§6. 代数的閉体と共役元

定義 6.1 体 L の代数拡大体が L のみであるとき，L を**代数的閉体**という．

つまり，L が代数的閉体であるとは，L のどんな拡大体 M をとっても,『$\alpha \in M$ が L 上代数的ならば $\alpha \in L$』 となることである．

例 6.2 (1) $\boldsymbol{C}$ は代数的閉体である（代数学の基本定理）．
(2) $\boldsymbol{R}$ は代数的閉体ではない．

定理 6.3 体 L に対して次は同値である．

(i) L は代数的閉体である．
(ii) L 上の既約多項式はすべて 1 次式である．
(iii) L 上の定数でない任意の多項式は L 上の 1 次式の積として表される．
(iv) L 上の定数でない任意の多項式は L で根をもつ．

証明 (i)⇒(ii): $f(X)$ を L 上の既約多項式とする． クロネッカーの定理（定理 5.6）より，L の拡大体 M と $\alpha \in M$ で $f(\alpha) = 0$ をみたすものがとれるが，仮定 (i) より $\alpha \in L$ であるから，$\deg f = [L(\alpha) : L] = 1$ を得る．
(ii)⇒(iii): L 上の定数でない任意の多項式は，L 上の既約多項式の積として表されるから，仮定 (ii) より (iii) が導かれる．
(iii)⇒(iv): あきらか．
(iv)⇒(i): M/L を代数拡大とするとき，任意の $\alpha \in M$ に対して，$\alpha \in L$ であることを確かめればよい． いま，α の L 上の最小多項式を $f(X)$ とすると，仮定 (iv) より，$f(X)$ は根 $\beta \in L$ をもつ． 一方，定理 5.10 より $L(\alpha)$ と $L(\beta)$ は L 上同型であり，とくに L 上の次数は等しいから $[L(\alpha) : L] = [L(\beta) : L] = 1$，ゆえに $L(\alpha) = L$，すなわち $\alpha \in L$ でなければならない． □

定義 6.4 体 K の代数拡大体であって代数的閉体であるものを K の**代数的閉包**という．

定理 6.5 Ω が代数的閉体ならば，Ω に含まれる任意の部分体に対して，その代数的閉包が Ω の中に一意的に存在する．

証明 （存在すること） K を Ω の任意の部分体とする． K 上代数的な Ω の元全体

$$L = \{\, \alpha \in \Omega \,|\, \alpha \text{ は } K \text{ 上代数的} \,\}$$

は，定理 4.7 または系 4.8 を用いれば，K 上の代数拡大体であることがわかる． そこで，以下，L が代数的閉体であることを示す． $f(X)$ を L 上の定数でない任意の多項式とする． $f(X)$ は Ω 上の多項式でもあるが，Ω が代数的閉体であるという仮定から，定理 6.3 (iv) を用いれば，$f(\alpha) = 0$ である $\alpha \in \Omega$ がとれる． また，$f(\alpha) = 0$ より α は L 上代数的であるが，L/K が代数拡大であることに注意すれば，定理 4.4 より α は K 上代数的，よって，L の定義から $\alpha \in L$ である． そこで，再び定理 6.3 (iv) を用いて，L が代数的閉体であることが導かれる．
（一意性） Ω の部分体 L_1, L_2 がどちらも K 上の代数的閉包であるとする． 任意の $\alpha \in L_1$ に対して，α は K 上代数的だから，もちろん L_2 上も代数的だが，L_2 は代数的閉体なので $\alpha \in L_2$． したがって $L_1 \subset L_2$． 役割を入れ替えれば $L_2 \subset L_1$ も導かれ，$L_1 = L_2$ が得られた． □

例 6.6 (1) $\boldsymbol{C}$ は $\boldsymbol{R}$ の代数的閉包である．
(2) $\boldsymbol{Q}$ の代数的閉包は $\boldsymbol{C}$ の中で一意的に定まるが，それは $\boldsymbol{C}$ ではない．
(3) L が K の代数的閉包ならば，L/K の任意の中間体 M は K 上の代数拡大体であり，さらに L は M の代数的閉包でもある．

定理 6.7（シュタイニッツ） 任意の体 K に対してその代数的閉包が存在する． さらに，L_1, L_2 がどちらも体 K の代数的閉包ならば，K 上の同型写像 $L_1 \to L_2$ が存在する．

証明 **(方針のみ)** K 上の代数拡大体全体 $\mathcal{A}$ は，包含関係を順序とする順序集合 $(\mathcal{A}, \subset)$ となっている． このとき，$(\mathcal{A}, \subset)$ は帰納的である． 実際，$\mathcal{S}$ を $\mathcal{A}$ の全順序部分集合とすると，$M_0 = \bigcup_{M \in \mathcal{S}} M$ はあきらかに $\mathcal{A}$ に属し $\mathcal{S}$ の上限となっている． したがって，**ツォルンの補題**により $\mathcal{A}$ は極大元 L をもつ． L/K は代数拡大だから，もし E/L が代数拡大ならば，定理 4.4 より，E/K も代数拡大，よって $E \in \mathcal{A}$ となるから L の極大性より $E = L$ でなければならい． このことは L が代数的閉体であること示している． したがって，L は K 上の代数的閉包である． 後半（同型写像の存在）もツォルンの補題を用いて証明できるが，ここでは省略する． （じつは，$\mathcal{A}$ が**集合**として定義されるかどうか疑わしいという意味で，この証明は不完全である． 単に “K 上の代数拡大体全体” というだけではなく，何らかの集合論的な制約を加えて $\mathcal{A}$ を定義しなおす必要がある．） □

以下において，体 K に対して，代数的閉包をひとつ固定し $\overline{K}$ で表す．
K 上の任意の代数拡大体は $\overline{K}/K$ の中間体と K 上同型になる．なぜなら，M/K を任意の代数拡大とすると，M の代数的閉包 L は K の代数的閉包でもあるから，

前定理より，K 上の同型写像 $L \to \overline{K}$ が存在し，それによる M の像は $\overline{K}/K$ の中間体となるからである．

そこで，とくに断らない限り以下では K 上の代数拡大体は $\overline{K}/K$ の中間体であり，また K 上代数的な元も $\overline{K}$ に属しているものとする．

定義 6.8 体の拡大 L/K に対して，L から L への K 上の同型写像を，L の K 上の**自己同型写像**，または L/K の自己同型写像という．それら全体の集合は，写像の合成に関して群になっている．それを $\mathrm{Aut}(L/K)$ で表し，L の K 上の**自己同型群**，または L/K の自己同型群という;

$$\mathrm{Aut}(L/K) = \{\,\sigma \mid \ \sigma : L \to L, \quad K \text{ 上の同型写像}\,\}.$$

$\sigma, \tau \in \mathrm{Aut}(L/K)$ の合成 $\sigma \circ \tau$ を，積のように $\sigma\tau$ で表す．

定理 6.9 L が $\overline{K}/K$ の中間体で，

$$\tau : L \longrightarrow \overline{K}$$

が K 上の準同型写像であるとする．このとき，τ の延長 $\sigma \in \mathrm{Aut}(\overline{K}/K)$ が存在する．すなわち，K 上の同型写像

$$\sigma : \overline{K} \longrightarrow \overline{K}$$

で，任意の $a \in L$ に対して $\sigma(a) = \tau(a)$ であるものがとれる．

この証明も，ふつう**ツォルンの補題**を使って行われる．少し面倒なので省略する．

定義 6.10 K を体とする．$\alpha, \beta \in \overline{K}$ それぞれの K 上の最小多項式が一致するとき，α, β は K 上**共役**であるという．また，β を α の K 上の**共役元**ともいう．α の K 上の共役元全体の集合を $\mathrm{Conj}(\alpha, K)$ で表す．言い換えると，α の K 上の最小多項式の（$\overline{K}$ における）根全体の集合が $\mathrm{Conj}(\alpha, K)$ である．

定理 6.11 体 K と $\alpha, \beta \in \overline{K}$ に対して次は同値である．

(i) α, β は K 上共役である．

(ii) $\sigma(\alpha) = \beta$ をみたす $\sigma \in \mathrm{Aut}(\overline{K}/K)$ が存在する．

証明 (i)⇒(ii): (i) を仮定すると，定理 5.10 より，K 上の同型写像

$$\tau : K(\alpha) \longrightarrow K(\beta) \subset \overline{K}$$

で $\tau(\alpha) = \beta$ であるものが存在する．そこで，定理 6.9 を適用すれば (ii) が得られる．
(ii)⇒(i): $f(X)$ を α の K 上の最小多項式とすれば，(ii) のような $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して，

$$f(\beta) = f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0.$$

これは，$f(X)$ が β の K 上の最小多項式でもあることを示しているから，(i) を得る．□

系 6.12　体 K と $\alpha \in \overline{K}$ に対して,

$$\mathrm{Conj}(\alpha, K) = \left\{ \sigma(\alpha) \,\middle|\, \sigma \in \mathrm{Aut}(\overline{K}/K) \right\}$$

が成り立つ.

例 6.13　$z \in \boldsymbol{C}$ の複素共役 $\bar{z}$ は, z の $\boldsymbol{R}$ 上の共役元であり, $\mathrm{Conj}(z, \boldsymbol{R}) = \{z, \bar{z}\}$, さらに $\mathrm{Aut}(\boldsymbol{C}/\boldsymbol{R})$ は複素共役写像を生成元とする位数 2 の巡回群である.

定理 6.14　体 K と $\alpha \in \overline{K}$ に対して,

$$|\mathrm{Aut}(K(\alpha)/K)| \leq |\mathrm{Conj}(\alpha, K)| \leq [K(\alpha) : K]$$

が成り立つ.

証明　$\sigma \in \mathrm{Aut}(K(\alpha)/K)$ に対して $\sigma(\alpha) \in \mathrm{Conj}(\alpha, K)$ を対応させることにより, 単射

$$\mathrm{Aut}(K(\alpha)/K) \longrightarrow \mathrm{Conj}(\alpha, K)$$

が定まり, 前半の不等式が導かれる. 次に, $f(X)$ を α の K 上の最小多項式とすると,

$$|\mathrm{Conj}(\alpha, K)| = \text{“}f(X) \text{ の根の個数”} \leq \deg f = [K(\alpha) : K]$$

を得る. □

注意　“$f(X)$ の根の個数” $\leq \deg f$ としたのは, $f(X)$ が重根をもつ可能性があるからである. 重根をもたない場合, 根の個数は次数と一致する.

例 6.15　$\sqrt{2}$ の $\boldsymbol{Q}$ 上の最小多項式は $X^2 - 2$, したがって

$$\mathrm{Conj}(\sqrt{2}, \boldsymbol{Q}) = \{\sqrt{2}, -\sqrt{2}\}.$$

また, $\sigma \in \mathrm{Aut}(\boldsymbol{Q}(\sqrt{2})/\boldsymbol{Q})$ とすると, $\sigma(\sqrt{2}) = \pm\sqrt{2}$. 符号のとり方により, $\sigma = \mathrm{id}$（恒等写像）または $\sigma(\sqrt{2}) = -\sqrt{2}$ となるから, 後者をあらためて σ と定めれば,

$$\mathrm{Aut}(\boldsymbol{Q}(\sqrt{2})/\boldsymbol{Q}) = \{\mathrm{id}, \sigma\}$$

となる. よって, 定理 6.14 の不等式はすべて等号になっている.

例 6.16　$X^3 - 2$ の実根 $\alpha = \sqrt[3]{2}$ と他の根 $\alpha\omega$, $\alpha\omega^2$ について,

$$\mathrm{Conj}(\alpha, \boldsymbol{Q}) = \left\{ \alpha, \alpha\omega, \alpha\omega^2 \right\}.$$

一方, 同型写像 $\boldsymbol{Q}(\alpha) \to \boldsymbol{Q}(\alpha)$ によって α は α にしか写らないから

$$\mathrm{Aut}(\boldsymbol{Q}(\alpha)/\boldsymbol{Q}) = \{\mathrm{id}\}.$$

よって, この場合は定理 6.14 の左の不等号は $1 < 3$ となっていて, 等号ではない.