせる．K ベクトル空間として有限次元である K 代数を有限 K 代数という．

例 A.1

(i) A, B を K 代数とするとき，直積環 $A \times B$ は自然に K 代数となる．A, B が有限 K 代数ならば $A \times B$ もそうである．

(ii) 多項式環 $K[T]$ は自然に K 代数の構造を持つ．

定義 A.2

A, B を K 代数とするとき，K ベクトル空間としてのテンソル積 $A \otimes_K B$ は以下のようにして K 代数の構造を持つ：

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb', \quad \iota_{A\otimes_K B} \colon K \to A \otimes_K B;\ a \mapsto a \otimes 1 = 1 \otimes a.$$

これを K 代数のテンソル積と呼び，同様に $A \otimes_K B$ と表す．

注意 A.3

A, B を K 代数とするとき，環準同型 $A \to A \otimes_K B;\ a \mapsto a \otimes 1$ および $B \to A \otimes_K B;\ b \mapsto 1 \otimes b$ がある．特に，L を K の拡大体とするとき，K 代数 A から L 代数 $L \otimes_K A$ が得られることになる．この操作を係数拡大と呼ぶ．

例 A.4

(i) A を K 代数とするとき，$A \otimes_K K[T] \xrightarrow{\cong} A[T];\ a \otimes f(T) \mapsto af(T)$ である．

(ii) $\mathbb{C} \cong \mathbb{R}[T]/(T^2+1)$ であることに注意すると，

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[T]/(T^2+1) \cong \mathbb{C}[T]/(T^2+1) \cong \mathbb{C}[T]/(T+i) \times \mathbb{C}[T]/(T-i) \cong \mathbb{C} \times \mathbb{C}$$

である（3 つ目の同型で中国剰余定理を用いた）．

係数拡大に関する次の命題は本文中で頻繁に用いられる．

命題 A.5（係数拡大の普遍性）

L を K の拡大体とし，A を K 代数，B を L 代数とする．このとき，次が成り立つ：

$$\mathrm{Hom}_K(A, B) \cong \mathrm{Hom}_L(L \otimes_K A, B).$$

証明　$f \in \mathrm{Hom}_K(A, B)$ に対し，L 代数の準同型 $L \otimes_K A \to B$ が $a \otimes x \mapsto af(x)$ で定まる．一方，$g \in \mathrm{Hom}_L(L \otimes_K A, B)$ に対し，K 代数の準同型 $A \to B$ が $x \mapsto g(1 \otimes x)$ で定まる．これらが互いに逆を与えることが容易に確かめられるのでよい． ∎

次の命題は命題 2.4 の証明中で用いられる．

命題 A.6

L を K の拡大体とし，A, B を K 代数とするとき，L 代数の自然な同型

$$L \otimes_K (A \otimes_K B) \cong (L \otimes_K A) \otimes_L (L \otimes_K B)$$

がある．すなわち，係数拡大はテンソル積と交換する．

証明　$L \otimes_K (A \otimes_K B) \to (L \otimes_K A) \otimes_L (L \otimes_K B);\ a \otimes (x \otimes y) \mapsto (a \otimes x) \otimes (1 \otimes y)$ および $(L \otimes_K A) \otimes_L (L \otimes_K B) \to L \otimes_K (A \otimes_K B);\ (a \otimes x) \otimes (b \otimes y) \mapsto ab \otimes (x \otimes y)$ はともに L 代数の準同型であり，互いに逆を与えることが確認できる． ∎

A.2　有限次拡大体

K を体とする．L が K の拡大体かつ有限 K 代数であるとき，L は K の有限次拡大体であるという．このとき，$\dim_K L$ のことを $[L : K]$ と書き，L の K 上の拡大次数という．

命題 A.7

L を K の有限次拡大体とし，E を L の有限次拡大体とするとき，E は K の有限次拡大体であり，$[E : K] = [E : L][L : K]$ が成り立つ．

証明　L ベクトル空間として $E \cong L^{[E:L]}$ であるから，特に K ベクトル空間としても $E \cong L^{[E:L]}$ である．一方，K ベクトル空間として $L \cong K^{[L:K]}$ である．よって K ベクトル空間として $E \cong (K^{[L:K]})^{[E:L]} =$

$K^{[E:L][L:K]}$ であるから，$\dim_K E = [E:L][L:K] < \infty$ である．したがって E は K の有限次拡大体であり，その拡大次数 $[E:K]$ は $[E:L][L:K]$ に等しい． ∎

命題 A.8
L を K の有限次拡大とするとき，$\mathrm{Hom}_K(L,L)$ の元は全て同型である．すなわち，L の K 自己同型全体のなす群を $\mathrm{Aut}_K(L)$ と書くと，$\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L,L)$ が成り立つ．

証明 $\phi \in \mathrm{Hom}_K(L,L)$ とする．$\phi\colon L \to L$ は明らかに単射である．次元の等しい有限次元 K ベクトル空間の間の単射 K 線型写像は同型であるから，ϕ は同型であることが分かる． ∎

L を K の（有限次とは限らない）拡大体とする．$a \in L$ に対し，K 代数の準同型 $\phi_a\colon K[T] \to L$; $f(T) \mapsto f(a)$ を考え，その核を I_a と書く．$I_a \neq 0$ であるとき，すなわち，$f(a) = 0$ となる多項式 $f(T) \in K[T] \setminus \{0\}$ が存在するとき，a は K 上代数的であるという．

命題 A.9
L が K の有限次拡大体であるとき，任意の $a \in L$ は K 上代数的である．

証明 $I_a = 0$ ならば ϕ_a は単射であるが，$\dim_K K[T] = \infty$, $\dim_K L < \infty$ より矛盾が起こる． ∎

定義 A.10
$a \in L$ を K 上代数的な元とする．$K[T]$ は PID であるから，I_a は単生成なイデアルとなり，I_a の生成元で最高次の係数が 1 となるものがただ一つ存在する．これを a の K 上の最小多項式という．

命題 A.11
$a \in L$ を K 上代数的な元とし，$f_a(T) \in K[T]$ をその最小多項式とする．
(i) a が生成する L の部分 K 代数を $K(a)$ とすると，$K(a)$ は K の有限次拡大体である．
(ii) $f_a(T)$ は既約多項式であり，K 代数の同型 $K(a) \cong K[T]/(f_a(T))$ が存在する．

証明 定義より，$\phi_a\colon K[T] \to L$ の像は $K(a)$ に一致する．よって，準同型定理と $I_a = (f_a(T))$ より，$K[T]/(f_a(T)) \cong K(a)$ が成り立つ．$f_a(T) \neq 0$ より左辺は K 上有限次元であるから，右辺もそうである．また，$K(a)$ は体 L の部分環であるから，整域である．したがって $(f_a(T))$ は $K[T]$ の素イデアルである．これと $f_a(T) \neq 0$ より，$f_a(T)$ は既約多項式であることが分かる．さらに $K[T]$ が PID であることから，$(f_a(T))$ は $K[T]$ の極大イデアルとなり，$K(a) \cong K[T]/(f_a(T))$ は体であることが従う．以上で (i), (ii) が示された． ∎

K を体とし，$f(T) \in K[T] \setminus K$ とする．

定義 A.12
K の有限次拡大体 E が $f(T)$ の分解体であるとは，$f(T) \in E[T]$ が一次式の積に分解することをいう．

例 A.13
$\mathbb{Q}(\sqrt{2})$ は $T^2 - 2 \in \mathbb{Q}[T]$ の分解体である．一方，$\mathbb{Q}(\sqrt[3]{2})$ は $T^3 - 2 \in \mathbb{Q}[T]$ の分解体ではない．

$\omega = (-1+\sqrt{-3})/2$ とおくと，$\mathbb{Q}(\sqrt[3]{2}, \omega)$ は $T^3 - 2$ の分解体である．

命題 A.14
$f(T)$ の分解体は存在する．

証明　組 $(K, f(T))$ に対する主張を $f(T)$ の次数 $\deg f$ に関する帰納法で示す．$\deg f = 1$ のときは K 自身が $f(T)$ の分解体となる．$\deg f \geq 2$ の場合を考える．$f(T)$ を割り切る既約多項式 $f_0(T)$ を一つとり，$L = K[T]/(f_0(T))$ とおく．これは K の有限次拡大体である．$T \in K[T]$ の L における像を a とおくと，$f_0(a) = 0$ なので $f(a) = 0$ も成り立つ．よって $L[T]$ において $f(T) = (T-a)g(T)$ $(g(T) \in L[T])$ と分解する．帰納法の仮定を $(L, g(T))$ に対し用いることで，$g(T)$ の分解体が存在することが分かるが，それは $f(T)$ の分解体にもなっているのでよい．∎

注意 A.15
E を $f(T)$ の分解体とし，E における $f(T)$ の根を $a_1, \ldots, a_n$ とする．このとき，K 上 $a_1, \ldots, a_n$ で生成される E の部分体 $K(a_1, \ldots, a_n)$ もまた $f(T)$ の分解体であり，さらに，$F \subsetneq K(a_1, \ldots, a_n)$ となる K の拡大体 F は $f(T)$ の分解体ではない．このような分解体を最小分解体という．分解体はたくさんあるが，最小分解体は同型を除いて一意的であることが証明できる．

A.3　群作用

G を群とする．K 代数 A への G の作用とは，写像 $G \times A \to A;\ (g, a) \mapsto ga$ で以下の条件を満たすもののことである：

- 各 $g \in G$ に対し，$A \to A;\ a \mapsto ga$ は K 代数の同型となる．
- 任意の $g, g' \in G$ に対し，$g(g'x) = (gg')x$.

命題 A.16
L を K の有限次拡大体とする．A に G の作用が定まっているとき，$L \otimes_K A$ への G の作用を $g(a \otimes x) = a \otimes gx$ で定めると，$(L \otimes_K A)^G \cong L \otimes_K A^G$ が成り立つ．

証明　自然な L 代数の準同型 $L \otimes_K A^G \to L \otimes_K A$ の像は明らかに $(L \otimes_K A)^G$ に含まれるので，L 代数の準同型 $L \otimes_K A^G \to (L \otimes_K A)^G$ が得られる．これが同型であることを示そう．K ベクトル空間の同型 $L \cong K^n$ $(n = \dim_K L)$ を固定すると，K ベクトル空間の同型

$$L \otimes_K A^G \cong K^n \otimes_K A^G \cong (A^G)^n, \quad (L \otimes_K A)^G \cong (K^n \otimes_K A)^G \cong (A^n)^G$$

が得られる（A^n への G の作用は成分ごとの作用とする）．さらに，$L \otimes_K A^G \to (L \otimes_K A)^G$ はこれらの同型によって自然な写像 $(A^G)^n \to (A^n)^G$ と同一視できる．後者は明らかに全単射であるのでよい．∎

謝辞　本稿の執筆の際には，越川皓永さんから多数の有益なコメントをいただきました．この場を借りてお礼を申し上げます．