

代 数 II

2026 年度版

中野 伸

(学習院大学・理学部・数学科)

目 次

§1.	2 次, 3 次, 4 次方程式の解の公式	1
§2.	体の拡大, 拡大次数	5
§3.	代数的元	9
§4.	代数拡大	13
§5.	根の添加	17
§6.	代数的閉体と共役元	21
§7.	標数	25
§8.	分離拡大	29
§9.	正規拡大	33
§10.	ガロア拡大	37
§11.	ガロア対応	41
§12.	ガロア対応の例	45
§13.	クンマー拡大	49
§14.	可解性	53
§15.	補遺	57

§1. 2次, 3次, 4次方程式の解の公式

定理 1.1 2次方程式

$$X^2 + bX + c = 0$$

の解は, $b^2 - 4c$ の平方根をひとつ固定し, それを R とするとき,

$$\frac{-b+R}{2}, \quad \frac{-b-R}{2}$$

で与えられる.

証明 解を α, β とすれば, 解と係数の関係から, $\alpha + \beta = -b$, $\alpha\beta = c$. よって,

$$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = b^2 - 4c$$

そこで, この平方根のひとつを R とし, α, β に関する連立一次方程式

$$\begin{cases} \alpha + \beta = -b \\ \alpha - \beta = R \end{cases}$$

を解けば,

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} -b \\ R \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -b \\ R \end{pmatrix} = \frac{1}{2} \begin{pmatrix} -b+R \\ -b-R \end{pmatrix}$$

を得る. □

定理 1.2 3次方程式

$$X^3 + bX^2 + cX + d = 0$$

の解は, Y に関する2次方程式

$$Y^2 + (2b^3 - 9bc + 27d)Y + (b^2 - 3c)^3 = 0$$

の2解それぞれの3乗根 R, S を, $RS = b^2 - 3c$ を満たすように一組固定するとき,

$$\frac{-b+R+S}{3}, \quad \frac{-b+\omega^2 R + \omega S}{3}, \quad \frac{-b+\omega R + \omega^2 S}{3}$$

で与えられる. ここで, ω は1の原始3乗根

$$\omega = e^{\frac{2\pi i}{3}} = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = \frac{-1 + \sqrt{-3}}{2}$$

である.

証明 3つの解を α, β, γ とし,

$$\begin{aligned} Q &= \alpha + \beta + \gamma, \\ R &= \alpha + \omega\beta + \omega^2\gamma, \\ S &= \alpha + \omega^2\beta + \omega\gamma \end{aligned}$$

とおく. これらを α, β, γ の連立方程式と考え, 係数行列を M とする. ここで

$$|M| = \begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix} = 3\omega^2 - 3\omega = 3\omega(\omega - 1) \neq 0$$

より, M は正則である. よって, Q, R, S が求まれば, M の逆行列を実際に計算することにより

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = M^{-1} \begin{pmatrix} Q \\ R \\ S \end{pmatrix}$$

から α, β, γ が得られる. さて, 解と係数の関係から $Q = -b$ だが,

$$R^3 + S^3 = -2b^3 + 9bc - 27d, \quad RS = b^2 - 3c$$

も, ちょっとがんばればわかる. したがって, R^3, S^3 は定理にある Y に関する2次方程式の解である. R, S は, これらの3乗根として求まり, 定理の主張が導かれる. $\square$

定理 1.3 4次方程式

$$X^4 + bX^3 + cX^2 + dX + e = 0$$

の解は, Y に関する3次方程式

$$Y^3 - (3b^2 - 8c)Y^2 + (3b^4 - 16b^2c + 16c^2 + 16bd - 64e)Y - (b^3 - 4bc + 8d)^2 = 0$$

の3解それぞれの平方根 R, S, T を, $RST = -b^3 + 4bc - 8d$ を満たすように一組固定するとき,

$$\frac{-b + R + S + T}{4}, \quad \frac{-b + R - S - T}{4}, \quad \frac{-b - R + S - T}{4}, \quad \frac{-b - R - S + T}{4}$$

で与えられる.

証明 $\alpha, \beta, \gamma, \delta$ を4つの解として

$$\begin{aligned} Q &= \alpha + \beta + \gamma + \delta, \\ R &= \alpha + \beta - \gamma - \delta, \\ S &= \alpha - \beta + \gamma - \delta, \\ T &= \alpha - \beta - \gamma + \delta \end{aligned}$$

とおく. Q, R, S, T が求まれば, 上の式を $\alpha, \beta, \gamma, \delta$ に関する連立方程式とみなして解けばよい. 解と係数の関係から $Q = -b$ だが,

$$\begin{aligned} R^2 + S^2 + T^2 &= 3b^2 - 8c, \\ R^2S^2 + S^2T^2 + T^2R^2 &= 3b^4 - 16b^2c + 16c^2 + 16bd - 64e, \\ RST &= -b^3 + 4bc - 8d \end{aligned}$$

も, うんとかんばって計算すれば得られる. したがって, R^2, S^2, T^2 は定理にある Y に関する 3 次方程式の解である. R, S, T は, これらの平方根として求まり, 定理の主張が導かれる. $\square$

定義 1.4 n 個の不定元 (変数) $x_1, x_2, \dots, x_n$ の多項式 $f(x_1, \dots, x_n)$ は, 任意の $\sigma \in S_n$ に対して

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n)$$

が成り立つとき, **対称式**であるという (正確には $x_1, \dots, x_n$ の対称式という).

定義 1.5 n 個の不定元 (変数) $x_1, x_2, \dots, x_n$ に対して,

$$(X - x_1)(X - x_2) \dots (X - x_n)$$

を展開した式

$$X^n - s_1X^{n-1} + s_2X^{n-2} + \dots + (-1)^{n-1}s_{n-1}X + (-1)^ns_n$$

によって定まる $s_1, \dots, s_n$ を, $x_1, \dots, x_n$ の**基本対称式**という. とくに, s_j を j 次の基本対称式という.

例 1.6 基本対称式は対称式である.

$$\begin{aligned} n = 2 \text{ のとき} & \quad \begin{cases} s_1 = x_1 + x_2 \\ s_2 = x_1x_2 \end{cases} \\ n = 3 \text{ のとき} & \quad \begin{cases} s_1 = x_1 + x_2 + x_3 \\ s_2 = x_1x_2 + x_1x_3 + x_2x_3 \\ s_3 = x_1x_2x_3 \end{cases} \\ n = 4 \text{ のとき} & \quad \begin{cases} s_1 = x_1 + x_2 + x_3 + x_4 \\ s_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ s_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ s_4 = x_1x_2x_3x_4 \end{cases} \end{aligned}$$

例 1.7 x_1, x_2, x_3 の対称式

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_1x_3 - x_2x_3$$

は, 上に定めた $n = 3$ のときの基本対称式 s_1, s_2, s_3 によって

$$f(x_1, x_2, x_3) = s_1^2 - 3s_2$$

と表すことができる.

定理 1.8 (対称式の基本定理) $x_1, \dots, x_n$ の任意の対称式 $f(x_1, \dots, x_n)$ に対して, ある n 変数多項式 $G(X_1, \dots, X_n)$ が存在して,

$$f(x_1, \dots, x_n) = G(s_1, \dots, s_n)$$

が成り立つ. すなわち, 任意の対称式は基本対称式の多項式として表すことができる.

例 1.9 証明は, 難しいことは使わないが煩雑なので省略する. 以下に例を挙げて証明の代わりとする.

(1) $f(x, y) = x^4 + y^4$ を x, y の基本対称式

$$s = x + y, \quad t = xy$$

の多項式として表す.

$$\begin{aligned} f(x, y) &= x^4 + y^4 \\ f(x, y) - s^4 &= -4x^3y - 6x^2y^2 - 4xy^3 \\ f(x, y) - s^4 + 4s^2t &= 2x^2y^2 \\ f(x, y) - s^4 + 4s^2t - 2t^2 &= 0 \end{aligned}$$

よって, $f(x, y) = s^4 - 4s^2t + 2t^2$.

(2) $g(x, y, z) = x^3(y + z) + y^3(z + x) + z^3(x + y)$ を x, y, z の基本対称式

$$s = x + y + z, \quad t = xy + yz + zx, \quad u = xyz$$

の多項式で表す.

$$\begin{aligned} g(x, y, z) &= x^3y + x^3z + xy^3 + xz^3 + y^3z + z^3y \\ g(x, y, z) - s^2t &= -2x^2y^2 - 5x^2yz - 2x^2z^2 - 5xy^2z - 5xyz^2 - 2y^2z^2 \\ g(x, y, z) - s^2t + 2t^2 &= -x^2yz - xy^2z - xyz^2 \\ g(x, y, z) - s^2t + 2t^2 + su &= 0 \\ \text{ゆえに, } g(x, y, z) &= s^2t - 2t^2 - su. \end{aligned}$$

§2. 体の拡大, 拡大次数

定義 2.1 体 K が体 L の部分体, つまり

$$K \subset L$$

のとき, L を K の**拡大体**という. このとき, 体の**拡大** L/K ということが多い. また, M が K の拡大体で, かつ L が M の拡大体, つまり

$$K \subset M \subset L$$

であるとき, M を拡大 L/K の**中間体**という.

定義 2.2 L/K を体の拡大とする.

- (1) L の部分集合 A に対して, A を含む最小の L/K の中間体を $K(A)$ と表し, K に A を**添加した体**という.
- (2) とくに A が有限集合で $A = \{\alpha_1, \dots, \alpha_n\}$ のとき, $K(A)$ を $K(\alpha_1, \dots, \alpha_n)$ と略記する.
- (3) ただひとつの $\alpha \in L$ により $K(\alpha)$ と表される体を K の**単純拡大体**という. この場合, α を拡大 $K(\alpha)/K$ の**原始元**という.

命題 2.3 L/K を体の拡大とする. $\alpha \in L$ に対して, $K(\alpha)$ は K 上 α で生成される可換環 (すなわち, K と α を含む L の最小の部分環)

$$K[\alpha] = \{ g(\alpha) \mid g(X) \in K[X] \}$$

の商体である. したがって

$$K(\alpha) = \left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(X), h(X) \in K[X], h(\alpha) \neq 0 \right\}$$

が成り立つ.

証明 $K(\alpha)$ は K と α を含む体だから, $g(X), h(X) \in K[X]$ とすると $g(\alpha), h(\alpha) \in K(\alpha)$, さらに $h(\alpha) \neq 0$ であれば $g(\alpha)/h(\alpha) \in K(\alpha)$. 一方,

$$\left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(X), h(X) \in K[X], h(\alpha) \neq 0 \right\}$$

は L の部分体なので, $K(\alpha)$ の最小性から命題の主張は正しいことがわかる. $\square$

例 2.4 有理数体 $\mathbf{Q}$ の拡大体について、いくつかの例をあげる.

$$(1) \mathbf{Q}(\sqrt{2}) = \mathbf{Q}(\sqrt{2} - 1) = \mathbf{Q}\left(\frac{1}{\sqrt{2}}\right) = \mathbf{Q}\left(\frac{1 + 3\sqrt{2}}{5 - 7\sqrt{2}}\right)$$

最初の等号は,

$$\sqrt{2} - 1 \in \mathbf{Q}(\sqrt{2}) \text{ だから } \mathbf{Q}(\sqrt{2} - 1) \subset \mathbf{Q}(\sqrt{2}),$$

$$\sqrt{2} = (\sqrt{2} - 1) + 1 \in \mathbf{Q}(\sqrt{2} - 1) \text{ だから } \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2} - 1)$$

よりわかる. 真ん中の等号はどうよ? 最後の等号は,

$$\alpha = \frac{1 + 3\sqrt{2}}{5 - 7\sqrt{2}} \text{ とおけば } \sqrt{2} = \frac{5\alpha - 1}{7\alpha + 3} \in \mathbf{Q}(\alpha)$$

となることを使えばわかるはず.

$$(2) \mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3}) = \mathbf{Q}(\sqrt{2} - \sqrt{3})$$

$\sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$ より $\mathbf{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$ は OK. 一方, $\beta = \sqrt{2} + \sqrt{3}$ とおけば, $\frac{1}{\beta} = \sqrt{3} - \sqrt{2}$ が成り立ち,

$$\mathbf{Q}(\sqrt{2} + \sqrt{3}) = \mathbf{Q}(\beta) = \mathbf{Q}\left(\frac{1}{\beta}\right) = \mathbf{Q}(\sqrt{2} - \sqrt{3}).$$

さらに,

$$\sqrt{2} = \frac{\beta - \frac{1}{\beta}}{2} \in \mathbf{Q}(\beta), \quad \sqrt{3} = \frac{\beta + \frac{1}{\beta}}{2} \in \mathbf{Q}(\beta)$$

よって, $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbf{Q}(\beta) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

$$(3) \mathbf{Q}(\sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{4})$$

$\gamma = \sqrt[3]{2}$, $\delta = \sqrt[3]{4}$ とおけば, $\delta = \gamma^2$ より $\mathbf{Q}(\delta) \subset \mathbf{Q}(\gamma)$. 逆に, $\gamma = \frac{\delta^2}{2}$ より $\mathbf{Q}(\gamma) \subset \mathbf{Q}(\delta)$.

$$(4) \mathbf{Q}(\mathbf{Z}) = \mathbf{Q}, \quad \mathbf{Q}(\mathbf{R}) = \mathbf{R}, \quad \mathbf{Q}(\mathbf{R}, \sqrt{-1}) = \mathbf{C}, \quad \mathbf{Q}(\sqrt{-1}) \subsetneq \mathbf{C}$$

定義 2.5 L/K を体の拡大とすると, L は K 上のベクトル空間ともみなすことができる (L における和をベクトルの和, K の元に L の元をかける操作をスカラー倍とする). このとき, K 上のベクトル空間としての L の次元を拡大 L/K の次数といい

$$[L : K]$$

で表す. $[L : K]$ が有限のとき, L/K は有限次拡大であるといい, そうでないと無限次拡大であるという.

例 2.6 (1) $\mathbb{Q}(\sqrt{7})$ は $\mathbb{Q}$ 上 2 次拡大である, $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$.

だって, $1, \sqrt{7}$ は, $\mathbb{Q}$ 上 1 次独立だし, $\mathbb{Q}$ 上 $\mathbb{Q}(\sqrt{7})$ を生成してるから, $\mathbb{Q}$ 上 $\mathbb{Q}(\sqrt{7})$ の基底だもん.

(2) $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ は 3 次拡大である, $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$.

なぜかという, $1, \sqrt[3]{5}, \sqrt[3]{25}$ は $\mathbb{Q}(\sqrt[3]{5})$ の $\mathbb{Q}$ 上の基底だから.

補題 2.7 M を体の拡大 L/K の中間体とし, $\alpha_1, \dots, \alpha_m \in M$, $\beta_1, \dots, \beta_n \in L$ とする.

$\alpha_1, \dots, \alpha_m$ が K 上 1 次独立であり, かつ $\beta_1, \dots, \beta_n$ が M 上 1 次独立

ならば, mn 個の L の元 $\alpha_i \beta_j$ ($i = 1, \dots, m, j = 1, \dots, n$) は K 上 1 次独立である.

証明 mn 個の元 $\alpha_i \beta_j$ に K 上の線形関係

$$\sum_{i=1}^m \sum_{j=1}^n c_{ij} \alpha_i \beta_j = 0 \quad (c_{ij} \in K)$$

があったとする. このとき, すべての i, j に対して $c_{ij} = 0$ が成り立つことを確かめればよい. いま, 上式を書き換えて

$$\sum_{j=1}^n \left(\sum_{i=1}^m c_{ij} \alpha_i \right) \beta_j = 0$$

を考えると, $\sum_{i=1}^m c_{ij} \alpha_i \in M$ であり, $\beta_1, \dots, \beta_n$ が M 上 1 次独立という仮定から,

$$\sum_{i=1}^m c_{ij} \alpha_i = 0 \quad (j = 1, \dots, n)$$

を得る. さらに, $c_{ij} \in K$ であり, かつ $\alpha_1, \dots, \alpha_m$ が K 上 1 次独立という仮定から

$$c_{ij} = 0 \quad (i = 1, \dots, m, j = 1, \dots, n)$$

が導かれる. □

補題 2.8 M を体の拡大 L/K の中間体とし, $\alpha_1, \dots, \alpha_m \in M$, $\beta_1, \dots, \beta_n \in L$ とする.

$\alpha_1, \dots, \alpha_m$ が K 上 M を生成し, かつ $\beta_1, \dots, \beta_n$ が M 上 L を生成する

ならば, mn 個の L の元 $\alpha_i \beta_j$ ($i = 1, \dots, m, j = 1, \dots, n$) は K 上 L を生成する.

証明 任意の $\gamma \in L$ が, mn 個の元 $\alpha_i \beta_j$ の K 上の 1 次結合で表されることを確かめる. いま, $\beta_1, \dots, \beta_n$ が M 上 L を生成するので,

$$\gamma = \sum_{j=1}^n b_j \beta_j$$

をみたす $b_j \in M$ が存在する. さらに, $\alpha_1, \dots, \alpha_m$ が K 上 M を生成するという仮定から,

$$b_j = \sum_{i=1}^m a_{ij} \alpha_i \quad (j = 1, \dots, n)$$

となる $a_{ij} \in K$ がとれる. よって,

$$\gamma = \sum_{j=1}^n \left(\sum_{i=1}^m a_{ij} \alpha_i \right) \beta_j = \sum_{i=1}^m \sum_{j=1}^n a_{ij} \alpha_i \beta_j$$

と書け, γ が $\alpha_i \beta_j$ たちの K 上の 1 次結合で表されることがいえた. $\square$

定理 2.9 M を体の拡大 L/K の中間体とすると,

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

が成り立つ. とくに, L/K が有限次拡大であるためには, L/M , M/K がともに有限次拡大であることが必要十分である.

証明 $\alpha_1, \dots, \alpha_m$ を M の K 上の基底, $\beta_1, \dots, \beta_n$ を L の M 上の基底とすると,

$$m = [M : K], \quad n = [L : M].$$

ここで, 補題 2.7 より, mn 個の元 $\alpha_i \beta_j$ は K 上 1 次独立だから

$$[L : K] \geq mn = [L : M][M : K],$$

一方, 補題 2.8 より, L は K 上 mn 個の元によって生成されるから,

$$[L : K] \leq mn = [L : M][M : K]$$

が成り立ち, したがって等式が導かれる. $\square$

例 2.10 $K = \mathbf{Q}(\sqrt{7})$, $M = \mathbf{Q}(\sqrt[3]{5})$ とおき, さらに $L = \mathbf{Q}(\sqrt{7}, \sqrt[3]{5})$ とおく. K, M はどちらも $L/\mathbf{Q}$ の中間体だから, 例 2.6 を使えば

$$[L : \mathbf{Q}] = [L : K][K : \mathbf{Q}] = 2[L : K], \quad [L : \mathbf{Q}] = [L : M][M : \mathbf{Q}] = 3[L : M],$$

よって, $[L : \mathbf{Q}]$ は 2, 3 の公倍数, すなわち 6 の倍数であり, $[L : \mathbf{Q}] \geq 6$ を得る. 一方, $L = M(\sqrt{7})$ より, L は M 上 2 個の元 $1, \sqrt{7}$ で生成され, $[L : M] \leq 2$, よって $[L : \mathbf{Q}] \leq 6$ が導かれる. したがって, $[L : \mathbf{Q}] = 6$ が得られた.

§3. 代数的元

定義 3.1 L/K を体の拡大とし $\alpha \in L$ とする. α を根とする K 上の零でない多項式が存在するとき, すなわち,

$$\exists f(X) \in K[X] - \{0\} \quad \text{s.t.} \quad f(\alpha) = 0$$

であるとき, α は K 上**代数的**であるという. K 上代数的でない元は, K 上**超越的**であるといわれる.

次の補題は上の定義から直ちに導かれる.

補題 3.2 L/K を体の拡大とし $\alpha \in L$ とする. α が K 上代数的ならば, L/K の任意の中間体 M について, α は M 上代数的である.

例 3.3 (1) 体 K のすべての元は K 上代数的である.

(2) $\sqrt{3}, \frac{1+\sqrt{2}}{\sqrt[3]{5}}$ は, どちらも $\mathbf{Q}$ 上代数的である.

(3) 円周率 π は $\mathbf{Q}$ 上超越的である (Lindemann の定理 (1882)).

(4) 自然対数の底 e は $\mathbf{Q}$ 上超越的である (Hermite の定理 (1873)).

以下, L/K を体の拡大とし $\alpha \in L$ とする. いま, α が K 上代数的であるかはいかにかわらず, 写像

$$\varphi_\alpha : K[X] \longrightarrow L, \quad g(X) \mapsto g(\alpha)$$

を考えることができる. φ_α は可換環の準同型写像であり, その像は $K[\alpha]$ だから, 準同型定理によって $K[X]/\text{Ker } \varphi_\alpha$ は $K[\alpha]$ と同型;

$$K[X]/\text{Ker } \varphi_\alpha \cong K[\alpha].$$

ここで, 核は α を根とする K 上の多項式全体

$$\text{Ker } \varphi_\alpha = \{f(X) \in K[X] \mid f(\alpha) = 0\}$$

であり, $K[X]$ のイデアルである.

補題 3.4 α が K 上代数的であれば, $K[\alpha]$ は体である. よって, $K[\alpha] = K(\alpha)$ であり, 変数 X の属する類を α に対応させることによって, 体の同型

$$K[X]/\text{Ker } \varphi_\alpha \cong K(\alpha)$$

が得られる.

証明 可換環の同型 $K[X]/\text{Ker } \varphi_\alpha \cong K[\alpha]$ において, $K[\alpha]$ は体 L の部分環だから整域, したがって $\text{Ker } \varphi_\alpha$ は $K[X]$ の素イデアルである. ここで, α が K 上代数的だから, $\text{Ker } \varphi_\alpha \neq (0)$ である. よって, $K[X]$ が PID であることを考慮すると, $\text{Ker } \varphi_\alpha$ は $K[X]$ の極大イデアル, したがって $K[\alpha]$ は体である. $\square$

注意 α が K 上超越的ならば, $\text{Ker } \varphi_\alpha = (0)$, すなわち $K[X] \cong K[\alpha]$ である. とくに, $K[\alpha]$ は体ではない.

補題 3.5 α が K 上代数的で, $f(X)$ が α を根にもつ K 上の m 次多項式 ($m > 0$) ならば, $K(\alpha)$ は K 上のベクトル空間として $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ によって生成される. とくに

$$[K(\alpha) : K] \leq m = \deg f.$$

証明 前補題から $K[\alpha] = K(\alpha)$ であることに注意すれば, 任意の $\beta \in K(\alpha)$ に対して, $\beta = g(\alpha)$ をみたす $g(X) \in K[X]$ が存在する. このとき,

$$g(X) = q(X)f(X) + r(X), \quad r(X) = 0 \text{ または } \deg r < m = \deg f$$

をみたす $q(X), r(X) \in K[X]$ がとれるが, $f(\alpha) = 0$ より

$$\beta = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha).$$

そこで, $r(X) = a_0 + a_1X + a_2X^2 + \dots + a_{m-1}X^{m-1} \in K[X]$ と表しておけば

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{m-1}\alpha^{m-1} \quad (a_i \in K)$$

と書けるから, $K(\alpha)$ は K 上 $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ によって生成される. $\square$

補題 3.6 $K(\alpha)/K$ が有限次拡大ならば, α を根にもつ多項式 $f(X) \in K[X]$ で

$$[K(\alpha) : K] = \deg f$$

をみたすものが存在する. とくに, α は K 上代数的である.

証明 $n = [K(\alpha) : K]$ とすると, $n+1$ 個の元 $1, \alpha, \alpha^2, \dots, \alpha^n$ は K 上 1 次従属, よって (どれかは 0 ではない) $c_i \in K$ が存在して

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_n\alpha^n = 0$$

が成り立つ. そこで, $f(X) \in K[X]$ を

$$f(X) = c_0 + c_1X + c_2X^2 + \dots + c_nX^n$$

と定めれば, $f(X)$ は α を根とする零でない K 上の多項式であり, 補題 3.5 より

$$[K(\alpha) : K] \leq \deg f \leq n.$$

さらに, n の定義より, 不等号は等号に置き換わり $[K(\alpha) : K] = \deg f$ を得る. $\square$

定理 3.7 α に対して次は同値である.

- (i) α は K 上代数的である.
- (ii) $K(\alpha)/K$ は有限次拡大である.

証明 補題 3.5 と補題 3.6 からわかる. □

定理 3.8 α が K 上代数的であるとき, α を根にもつ $f(X) \in K[X]$ に対して次は同値である.

- (i) $f(X)$ は K 上既約である.
- (ii) $\text{Ker } \varphi_\alpha = (f(X))$.
- (iii) $[K(\alpha) : K] = \deg f$.
- (iv) $f(X)$ の次数は最小である. すなわち, $g(X) (\neq 0) \in K[X]$ が α を根にもつならば, $\deg f \leq \deg g$.

証明 まず, $f(\alpha) = 0$ より $f(X) \in \text{Ker } \varphi_\alpha$, 言い換えれば $(f(X)) \subset \text{Ker } \varphi_\alpha$ が成り立つことに注意する.

(i) $\Rightarrow$ (ii): (i) を仮定すれば, 単項イデアル $(f(X))$ は極大イデアルなので, (ii) を得る.

(ii) $\Rightarrow$ (iii): 補題 3.5 から $[K(\alpha) : K] \leq \deg f$ が成り立つ. とくに $K(\alpha)/K$ は有限次だから, 補題 3.6 を用いれば, $[K(\alpha) : K] = \deg g$ をみたす $g(X) \in \text{Ker } \varphi_\alpha$ がとれ, さらに仮定 (ii) より $g(X) = f(X)h(X)$ ($h(X) \in K[X]$) と表される. よって

$$[K(\alpha) : K] \leq \deg f \leq \deg f + \deg h = \deg g = [K(\alpha) : K],$$

したがって $[K(\alpha) : K] = \deg f$ を得る.

(iii) $\Rightarrow$ (iv): 補題 3.5 からすぐにわかる.

(iv) $\Rightarrow$ (i): $f(X)$ が K 上可約だとすると,

$$f(X) = g(X)h(X), \quad 1 \leq \deg g, \deg h < \deg f$$

をみたす $g(X), h(X) \in K[X]$ が存在する. ここで $g(\alpha)h(\alpha) = f(\alpha) = 0$ だから, $g(\alpha) = 0$ または $h(\alpha) = 0$ である. $g(\alpha) = 0$ のとき, 仮定 (iv) より $\deg f \leq \deg g$ となって $g(X)$ の取り方に矛盾する. $h(\alpha) = 0$ の場合も同様に矛盾する. よって $f(X)$ は K 上既約でなければならない. □

定義 3.9 前定理の (i)-(iv) のどれか (したがってすべて) をみたす多項式 $f(X) \in K[X]$ のうちモニックなものは一意的に定まる. これを α の K 上の**最小多項式**という. ここで, モニックな多項式とは, 最高次の係数が 1, すなわち

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

の形をした多項式のことである.

定理 3.10 α が K 上代数的ならば, α の K 上の最小多項式が存在する.

証明 定理 3.7, 補題 3.6 および最小多項式の定義から直ちに導かれる. $\square$

定理 3.11 $K(\alpha)/K$ が有限次拡大で $[K(\alpha) : K] = n$ ならば,

$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

は K 上ベクトル空間としての $K(\alpha)$ の基底である.

証明 $f(X)$ を α の K 上の最小多項式とすると, $n = \deg f$ である. さらに $f(\alpha) = 0$ であるから, 補題 3.5 から, n 個の元 $1, \alpha, \dots, \alpha^{n-1}$ は K 上 $K(\alpha)$ を生成している. 一方, $K(\alpha)$ は K 上 n 次元のベクトル空間だから, これらは基底となる. $\square$

例 3.12 (1) $\sqrt{3}$ の $\mathbf{Q}$ 上の最小多項式は $X^2 - 3$.

(2) $1 - \sqrt{5}$ の $\mathbf{Q}$ 上の最小多項式は $X^2 - 2X - 4$.

(3) $\frac{1}{\sqrt[3]{7}}$ の $\mathbf{Q}$ 上の最小多項式は $X^3 - \frac{1}{7}$.

(4) $\sqrt{2} + \sqrt[3]{3}$ の $\mathbf{Q}$ 上の最小多項式は $X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$.

最後の例は, たとえば, 以下を順に示すことで得られる; ただし,

$$\alpha = \sqrt{2} + \sqrt[3]{3}, \quad f(X) = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$$

とする.

(a) $f(\alpha) = 0$ より $[\mathbf{Q}(\alpha) : \mathbf{Q}] \leq \deg f = 6$ (補題 3.5)

(b) $\sqrt[3]{3} = \alpha - \sqrt{2}$ の両辺を 3 乗することにより, $\sqrt{2} \in \mathbf{Q}(\alpha)$

(c) $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, \sqrt[3]{3})$

(d) $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ は 2 でも 3 でも割り切れる (定理 2.9) から, $[\mathbf{Q}(\alpha) : \mathbf{Q}] \geq 6$

(e) (a), (d) をあわせて, $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 6 = \deg f$

(f) $f(X)$ は α の最小多項式であり, さらに $\mathbf{Q}$ 上既約である (定理 3.8).

§4. 代数拡大

定義 4.1 L/K を体の拡大とする. L の任意の元が K 上代数的であるとき, L は K 上代数的であるという. また, L/K を**代数拡大**という. L が K 上代数的でないとき, L は K 上**超越的**であるといい, L/K を**超越拡大**という.

命題 4.2 有限次拡大は代数拡大である.

証明 L/K を有限次拡大とする. 任意の $\alpha \in L$ に対して, L/K の中間体である $K(\alpha)$ は, 定理 2.9 より K 上の有限次拡大体だから, 定理 3.7 によって, α は K 上代数的である. L の任意の元が K 上代数的であることが示されたから, L/K は代数拡大である. $\square$

命題 4.3 体の拡大 L/K に対して次は同値である.

- (i) L/K は有限次拡大である.
- (ii) K 上代数的な有限個の元 $\alpha_1, \dots, \alpha_n \in L$ が存在して, $L = K(\alpha_1, \dots, \alpha_n)$ が成り立つ.

証明 (i) のとき, ベクトル空間としての L の K 上の基底 $\alpha_1, \dots, \alpha_n$ をとれば, 前命題よりこれらはすべて K 上代数的であり, (ii) が導かれる. 逆に, (ii) のときは,

$$K_0 = K, \quad K_1 = K_0(\alpha_1), \quad K_2 = K_1(\alpha_2), \quad \dots, \quad K_n = K_{n-1}(\alpha_n)$$

とおけば, 各 $i = 1, \dots, n$ について, α_i は K_{i-1} 上代数的だから, 定理 3.7 より K_i/K_{i-1} は有限次, よって, 定理 2.9 から $L = K_n$ は K 上有限次であり, (i) を得る. $\square$

定理 4.4 M を体の拡大 L/K の中間体とすると, 次は同値である.

- (i) L/K は代数拡大である.
- (ii) $L/M, M/K$ はともに代数拡大である.

証明 (i) ならば (ii) が成り立つのはあきらかなので, 以下, (ii) を仮定して (i), すなわち, 任意の $\alpha \in L$ が K 上代数的であることを確かめればよい. (ii) より L/M は代数的だから, α は M 上代数的, したがって, α を根とする M 上の零でない多項式

$$g(X) = c_0 + c_1X + \dots + c_nX^n \quad (c_i \in M)$$

が存在する. いま, $M_0 = K(c_0, c_1, \dots, c_n)$ とおくと, α は M_0 上代数的であるから, 定理 3.7 より $M_0(\alpha)/M_0$ は有限次である. 一方, 仮定 (ii) より M/K も代数的なので c_i は K 上代数的, よって, 前命題より M_0/K は有限次である. したがって, 定理 2.9 から, $M_0(\alpha)/K$ は有限次拡大であり, さらに命題 4.2 から代数拡大でもある. とくに α は K 上代数的である. $\square$

例 4.5 自然数 n に対して, $X^n - 1 = 0$ の根である複素数全体を W_n とする;

$$W_n = \{z \in \mathbf{C} \mid z^n = 1\}.$$

いま,

$$\zeta_n = e^{\frac{2\pi\sqrt{-1}}{n}} = \cos \frac{2\pi}{n} + \sqrt{-1} \sin \frac{2\pi}{n}$$

とおけば, $W_n = \{\zeta_n^j \mid j = 0, 1, \dots, n-1\}$ と具体的にかけ, これが $X^n - 1$ の根全体の集合と一致する. よって, 命題 4.3 より $\mathbf{Q}(W_n)/\mathbf{Q}$ は有限次, したがって, 命題 4.2 より代数拡大である (実際には, $\mathbf{Q}(W_n) = \mathbf{Q}(\zeta_n)$ が成り立っているのので, 命題 4.3 は必要とせず, 定理 3.7 を使えばよい). とくに n が素数 p の場合, ζ_p は $X^p - 1$ の既約因子 $X^{p-1} + X^{p-2} + \dots + X + 1$ の根だから, 定理 3.8 より,

$$[\mathbf{Q}(W_p) : \mathbf{Q}] = [\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1.$$

この等式は, 任意の自然数 n に対して, オイラー関数 φ を用いた等式

$$[\mathbf{Q}(W_n) : \mathbf{Q}] = [\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(n)$$

に拡張されるが, 証明は少し難しい.

補題 4.6 L/K を体の拡大とし, $A \subset L$ とすると, $K(A)$ は A の有限部分集合 B のすべてを走らせることにより

$$K(A) = \bigcup_B K(B)$$

と表される. すなわち, 任意の $\alpha \in K(A)$ に対して, $\alpha \in K(\beta_1, \dots, \beta_n)$ であるような有限個の $\beta_1, \dots, \beta_n \in A$ がとれる.

証明 $M = \bigcup_B K(B)$ とおく. このとき, $M \subset K(A)$ は直ちにわかる. 一方, あきらかに $K \subset M$ であり, また $A \subset M$ もすぐにわかるから, M が体であれば $K(A) \subset M$, したがって補題を得る. 以下, M が体であることを確かめる. M の任意の元 $\beta, \gamma \neq 0$ に対して, $\beta \in K(B)$, $\gamma \in K(C)$ をみたす A の有限部分集合 B, C がとれる. $D = B \cup C$ とおけば, D も A の有限部分集合であって $\beta, \gamma \in K(D)$ であるが, $K(D)$ は体なので, β, γ の和, 差, 積, 商は $K(D)$ に属する. さらに $K(D) \subset M$ なので, これらは M に属する. よって, M は体である. $\square$

定理 4.7 L/K を体の拡大とし, $A \subset L$ とする. A の任意の元が K 上代数的ならば $K(A)/K$ は代数拡大である.

証明 任意の $\alpha \in K(A)$ に対して, 前補題から, $\alpha \in K(\beta_1, \dots, \beta_n)$ をみたす $\beta_i \in A$ がとれる. 仮定より β_i は K 上代数的だから, 拡大 $K(\beta_1, \dots, \beta_n)/K$ は, 命題 4.3 より有限次, よって命題 4.2 より代数的, とくに α は K 上代数的である. $\square$

系 4.8 L/K を体の拡大とする. $\alpha, \beta \in L$ ($\beta \neq 0$) がともに K 上代数的ならば, それらの和と差 $\alpha \pm \beta$, 積 $\alpha\beta$, 商 α/β はどれも K 上代数的である.

証明 前定理より $K(\alpha, \beta)$ は K 上代数的であり, $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha, \beta)$ だから結論を得る. $\square$

例 4.9 複素数平面における単位円を S とする. また, ある自然数 n に対して, $z^n = 1$ をみたす複素数全体を W で表す.

$$S = \{z \in \mathbf{C} \mid |z| = 1\} = \{x + iy \in \mathbf{C} \mid x, y \in \mathbf{R}, x^2 + y^2 = 1\},$$

$$W = \{z \in \mathbf{C} \mid \exists n \in \mathbf{N} \text{ s.t. } z^n = 1\} = \bigcup_{n=1}^{\infty} W_n.$$

すべての $n \in \mathbf{N}$ について, $W_n \subset W \subset S$, したがって $\mathbf{Q}(W_n) \subset \mathbf{Q}(W) \subset \mathbf{Q}(S)$. このとき, 以下が成り立つ.

- (1) $\mathbf{Q}(W)/\mathbf{Q}$ は有限次ではない代数拡大である.
- (2) $\mathbf{Q}(S)/\mathbf{Q}$ は超越拡大である. したがって $\mathbf{Q}(S)/\mathbf{Q}(W)$ も超越拡大である.

(1) は, 定理 4.7 および例 4.5 から容易に証明できる. また, $0 < \varepsilon < 1$ をみたす $\mathbf{Q}$ 上超越的な実数 ε (たとえば $\varepsilon = \pi/4$ など...) をとれば, $\sqrt{1-\varepsilon^2} + \varepsilon i$ は S に属し, $\mathbf{Q}$ 上超越的であることが確かめられるから, (2) も示される.

命題 4.10 L/K を体の拡大とし, M をその中間体とする. $\alpha \in L$ が K 上代数的であるとき,

$$[M(\alpha) : M] \leq [K(\alpha) : K]$$

が成り立つ.

証明 α の K 上の最小多項式を $f(X)$ とすると, $\deg f = [K(\alpha) : K]$. 一方, $f(X)$ は M 上の多項式でもあるから, 補題 3.5 より, $[M(\alpha) : M] \leq \deg f$ であり, 求める不等式を得る. $\square$

例 4.11 $X^3 - 1$ の 1 でない根のひとつを ω とする (1 の原始 3 乗根). このとき, ω, ω^2 は $X^2 + X + 1$ の 2 根である. $X^3 - 2$ の実根を α とすれば, 他の根は $\alpha\omega, \alpha\omega^2$ で与えられる. $X^3 - 2$ は $\mathbb{Q}$ 上既約だから, 定理 3.8 より $\mathbb{Q}(\alpha)/\mathbb{Q}$ は 3 次拡大である. このとき,

- (a) $M_1 = \mathbb{Q}(\omega)$ とおけば, $[M_1(\alpha) : M_1] = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$,
- (b) $M_2 = \mathbb{Q}(\alpha\omega)$ とおけば, $[M_2(\alpha) : M_2] = 2 < 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$

が成り立ち, それぞれ, 前命題において, 等号が成り立つ例, 成り立たない例となっている.

定義 4.12 Ω/K を体の拡大とし, L, M をその中間体とすると, L, M をともに含む Ω の最小の部分体を L, M の**合成体**といい LM で表す. すなわち, $LM = L(M) = M(L)$ である.

定理 4.13 L, M を体の拡大 Ω/K の中間体とする. L/K が有限次拡大ならば,

$$[LM : M] \leq [L : K]$$

が成り立ち, とくに, LM/M も有限次拡大である.

証明 命題 4.3 より, $L = K(\alpha_1, \dots, \alpha_n)$ をみたす K 上代数的な元 α_i がとれる. そこで, 体の拡大列 $K_0 \subset K_1 \subset \dots \subset K_n$ および $M_0 \subset M_1 \subset \dots \subset M_n$ を

$$\begin{aligned} K_0 &= K, & K_1 &= K_0(\alpha_1), & K_2 &= K_1(\alpha_2), & \dots, & K_n &= K_{n-1}(\alpha_n) \\ M_0 &= M, & M_1 &= M_0(\alpha_1), & M_2 &= M_1(\alpha_2), & \dots, & M_n &= M_{n-1}(\alpha_n) \end{aligned}$$

と定めれば, 命題 4.10 より $[M_i : M_{i-1}] \leq [K_i : K_{i-1}]$. さらに, $L = K_n$ かつ $LM = M_n$ だから, 定理 2.9 を何度か適用して

$$[LM : M] = [M_n : M_{n-1}] \cdots [M_1 : M_0] \leq [K_n : K_{n-1}] \cdots [K_1 : K_0] = [L : K]$$

が導かれる. $\square$

§5. 根の添加

以下で扱う準同型写像はどれも零写像ではないとする。このとき、

体から（単位元をもつ）環への準同型写像は単射

であることに注意する。【理由】 体 K から環 R への準同型写像 $\sigma : K \rightarrow R$ の核 $\text{Ker } \sigma$ は体 K のイデアルだから、 $\{0\}$ または K のどちらかであるが、いま、 σ は零写像ではないとしているので、 $\text{Ker } \sigma = \{0\}$ 。したがって σ は単射である。

とくに、以下において、体から体への準同型写像が頻繁に現れるが、これらはすべて単射準同型である。

定義 5.1 L/K を体の拡大とする。 $\sigma : L \rightarrow M$, $\tau : K \rightarrow M$ がそれぞれ L, K から体 M への準同型写像であって、

$$\forall a \in K \quad \text{に対して} \quad \sigma(a) = \tau(a)$$

をみたすとき、 σ は τ の L への**延長**、あるいは、 τ は σ の K への**制限**であるという。また、このとき $\tau = \sigma|_K$ と表す。

定義 5.2 L, M がともに体 K の拡大体で、準同型写像 $\sigma : L \rightarrow M$ が K の恒等写像 $\text{id}_K : K \rightarrow K$ の延長であるとき、つまり、すべての $a \in K$ について $\sigma(a) = a$ が成り立つとき、 σ を K 上の**準同型写像**という。

定義 5.3 体 L から体 M への準同型写像 $\sigma : L \rightarrow M$ が全射であるとき、 σ を**同型写像**といい、 L と M は**同型**であるという。このとき

$$L \cong M$$

と表すことが多い。

定義 5.4 可換環 R から可換環 S への準同型写像

$$\sigma : R \longrightarrow S$$

が与えられたとき、 R 上の多項式 $f(X) \in R[X]$ に対して、その係数に σ をほどこして得られる S 上の多項式を $f^\sigma(X)$ と表す。すなわち、 $f(X) = \sum c_i X^i$ のとき $f^\sigma(X) = \sum \sigma(c_i) X^i$ と定める。このようにして、多項式環の間の準同型写像

$$R[X] \longrightarrow S[X]. \quad f(X) \mapsto f^\sigma(X)$$

が自然に定義される。

定理 5.5 $f(X)$ が体 K 上の既約多項式ならば、剰余環 $K[X]/(f(X))$ は体である。ここで、

$$\text{包含写像 } \iota: K \longrightarrow K[X], \quad \text{自然な全射 } \nu: K[X] \longrightarrow K[X]/(f(X))$$

の合成写像として

$$\sigma = \nu \circ \iota: K \longrightarrow K[X]/(f(X))$$

を定めると、 σ は体の準同型写像である。さらに、 $\alpha \in K[X]/(f(X))$ を

$$\alpha = \nu(X) = X + (f(X))$$

と定めれば（すなわち、 X の属する $K[X]/(f(X))$ の類を α とすれば）、 $f^\sigma(\alpha) = 0$ が成り立つ。

証明 $K[X]$ は PID だから、既約元で生成されるイデアル $(f(X))$ は極大イデアルであり、したがって、それによる剰余環 $K[X]/(f(X))$ は体である。また、 ι, ν はどちらも準同型写像だから、 σ は準同型写像である。いま、

$$f(X) = c_0 + c_1X + \cdots + c_nX^n \quad (c_i \in K)$$

とすれば、 $\iota(c_i) = c_i \in K \subset K[X]$ だから、 $\sigma(c_i) = \nu(c_i)$ 、したがって

$$f^\sigma(\alpha) = \nu(c_0) + \nu(c_1)\nu(X) + \cdots + \nu(c_n)\nu(X)^n = \nu(f(X)) = 0$$

となる。 □

定理 5.6 (クロネッカー) 体 K 上の定数でない任意の多項式 $f(X)$ に対して、 K の拡大体 L とその元 α で $f(\alpha) = 0$ をみたすものが存在する。

証明 $f(X)$ の K 上の既約因子をあらためて $f(X)$ とおくことにより、初めから $f(X)$ は K 上の既約多項式であるとしてよい。このとき、 $L = K[X]/(f(X))$ 、 $\alpha = X + (f(X)) \in L$ とおけば、定理 5.5 より、 L は体であり、単射準同型写像 $\sigma: K \rightarrow L$ が定義できて、 $f^\sigma(\alpha) = 0$ をみたす。そこで、 σ の像 $\sigma(K)$ を K と同一視すればよい。 □

注意 定理 5.6 から、 K 上の既約多項式 $f(X)$ に対して、 K の拡大体 L と $f(X)$ の根 $\alpha \in L$ が存在する。この α を用いて、準同型写像

$$\varphi_\alpha: K[X] \longrightarrow L, \quad g(X) \mapsto g(\alpha)$$

が定義できて、 $\text{Im } \varphi_\alpha = K(\alpha) \subset L$ がわかる (§3 を参照)。一方、 $\text{Ker } \varphi_\alpha$ が $K[X]$ のイデアル $(f(X))$ に一致することが、 $f(X)$ の K 上の既約性から確認できる (定理 3.8 参照)。したがって、準同型定理より、 φ_α は同型写像

$$\tilde{\varphi}_\alpha: K[X]/(f(X)) \longrightarrow K(\alpha)$$

を引き起こす。なお、定理 5.5 の準同型写像 σ と $\tilde{\varphi}_\alpha$ との合成 $\tilde{\varphi}_\alpha \circ \sigma$ は、 K から $K(\alpha)$ への包含写像に他ならない。

例 5.7 $X^2 + 1$ は実数体 $\mathbf{R}$ 上の既約多項式であり, その根 i に対して, $\mathbf{R}(i)$ は剰余環 $\mathbf{R}[X]/(X^2 + 1)$ と同型である. $\mathbf{C} = \mathbf{R}(i)$ とかけば,

$$\mathbf{C} \cong \mathbf{R}[X]/(X^2 + 1).$$

$1, i$ は $\mathbf{C}$ の $\mathbf{R}$ 上の基底であって, $\mathbf{C}$ の任意の元は $a + bi$ ($a, b \in \mathbf{R}$) の形に一意的に表される. ここで, $\mathbf{C}$ の 2 元

$$a + bi, \quad c + di \quad (a, b, c, d \in \mathbf{R})$$

に “対応” する多項式 $a + bX, c + dX \in \mathbf{R}[X]$ の積

$$ac + (ad + bc)X + bdX^2 = (ac - bd) + (ad + bc)X + bd(X^2 + 1)$$

は, $\mathbf{R}[X]/(X^2 + 1)$ においては $(ac - bd) + (ad + bc)X$ と同じ類に属する. つまり

$$(a + bX)(c + dX) \equiv (ac - bd) + (ad + bc)X \pmod{(X^2 + 1)}$$

であり, これはよく知られた複素数における積の公式

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

に対応する. この例は, 虚数単位 i を導入しなくても複素数体が構成できることを示している.

例 5.8 $f(X) = X^3 - 4X + 2$ は $\mathbf{Q}$ 上既約であり, その任意の根 α に対して, $\mathbf{Q}(\alpha)$ は剰余環 $\mathbf{Q}[X]/(f(X))$ と同型である;

$$\mathbf{Q}(\alpha) \cong \mathbf{Q}[X]/(f(X)).$$

$1, \alpha, \alpha^2$ は $\mathbf{Q}(\alpha)$ の $\mathbf{Q}$ 上の基底であり, $\mathbf{Q}(\alpha)$ の任意の元は $1, \alpha, \alpha^2$ の $\mathbf{Q}$ 上の 1 次結合で表される. たとえば

$$\beta = 1 + \alpha^2, \quad \gamma = 3 - 2\alpha + \alpha^2$$

の積は, 次の様に計算される. まず, 多項式の積を計算して得られる 4 次式

$$(1 + X^2)(3 - 2X + X^2) = X^4 - 2X^3 + 4X^2 - 2X + 3$$

を $f(X)$ で割って

$$X^4 - 2X^3 + 4X^2 - 2X + 3 = (X - 2)f(X) + (8X^2 - 12X + 7).$$

このとき, 余り $8X^2 - 12X + 7$ に対応する $\mathbf{Q}(\alpha)$ の元が $\beta\gamma$ である. こうして, 積 $\beta\gamma = 7 - 12\alpha + 8\alpha^2$ が計算できた.

例 5.9 $g(X) = X^3 + X^2 + X + 1$ は $\mathbf{Q}$ 上既約ではなく, $g(X) = (X+1)(X^2+1)$ のように $\mathbf{Q}$ 上の既約因子に分解される. この分解に対応して, 剰余環 $\mathbf{Q}[X]/(g(X))$ は

$$\mathbf{Q}[X]/(g(X)) \cong (\mathbf{Q}[X]/(X+1)) \oplus (\mathbf{Q}[X]/(X^2+1)) \cong \mathbf{Q} \oplus \mathbf{Q}(i).$$

のように体の直和と同型になることが確かめられる. 一般に, 体 K 上の多項式 $g(X)$ が可約であってかつ重根をもたないならば, 剰余環 $K[X]/(g(X))$ は複数個の体の直和と同型である.

定理 5.10 体 K 上の既約多項式 $f(X)$ とその任意の 2 根 α, β に対して, K 上の同型写像

$$\sigma: K(\alpha) \longrightarrow K(\beta)$$

で, $\sigma(\alpha) = \beta$ をみたすものが存在する.

証明 定理 5.6 の後の注意より, $g(X) \in K[X]$ を $g(\alpha)$ または $g(\beta)$ に写すことで定まる準同型写像

$$K[X] \longrightarrow K(\alpha), \quad K[X] \longrightarrow K(\beta)$$

は, 同型写像

$$\tau: K[X]/(f(X)) \longrightarrow K(\alpha), \quad \rho: K[X]/(f(X)) \longrightarrow K(\beta)$$

をそれぞれ引き起こす. このとき, $\sigma = \rho \circ \tau^{-1}$ が求める同型写像となる. $\square$

例 5.11 $X^2 + 1$ のひとつの根を i とすれば, もうひとつの根は $-i$ である. このとき, $\mathbf{C} = \mathbf{R}(i)$ から自分自身への写像

$$\mathbf{C} \longrightarrow \mathbf{C}, \quad a + bi \mapsto a - bi \quad (\text{ただし } a, b \in \mathbf{R})$$

が $\mathbf{R}$ 上の同型写像になっている. この写像は, ふつう複素共役写像とよばれる.

例 5.12 $X^3 - 2$ は $\mathbf{Q}$ 上既約であり, その実根を $\alpha = \sqrt[3]{2}$ とすると, 他の根は $\alpha\omega, \alpha\omega^2$ ($\omega = e^{2\pi i/3}$ は 1 の原始 3 乗根) である. このとき, 3 つの体 $\mathbf{Q}(\alpha), \mathbf{Q}(\alpha\omega), \mathbf{Q}(\alpha\omega^2)$ は互いに同型である. より具体的には, 写像

$$\begin{aligned} \sigma: \mathbf{Q}(\alpha) &\longrightarrow \mathbf{Q}(\alpha\omega), & a + b\alpha + c\alpha^2 &\mapsto a + b\alpha\omega + c\alpha^2\omega^2 \\ \tau: \mathbf{Q}(\alpha) &\longrightarrow \mathbf{Q}(\alpha\omega^2), & a + b\alpha + c\alpha^2 &\mapsto a + b\alpha\omega^2 + c\alpha^2\omega \end{aligned}$$

が $\mathbf{Q}$ 上の同型写像となっている ($a, b, c \in \mathbf{Q}$). $\mathbf{Q}(\alpha)$ は実数体の部分体であり, $\mathbf{Q}(\alpha\omega)$ と $\mathbf{Q}(\alpha\omega^2)$ は実数体には含まれていないが, これら 3 つの体は代数的には同等の性質をもっている.

§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) $\mathbb{C}$ は代数的閉体である (代数学の基本定理).
 (2) $\mathbb{R}$ 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 2 次以上の任意の多項式は L 上可約である.
- (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) $\Rightarrow$ (ii): L 上の既約多項式 $f(X)$ が, 仮定 (i) の下で 1 次であることを確かめればよい. 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) $\Rightarrow$ (iii): 一般に体上の多項式環は UFD である. とくに, 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) $\Rightarrow$ (iv): あきらか.
(iv) $\Rightarrow$ (i): M/L を代数拡大とすると, 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. $\square$

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

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

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. $\square$

例 6.6 (1) C は R の代数的閉包である.

(2) Q の代数的閉包は C の中で一意的に定まるが, それは 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 $L_1 \rightarrow L_2$ 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 $E = L$ でなければならない. このことは L が代数的閉体であることを示している. 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.) $\square$

以下において, 体 K に対して, 代数的閉包をひとつ固定し $\bar{K}$ で表す.

K 上の任意の代数拡大体は $\bar{K}/K$ 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 $L \rightarrow \overline{K}$ 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 $\text{Aut}(L/K)$ 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;

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

$\sigma, \tau \in \text{Aut}(L/K)$ 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 $\sigma \in \text{Aut}(\overline{K}/K)$ 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 $\text{Conj}(\alpha, K)$ 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 $\text{Conj}(\alpha, K)$ 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 $\sigma \in \text{Aut}(\overline{K}/K)$ が存在する.

証明 (i) $\Rightarrow$ (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) $\Rightarrow$ (i): $f(X)$ を α の K 上の最小多項式とすれば, (ii) のような $\sigma \in \text{Aut}(\overline{K}/K)$ 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. $\square$

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

$$\text{Conj}(\alpha, K) = \{ \sigma(\alpha) \mid \sigma \in \text{Aut}(\overline{K}/K) \}$$

が成り立つ.

例 6.13 $z \in \mathbf{C}$ の複素共役 $\bar{z}$ は, z の $\mathbf{R}$ 上の共役元であり, $\text{Conj}(z, \mathbf{R}) = \{z, \bar{z}\}$, さらに $\text{Aut}(\mathbf{C}/\mathbf{R})$ 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,

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

が成り立つ.

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

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

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,

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

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 $\mathbf{Q}$ 上の最小多項式は $X^2 - 2$, したがって

$$\text{Conj}(\sqrt{2}, \mathbf{Q}) = \{ \sqrt{2}, -\sqrt{2} \}.$$

また, $\sigma \in \text{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ とすると, $\sigma(\sqrt{2}) = \pm\sqrt{2}$. 符号のとり方により, $\sigma = \text{id}$ (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,

$$\text{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q}) = \{ \text{id}, \sigma \}$$

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,

$$\text{Conj}(\alpha, \mathbf{Q}) = \{ \alpha, \alpha\omega, \alpha\omega^2 \}.$$

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

$$\text{Aut}(\mathbf{Q}(\alpha)/\mathbf{Q}) = \{ \text{id} \}.$$

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.

§7. 標数

K を体とする. 自然数 n に対して $1 \in K$ の n 個の和を $\Gamma(n)$ とする;

$$\Gamma(n) = \underbrace{1 + \cdots + 1}_n$$

さらに, $\Gamma(-n) = -\Gamma(n)$, $\Gamma(0) = 0$ と定める.

補題 7.1 上で定めた写像

$$\Gamma: \mathbf{Z} \longrightarrow K$$

は, 可換環の準同型写像であり, その核は, $p = 0$ または素数によって, $\text{Ker } \Gamma = (p)$ と表される ($\text{Ker } \Gamma = p\mathbf{Z}$ と表してもよい).

証明 【準同型であること】 すべての $m, n \in \mathbf{Z}$ に対して

$$\Gamma(m+n) = \Gamma(m) + \Gamma(n), \quad \Gamma(mn) = \Gamma(m)\Gamma(n)$$

が成り立つことを確かめればよい. m, n のどちらかが 0 のときはあきらかに成り立つ. $m, n > 0$ のときは数学的帰納法を用いて確認できる. $n < 0$ のときは $\Gamma(-n) = -\Gamma(n)$ を使って正のときに帰着させればよい. $m < 0$ のときも同様である.

【核について】 Γ の像は体 K の部分環なので整域である. よって, 準同型定理より Γ の核は $\mathbf{Z}$ の素イデアル, したがって $\text{Ker } \Gamma = (0)$, または素数 p を用いて $\text{Ker } \Gamma = (p)$ と表される. $\square$

定義 7.2 体 K に対して, $\text{Ker } \Gamma = (p)$ をみたす $p \geq 0$ を K の**標数**という.

補題 7.1 より, K の標数は 0 または素数である. さらに, 整域 R に対しても同様にして標数を定義することができ, その場合でも, 標数は 0 または素数である.

写像 Γ を用いず直接的に標数を定義することもできる. K の単位元 1 を 2 個以上 p 個足し合わせて初めて 0 となる (すなわち

$$\underbrace{1 + \cdots + 1}_p = 0$$

となる) とき, p は素数である (証明してみよ). この p を K の標数とする. 1 をいくつ足し合わせても 0 にならないとき, K の標数を 0 とする.

定義 7.3 素数 p に対して

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$$

とかく. $\mathbf{F}_p$ は p 個の元からなる有限体であって, 標数は p である.

定理 7.4 K を標数 p の体とする.

(1) $p = 0$ ならば, 単射準同型

$$\mathbf{Q} \longrightarrow K$$

が一意的に存在する. すなわち, K は有理数体 $\mathbf{Q}$ と同型な部分体をもつ.

(2) $p > 0$ すなわち p が素数ならば, 単射準同型

$$\mathbf{F}_p \longrightarrow K$$

が一意的に存在する. すなわち, K は有限体 $\mathbf{F}_p$ と同型な部分体をもつ.

証明 (1) $n \neq 0$ ならば $\Gamma(n) \neq 0$ なので, $a = \frac{m}{n} \in \mathbf{Q}$ ($m, n \in \mathbf{Z}, n \neq 0$) のとき,

$$\tilde{\Gamma}(a) = \frac{\Gamma(m)}{\Gamma(n)}$$

とおくことによって

$$\tilde{\Gamma} : \mathbf{Q} \longrightarrow K$$

を定めることができる. $\tilde{\Gamma}$ が準同型写像であることを示すのは難しくない. よって $\tilde{\Gamma}$ は単射準同型写像である. 次に一意性を示すために,

$$\Delta : \mathbf{Q} \longrightarrow K$$

も単射準同型であるとする. このとき, $\tilde{\Gamma}(1) = 1 = \Delta(1)$ であり, 数学的帰納法を用いて $\tilde{\Gamma}(n) = \Delta(n)$ がすべての $n \in \mathbf{N}$ に対して成り立つことがわかる. このことから, すべての $a \in \mathbf{Q}$ に対して $\tilde{\Gamma}(a) = \Delta(a)$ を示すことは難しくない.

(2) $\Gamma : \mathbf{Z} \rightarrow K$ の核が $(p) = p\mathbf{Z}$ であることから, 準同型定理を適用すれば, 単射準同型写像

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \longrightarrow K$$

が得られる. 一意性については, $\mathbf{F}_p$ の元が $1 + \cdots + 1$ と表されることを使えば, すぐにわかる. $\square$

定理 7.5 K が有限体ならば, K の標数 p は素数であり, K は $\mathbf{F}_p$ の有限次拡大体と同型である. とくに, K が $\mathbf{F}_p$ の n 次拡大体と同型ならば, K は p^n 個の元からなる有限体である.

証明 前半は前定理からあきらかなので, 後半のみ示す. K は $\mathbf{F}_p$ の n 次拡大体であるとしてよい. $\alpha_1, \dots, \alpha_n$ を K の $\mathbf{F}_p$ 上の基底とすれば, K の任意の元は

$$c_1\alpha_1 + \cdots + c_n\alpha_n \quad (c_i \in \mathbf{F}_p)$$

の形に一意的に表され, 各 c_i の取り方は p 通りだから, K の元の個数は p^n である. $\square$

命題 7.6 p を素数とする.

(1) 体 K の標数が $p > 0$ ならば, 任意の $a, b \in K$ に対して

$$(a + b)^p = a^p + b^p$$

が成り立つ.

(2) $\mathbf{F}_p$ 上の多項式 $f(X)$ に対して,

$$f(X)^p = f(X^p)$$

が成り立つ.

証明 (1) 二項定理より

$$(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p.$$

ここで, p は素数なので, $1 \leq j \leq p-1$ のときの二項係数は

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} \equiv 0 \pmod{p}.$$

よって, K において $\binom{p}{j}a^j b^{p-j} = 0$ となり, 求める等式を得る.

(2) $f(X)$ を具体的に

$$f(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0 \quad (c_i \in \mathbf{F}_p)$$

と表せば, (1) の証明と同様の議論を繰り返し使って

$$f(X)^p = c_n^p X^{np} + c_{n-1}^p X^{(n-1)p} + \cdots + c_1^p X^p + c_0^p.$$

ここで, **フェルマーの定理**より $c_i^p = c_i$ が成り立つから,

$$f(X)^p = c_n (X^p)^n + c_{n-1} (X^p)^{n-1} + \cdots + c_1 X^p + c_0 = f(X^p)$$

を得る. □

例 7.7 -1 は 3 を法として平方非剰余なので, $X^2 + 1$ は $\mathbf{F}_3$ 上既約である. したがって, §5 の考察から, 2 次拡大 $K/\mathbf{F}_3$ がとれて, K において $X^2 + 1$ は根をもつ. 実際には K は剰余環 $\mathbf{F}_3[X]/(X^2 + 1)$ と同型であり, X の属する類に対応する K の元を α とすると, 具体的に

$$K = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}.$$

と書ける. ただし, $\mathbf{F}_3 = \{0, 1, 2\}$ とする. このとき, $\alpha^2 = -1$ に注意すれば

$$(1 + \alpha)(2\alpha) = 2\alpha + 2\alpha^2 = 2\alpha - 2 = 1 + 2\alpha$$

のように積が計算できる (すべての積をチェックして, K の乗積表を作成してみよ).

例 7.8 任意の素数 p に対して, F_p 上の 2 次拡大が存在することが以下のよう
にしてわかる.

- (1) p が奇素数の場合, p を法として平方非剰余である整数 u が存在するから,
前の例と同様にして, $F_p[X]/(X^2 - u)$ と同型な F_p 上の 2 次拡大が存在する.
(3) $p = 2$ の場合, $X^2 + X + 1$ が F_2 上既約であるから, やはり F_2 上の 2 次
拡大が存在する.

例 7.9 p を素数とし, K/F_p を有限次拡大で $n = [K : F_p]$ とする. 写像 ϕ を

$$\phi : K \longrightarrow K, \quad \alpha \mapsto \alpha^p$$

によって定める. このような ϕ を K の**フロベニウス写像**という.

- (1) ϕ は K から K への準同型写像である.
なぜなら, $\alpha, \beta \in K$ に対して, $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ はあきらかであり, さらに定
理 7.6 から $\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta)$ もいえるから.
(2) ϕ は F_p 上の同型写像である. すなわち $\phi \in \text{Aut}(K/F_p)$.
なぜなら, $a \in F_p$ に対して $\phi(a) = a^p = a$ がいえるから (フェルマーの定理).
(3) 自然数 j に対して, ϕ の j 個の合成を ϕ^j とする;

$$\phi^j = \underbrace{\phi \circ \cdots \circ \phi}_j$$

さらに $\phi^0 = \text{id}$ (恒等写像) とする. $\phi^j \in \text{Aut}(K/F_p)$ である.

- (4) $0 < j < n$ のとき, $\phi^j \neq \text{id}$.
なぜなら, もし $\phi^j = \text{id}$ ならば, すべての $\alpha \in K$ に対して $\alpha = \phi^j(\alpha) = \alpha^{p^j}$ だか
ら, K のすべての元は多項式 $X^{p^j} - X$ の根である. しかし, 定理 7.5 より, K
の元の個数は p^n なので, p^j 次多項式の根だけでは尽くせないはずなので矛盾.

- (5) ϕ^j ($0 \leq j < n$) は互いに相異なる.
なぜなら, もし $\phi^j = \phi^k$ ($0 \leq j < k < n$) ならば $\phi^{k-j} = \text{id}$ となって (4) に反する.

- (6) $\text{Aut}(K/F_p) = \{\text{id}, \phi, \phi^2, \dots, \phi^{n-1}\}$.
なぜなら, あきらかに $\text{Aut}(K/F_p) \supset \{\text{id}, \phi, \phi^2, \dots, \phi^{n-1}\}$. (5) より右辺は n 個
の元をもつから $|\text{Aut}(K/F_p)| \geq n$. 一方, 命題 15.1 (§15 補遺参照) より, $K^\times$
は巡回群であり, その生成元を γ とすれば $K = F_p(\gamma)$ なので, 定理 6.14 が適用
できて $|\text{Aut}(K/F_p)| \leq [K : F_p] = n$. よって, 不等式はすべて等号に置き換わ
り, 上の包含関係も等号で結ばれることがわかる.

- (7) $\phi^n = \text{id}$.
なぜなら, $\phi^n \in \text{Aut}(K/F_p)$ だから, (6) より $\phi^n = \phi^j$ ($0 \leq j < n$) をみたす j が
ある. もし $j > 0$ ならば, $\phi^{n-j} = \text{id}$ かつ $0 < n-j < n$ であり (4) に反する.
したがって $j = 0$ であり $\phi^n = \phi^0 = \text{id}$.

§8. 分離拡大

定理 6.3 より, 体 K 上の多項式 $f(X)$ は, $\overline{K}$ において $X - \alpha$ の形の 1 次式の積に分解される. 同じ 1 次式をまとめてしまえば

$$f(X) = c(X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2} \cdots (X - \alpha_r)^{m_r}$$

ただし $c \in K, \alpha_i \in \overline{K}, m_i \in \mathbf{N}$

と表すことができる. ここで, $\alpha_1, \dots, \alpha_r$ は $f(X)$ の相異なる根のすべてである. このとき, $m_i = 1$ であるような α_i を $f(X)$ の**単根**といい, $m_i \geq 2$ である α_i を**重根**という.

定義 8.1 体 K 上の多項式 $f(X)$ について, $\overline{K}$ におけるすべての根が単根であるとき, **分離的**であるという. 一方, $\overline{K}$ において重根をもつとき, **非分離的**であるという. 分離的な多項式を**分離多項式**, 非分離的な多項式を**非分離多項式**ともいう.

定理 8.2 K を標数 0 の体, または有限体とすると, K 上の任意の既約多項式は分離的である.

証明 K 上の既約多項式 $f(X)$ が重根 α をもつとする. このとき

$$f(X) = (X - \alpha)^2 g(X) \quad (g(X) \in \overline{K}[X])$$

とかけるが, 微分すれば

$$f'(X) = 2(X - \alpha)g(X) + (X - \alpha)^2 g'(X),$$

したがって, $f(\alpha) = f'(\alpha) = 0$ となる. ここで, K が標数 0 の体ならば, $f'(X)$ は零多項式ではなく, $\deg f'(X) < \deg f(X)$ が成り立つ. 一方で, $f(X)$ は α の K 上の最小多項式 (の定数倍) なので矛盾する. そこで以下, K は標数 $p > 0$ の有限体であるとする. この場合でも, $f'(X)$ が零多項式でなければ同様に矛盾する. $f'(X)$ が零多項式であるとする, 簡単な考察から

$$f(X) = c_0 + c_1 X^p + c_2 X^{2p} + \cdots + c_m X^{mp} \quad (c_i \in K)$$

と書けることが確かめられる. 一方, 定理 7.5 より $|K| = p^n$ ($n \geq 1$) とかけるが, このとき, 任意の $c \in K$ に対して $c^{p^n} = c$ が成り立つから, とくに $c_i = b_i^p$ ($b_i \in K$) と表すことができ, したがって

$$f(X) = b_0^p + b_1^p X^p + b_2^p X^{2p} + \cdots + b_m^p X^{mp} = (b_0 + b_1 X + b_2 X^2 + \cdots + b_m X^m)^p$$

となって, $f(X)$ の既約性に矛盾する. □

定義 8.3 K を体とする. $\alpha \in \overline{K}$ の K 上の最小多項式が分離的であるとき, α は K 上分離的であるという.

定理 6.14 の直後の注意から, 次の定理を得る.

定理 8.4 K を体とする. $\alpha \in \overline{K}$ について, 次は同値である.

- (i) α は K 上分離的である.
- (ii) $|\text{Conj}(\alpha, K)| = [K(\alpha) : K]$ が成り立つ.

補題 8.5 K を体とし, $\beta, \gamma \in \overline{K}$ とする. β が K 上分離的ならば,

$$K(\beta, \gamma) = K(\alpha)$$

をみたす $\alpha \in K(\beta, \gamma)$ が存在する.

証明 K が有限体のとき: K の有限次拡大体である $K(\beta, \gamma)$ も有限体なので, §15 補遺で証明される命題 15.1『体の乗法群の有限部分群は巡回群である』を使えば, $K(\beta, \gamma)^\times$ は巡回群である. α をその生成元とすれば, $K(\beta, \gamma) = K(\alpha)$ が成り立つ.

K が無限体のとき: β, γ から定まる $\overline{K}$ の有限部分集合

$$S = \left\{ \frac{\gamma - \gamma'}{\beta' - \beta} \mid \beta \neq \beta' \in \text{Conj}(\beta, K), \gamma' \in \text{Conj}(\gamma, K) \right\}$$

に属さない $s \in K$ がとれる. $\alpha = \gamma + s\beta$ とおく. このとき $K(\alpha) \subset K(\beta, \gamma)$ であるが, 一方で, もし $\beta \in K(\alpha)$ が示されれば, $\gamma = \alpha - s\beta \in K(\alpha)$ がいえて $K(\beta, \gamma) = K(\alpha)$ が得られる. そこで, 以下, $\beta \notin K(\alpha)$ を仮定して矛盾を導く. さて, β は K 上分離的だから $K(\alpha)$ 上も分離的であり, したがって定理 8.4 より

$$|\text{Conj}(\beta, K(\alpha))| = [K(\alpha, \beta) : K(\alpha)]$$

が成り立つが, $\beta \notin K(\alpha)$ を仮定したから右辺は 1 より大きくなっている. よって, $\beta' \neq \beta$ である $\beta' \in \text{Conj}(\beta, K(\alpha))$ がとれる. ここで, $\text{Conj}(\beta, K(\alpha)) \subset \text{Conj}(\beta, K)$ だから $\beta' \in \text{Conj}(\beta, K)$ でもあることに注意する. いま, $g(X)$ を γ の K 上の最小多項式とし, $G(X) = g(\alpha - sX)$ とおくと, $G(X)$ は $K(\alpha)$ 上の多項式であって

$$G(\beta) = g(\alpha - s\beta) = g(\gamma) = 0.$$

よって, $G(X)$ は β の $K(\alpha)$ 上の最小多項式で割り切れ, したがって $G(\beta') = 0$ が成り立つ. よって, $g(\alpha - s\beta') = 0$ より, $\alpha - s\beta' \in \text{Conj}(\gamma, K)$. そこで $\gamma' = \alpha - s\beta'$ とおけば

$$\gamma' = (\gamma + s\beta) - s\beta', \quad \therefore s = \frac{\gamma - \gamma'}{\beta' - \beta} \in S$$

となって s の取り方に矛盾する. □

定義 8.6 代数拡大 L/K において, すべての $\alpha \in L$ が K 上分離的であるとき, L/K を**分離拡大**という. また, このとき L は K 上**分離的**であるともいう.

定理 8.7 (原始元定理) 任意の有限次分離拡大は単純拡大である. すなわち L/K が有限次分離拡大ならば, $L = K(\alpha)$ をみたす $\alpha \in L$ が存在する.

証明 次数 $[L : K]$ に関する数学的帰納法で示す. $[L : K] = 1$ すなわち $L = K$ のときはあきらか. 以下, $[L : K] > 1$ とし, 次数が $[L : K]$ より小さい場合は成り立つと仮定する (帰納法の仮定). $[L : K] > 1$ より, $\beta \notin K$ である $\beta \in L$ が存在する. このとき

$$[L : K(\beta)] < [L : K] \quad \text{かつ} \quad L/K(\beta) \text{ は分離拡大}$$

だから, 帰納法の仮定より $L = K(\beta, \gamma)$ をみたす $\gamma \in L$ が存在する. そこで, 補題 8.5 を適用すれば, 定理の主張を得る. $\square$

定理 8.8 K を標数 0 の体, または有限体とする.

- (1) K 上のすべての既約多項式は分離的である.
- (2) K 上のすべての代数拡大体は分離的である.
- (3) K 上のすべての有限次拡大体は単純である.

証明 定理 8.2 および定理 8.7 からすぐに得られる. $\square$

次の補題は, 定理 6.11 を使って証明される (§15 補遺を参照).

補題 8.9 体 K 上代数的である α, β が, $\beta \in K(\alpha)$ をみたすならば,

$$|\text{Conj}(\alpha, K)| = |\text{Conj}(\alpha, K(\beta))| |\text{Conj}(\beta, K)|$$

が成り立つ.

命題 8.10 体 K 上分離的である α に対して, $K(\alpha)/K$ は分離拡大である.

証明 定理 6.14 より, 任意の $\beta \in K(\alpha)$ に対して

$$|\text{Conj}(\alpha, K(\beta))| \leq [K(\alpha) : K(\beta)], \quad |\text{Conj}(\beta, K)| \leq [K(\beta) : K]$$

が一般に成り立っている. もし, β が K 上分離的でないならば, 定理 8.4 より後者の等号は成り立たず, したがって, 前補題から

$$|\text{Conj}(\alpha, K)| < [K(\alpha) : K(\beta)][K(\beta) : K] = [K(\alpha) : K].$$

ところが, α は K 上分離的だから, 再び定理 8.4 より $|\text{Conj}(\alpha, K)| = [K(\alpha) : K]$ でなければならない, 矛盾である. よって, すべての $\beta \in K(\alpha)$ は K 上分離的である. $\square$

定理 8.11 M を代数拡大 L/K の中間体とすると、次は同値である。

- (i) L/K は分離拡大である。
- (ii) $L/M, M/K$ はともに分離拡大である。

証明 (i) ならば (ii) は明らかなので、以下では (ii) を仮定して (i)、すなわち、 L/K が分離的であることを示す。

L/K が有限次拡大のとき: $L/M, M/K$ はともに有限次分離拡大だから、原始元定理 (定理 8.7) より、 $M = K(\beta), L = M(\gamma)$ をみたす $\beta \in M, \gamma \in L$ が存在する。 β は K 上分離的だから、定理 8.4 より

$$|\text{Conj}(\beta, K)| = [K(\beta) : K]$$

が成り立ち、さらに $L = K(\beta, \gamma)$ に補題 8.5 が適用できて、 $L = K(\alpha)$ となる $\alpha \in L$ を取ることができる。このとき、 α は $M = K(\beta)$ 上分離的だから、再び定理 8.4 から

$$|\text{Conj}(\alpha, K(\beta))| = [K(\beta, \alpha) : K(\beta)] = [K(\alpha) : K(\beta)].$$

したがって、補題 8.9 を用いて

$$|\text{Conj}(\alpha, K)| = [K(\alpha) : K]$$

が導かれ、定理 8.4 と命題 8.10 から、 $L = K(\alpha)$ が K 上分離的であることが示された。

L/K が無限次拡大のとき: 任意の $\delta \in L$ が K 上分離的であることを確かめればよい。 δ の M 上の最小多項式の係数をすべて K に添加した M の部分体を M_0 とする。このとき、 M_0/K が分離的であることはあきらかだが、命題 8.10 より $M_0(\delta)/M_0$ も分離的であり、しかも $M_0(\delta)/K$ は有限次拡大である。よって、上で示したことから $M_0(\delta)/K$ は分離的、とくに δ が K 上分離的であることが確かめられた。 $\square$

命題 8.12 K を体とし、 $\alpha, \beta \in \overline{K}$ が K 上分離的であるとする。このとき、 $K(\alpha, \beta)/K$ は分離拡大である。とくに、 $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ はどれも K 上分離的である。

証明 命題 8.10 より、 $K(\alpha)/K$ は分離拡大、さらに、 β は $K(\alpha)$ 上も分離的だから、 $K(\alpha, \beta)/K(\alpha)$ も分離拡大である。よって、前定理より結論を得る。 $\square$

定理 8.13 L, E がともに K 上分離的ならば、 $LE, L \cap E$ はどちらも K 上分離的である。

証明 LE の元は $L \cup E$ の有限個の元から加減乗除によって表されるから、前命題によって K 上分離的であることがわかり、したがって LE/K は分離拡大である。 $(L \cap E)/K$ が分離拡大であることは明らかである。 $\square$

§9. 正規拡大

定理 9.1 代数拡大 L/K について, 次は同値である.

- (i) すべての $\sigma \in \text{Aut}(\overline{K}/K)$ に対して $\sigma(L) \subset L$.
- (ii) すべての $\sigma \in \text{Aut}(\overline{K}/K)$ に対して $\sigma(L) = L$.
- (iii) すべての $\alpha \in L$ に対して $\text{Conj}(\alpha, K) = \{ \sigma(\alpha) \mid \sigma \in \text{Aut}(L/K) \}$.
- (iv) すべての $\alpha \in L$ に対して $\text{Conj}(\alpha, K) \subset L$.

証明 (i) $\Rightarrow$ (ii): $\sigma \in \text{Aut}(\overline{K}/K)$ ならば, $\sigma^{-1} \in \text{Aut}(\overline{K}/K)$ でもあるから, $\sigma^{-1}(L) \subset L$ が (i) より得られ, $L = \sigma(\sigma^{-1}(L)) \subset \sigma(L)$. よって (ii) が導かれた.

(ii) $\Rightarrow$ (iii): $\alpha \in L$ とし, その K 上の最小多項式を $f(X)$ とする. 任意の $\sigma \in \text{Aut}(L/K)$ に対して, $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ より, $\sigma(\alpha) \in \text{Conj}(\alpha, K)$,

$$\therefore \{ \sigma(\alpha) \mid \sigma \in \text{Aut}(L/K) \} \subset \text{Conj}(\alpha, K).$$

逆の包含関係を示すために, $\beta \in \text{Conj}(\alpha, K)$ とすると, 定理 6.11 (または系 6.12) から, $\beta = \tau(\alpha)$ をみたす $\tau \in \text{Aut}(\overline{K}/K)$ がとれる. このとき (ii) より $\tau(L) = L$ なので, $\sigma = \tau|_L$ とおけば, $\sigma \in \text{Aut}(L/K)$ であって, かつ $\beta = \tau(\alpha) = \sigma(\alpha)$ であるから, 逆の包含関係が示された.

(iii) $\Rightarrow$ (iv): $\alpha \in L$ ならば $\{ \sigma(\alpha) \mid \sigma \in \text{Aut}(L/K) \} \subset L$, よって (iii) より (iv) を得る.

(iv) $\Rightarrow$ (i): $\alpha \in L$ とすると, 系 6.12 より, $\sigma \in \text{Aut}(\overline{K}/K)$ のとき $\sigma(\alpha) \in \text{Conj}(\alpha, K)$. よって (iv) より $\sigma(\alpha) \in L$ となり, (i) が得られた. $\square$

定義 9.2 前定理の条件が成り立つような代数拡大 L/K を**正規拡大**という. L は K 上**正規**であるともいう.

命題 9.3 任意の体 K の任意の 2 次拡大体は K 上正規である.

証明 L/K を 2 次拡大とする. 定理 9.1 の条件 (iv), すなわち, 任意の $\alpha \in L$ に対して $\text{Conj}(\alpha, K) \subset L$ を確かめればよい. $\alpha \in K$ ならばあきらかなので, $\alpha \notin K$ とする. このとき, α の K 上の最小多項式は 2 次式であり $X^2 - cX + d$ ($c, d \in K$) とすれば, 解と係数の関係から $\text{Conj}(\alpha, K) = \{ \alpha, c - \alpha \} \subset L$. $\square$

定義 9.4 体 K 上の多項式 $f(X)$ に対して, その $\overline{K}$ における根すべてを K に添加して得られる $\overline{K}$ の部分体を $f(X)$ の K 上の**最小分解体**という. すなわち,

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n), \quad a \in K^\times, \quad \alpha_i \in \overline{K}$$

とするとき, $K(\alpha_1, \dots, \alpha_n)$ が $f(X)$ の K 上の最小分解体である.

例 9.5 α が K 上代数的であるとき, α の K 上の最小多項式の K 上の最小分解体は $K(\text{Conj}(\alpha, K))$ で与えられる.

定理 9.6 代数拡大 L/K について, 次は同値である.

- (i) L/K は有限次正規拡大である.
- (ii) L は K 上のある多項式の K 上の最小分解体である.

証明 (i) $\Rightarrow$ (ii): L/K は有限次拡大だから, K 上代数的な有限個の $\alpha_1, \dots, \alpha_n$ によって $L = K(\alpha_1, \dots, \alpha_n)$ と表される. L/K が正規であるという仮定より $\text{Conj}(\alpha_i, K) \subset L$ が成り立つ. 一方, $f_i(X)$ を α_i の K 上の最小多項式とすると, $\text{Conj}(\alpha_i, K)$ は $f_i(X)$ の根全体の集合と一致する. したがって,

$$f(X) = f_1(X) \cdots f_n(X)$$

とおくと, その K 上の最小分解体は

$$K(\text{Conj}(\alpha_1, K) \cup \cdots \cup \text{Conj}(\alpha_n, K)) \subset L$$

であるが, 左辺が $K(\alpha_1, \dots, \alpha_n) = L$ を含むのはあきらかなので (ii) が得られた.

(ii) $\Rightarrow$ (i): L が $f(X) \in K[X]$ の K 上の最小分解体であるとする. すなわち, $f(X)$ の根全体の集合を A とすれば, $L = K(A)$ が成り立つ. いま, $\sigma \in \text{Aut}(\bar{K}/K)$ を任意にとる. $\alpha \in A$ ならば, 定理 6.11 より $\sigma(\alpha) \in \text{Conj}(\alpha, K)$ であり, さらに α の K 上の最小多項式は $f(X)$ の因子だから, $\text{Conj}(\alpha, K) \subset A$, よって $\sigma(A) \subset A$ が成り立つ (実際には $\sigma(A) = A$ がいえる). したがって, 定理 9.1 の (i) より, L は K 上正規である. $\square$

定理 9.7 α が体 K 上代数的であるとき, 次は同値である.

- (i) $K(\alpha)/K$ は正規拡大である.
- (ii) $K(\alpha)$ は α の K 上の最小多項式の K 上の最小分解体である.
- (iii) $K(\alpha) = K(\text{Conj}(\alpha, K))$ が成り立つ.
- (iv) $|\text{Aut}(K(\alpha)/K)| = |\text{Conj}(\alpha, K)|$ が成り立つ.

証明 (i) $\Rightarrow$ (iv): 定理 6.14 の証明で見たように, 単射

$$\Phi : \text{Aut}(K(\alpha)/K) \longrightarrow \text{Conj}(\alpha, K), \quad \sigma \mapsto \sigma(\alpha)$$

が定まる. いま, $\beta \in \text{Conj}(\alpha, K)$ を任意にとれば, 仮定 (i) より $\beta \in K(\alpha)$ だから $K(\beta) \subset K(\alpha)$, さらに K 上の次数を考えることにより $K(\beta) = K(\alpha)$ である. 一方, 定理 6.11 より $\tau(\alpha) = \beta$ をみたす $\tau \in \text{Aut}(\bar{K}/K)$ が存在する. そこで, $\sigma = \tau|_{K(\alpha)}$ とおけば,

$$\sigma(K(\alpha)) = K(\sigma(\alpha)) = K(\beta) = K(\alpha),$$

よって $\sigma \in \text{Aut}(K(\alpha)/K)$ であって、もちろん $\sigma(\alpha) = \beta$. したがって、上記写像 Φ が全単射であることがわかり、(iv) を得る.

(iv) $\Rightarrow$ (iii): 上で定めた Φ は、仮定 (iv) より全単射である. すなわち、 $\beta \in \text{Conj}(\alpha, K)$ ならば、 $\sigma(\alpha) = \beta$ をみたす $\sigma \in \text{Aut}(K(\alpha)/K)$ が存在し、とくに $\beta \in K(\alpha)$. したがって

$$K(\text{Conj}(\alpha, K)) \subset K(\alpha).$$

逆の包含関係はあきらかだから、(iii) が示された.

(iii) $\Rightarrow$ (ii): は最小分解体の定義より直ちにわかる.

(ii) $\Rightarrow$ (i): も定理 9.6 よりあきらかである. □

例 9.8 K が $\mathbf{R}$ の部分体で、 $K(\alpha)/K$ が 3 次拡大であるとする. $f(X)$ を α の K 上の最小多項式とすると、

- (a) $K(\alpha)/K$ が正規拡大ならば、 $f(X)$ の 3 根はすべて実数である.
- (b) $f(X)$ の実根がただひとつならば、 $K(\alpha)/K$ は正規ではない.

例 9.9 3 次既約多項式 $g(X) = X^3 - 3X + 1$ の任意のひとつの根を β とすると、 $\mathbf{Q}(\beta)/\mathbf{Q}$ は正規拡大である. 実際、

$$g\left(\frac{1}{1-\beta}\right) = -\frac{g(\beta)}{(1-\beta)^3} = 0, \quad g\left(1 - \frac{1}{\beta}\right) = -\frac{g(\beta)}{\beta^3} = 0$$

より、 $g(X)$ の他の 2 根が $\frac{1}{1-\beta}$, $1 - \frac{1}{\beta}$ であることが確かめられるので、 $\mathbf{Q}(\beta)$ は $g(X)$ の $\mathbf{Q}$ 上の最小分解体、よって定理 9.7 より正規であることがわかる.

例 9.10 ω を 1 の原始 3 乗根とし、

$$K = \mathbf{Q}(\omega), \quad M = \mathbf{Q}(\sqrt[3]{5}), \quad L = KM = \mathbf{Q}(\omega, \sqrt[3]{5})$$

とおく. $K = \mathbf{Q}(\sqrt{-3})$, $L = \mathbf{Q}(\sqrt[3]{5}, \sqrt{-3})$ と表せることに注意.

- (a) K は、 $X^2 + X + 1$ の $\mathbf{Q}$ 上の最小分解体であり、 $\mathbf{Q}$ 上正規である.
- (b) L は、 $X^3 - 5$ の $\mathbf{Q}$ 上の最小分解体であり、 $\mathbf{Q}$ 上正規である.
- (c) M は、 $\text{Conj}(\sqrt[3]{5}, \mathbf{Q}) = \{\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}\} \not\subset M$ より、 $\mathbf{Q}$ 上正規ではない.

例 9.11 自然数 n に対して $\zeta_n \in \mathbf{C}^\times$ を 1 の原始 n 乗根とする ($\zeta_n = e^{2\pi i/n}$ であるとしてよい). このとき、 $\mathbf{Q}(\zeta_n)$ は $\mathbf{Q}$ 上正規である. 実際、 $\mathbf{Q}(\zeta_n)$ は $X^n - 1$ の $\mathbf{Q}$ 上の最小分解体である.

例 9.12 $\mathbb{Q}$ 上の拡大体 K が $\zeta_n \in K$ をみたすとき, 任意の $a \in K$ に対して $K(\sqrt[n]{a})/K$ は正規拡大である. 実際, L を $X^n - a$ の K 上の最小分解体とすると,

$$L = K(\sqrt[n]{a}, \zeta_n \sqrt[n]{a}, \dots, \zeta_n^{n-1} \sqrt[n]{a})$$

であって, L/K は正規拡大である. ここで, $\zeta_n \in K$ に注意すれば, 任意の $j \in \mathbb{Z}$ に対して $\zeta_n^j \sqrt[n]{a} \in K(\sqrt[n]{a})$, よって $L = K(\sqrt[n]{a})$ となる.

定理 9.13 L/K を正規拡大とすると, 任意の中間体 M に対して L/M は正規拡大である.

証明 $\alpha \in L$ のとき, $\text{Conj}(\alpha, M) \subset \text{Conj}(\alpha, K)$ だから, 定理 9.1 (iv) を使えばよい. $\square$

注意 正規拡大 L/K の中間体 M は, 一般には K 上正規にはならない. 例 9.10 を参照.

定理 9.14 L, E がともに K 上正規ならば, $LE, L \cap E$ はどちらも K 上正規である.

証明 定理 9.1 の条件 (i) を使えばよい. $\square$

定理 9.15 L/K を正規拡大とすると, 任意の拡大 F/K に対して LF/F は正規拡大である.

証明 合成体 LF を扱う場合, L, F を含む体 Ω の存在を仮定していることに注意する (定義 4.12 参照). さらに Ω は代数的閉体であるとしてよく, また, K, F の代数的閉包 $\bar{K}, \bar{F}$ が Ω の部分体として一意的に定まり $\bar{K} \subset \bar{F}$ が成り立つことが, §6 での考察からわかる. この状況の下で, $\sigma \in \text{Aut}(\bar{F}/F)$ に対して, $\sigma|_{\bar{K}} \in \text{Aut}(\bar{K}/K)$ が成り立つことを確かめるのは難しくない. よって, L/K が正規であるという仮定より $\sigma(L) \subset L$ となるので, $\sigma(LF) = \sigma(L)\sigma(F) \subset LF$ が得られ, LF/F は正規である. $\square$

定義 9.16 代数拡大 L/K に対して, L を含む K 上の最小の正規拡大体を L/K の正規閉包という.

命題 9.17 α が K 上代数的であるとき, $K(\alpha)/K$ の正規閉包は $K(\text{Conj}(\alpha, K))$ である.

証明 L を $K(\alpha)$ の正規閉包とする. 例 9.5 と定理 9.6 より, $K(\text{Conj}(\alpha, K))$ は K 上正規だから, 最小の正規拡大である L は $K(\text{Conj}(\alpha, K))$ に含まれる. 一方, $\alpha \in L$ だから, 定理 9.1 の条件 (iv) より, $\text{Conj}(\alpha, K) \subset L$, したがって $K(\text{Conj}(\alpha, K)) \subset L$. よって $L = K(\text{Conj}(\alpha, K))$ を得る. $\square$

§10. ガロア拡大

定義 10.1 分離拡大かつ正規拡大である体の拡大を**ガロア拡大**という. L/K がガロア拡大のとき, $\text{Aut}(L/K)$ をとくに $\text{Gal}(L/K)$ と表し, L/K の**ガロア群**, または L の K 上のガロア群という.

定理 10.2 有限次拡大 L/K に対して, 次は同値である.

- (i) L/K はガロアである.
- (ii) L は K 上のある分離多項式の K 上の最小分解体である.

証明 $(i) \Rightarrow (ii)$: 仮定 (i) より, とくに L/K は有限次分離拡大, よって定理 8.7 より, ある $\alpha \in L$ を用いて $L = K(\alpha)$ とかける. α は K 上分離的だからその最小多項式 $f(X) \in K[X]$ は分離多項式である. さらに L/K は正規だから $\text{Conj}(\alpha, K) \subset L$, したがって, $f(X)$ の K 上の最小分解体 $K(\text{Conj}(\alpha, K))$ は L に等しい.

$(ii) \Rightarrow (i)$: L が K 上の分離多項式 $f(X)$ の K 上の最小分解体であるとする. このとき, 定理 9.6 より L/K は正規拡大である. 一方, $f(X)$ の根すべてを $\alpha_i (i = 1, \dots, r)$ とすれば, $L = K(\alpha_1, \dots, \alpha_r)$ と表されるが, 各 α_i は K 上分離的なので, 命題 8.12 を繰り返し適用すれば, L/K が分離的であることが導かれる. $\square$

定理 10.3 L/K が有限次ガロア拡大ならば, $|\text{Gal}(L/K)| = [L : K]$ が成り立つ.

証明 L/K は有限次分離拡大なので, 原始元定理 (定理 8.7) によって $L = K(\alpha)$ と表され, さらに定理 8.4 より, $|\text{Conj}(\alpha, K)| = [K(\alpha) : K]$ が成り立つ. 一方, $L = K(\alpha)$ は K 上正規でもあるので, 定理 9.7 より $|\text{Gal}(K(\alpha)/K)| = |\text{Conj}(\alpha, K)|$, したがって結論の等式を得る. $\square$

定義 10.4 L を体とし, Ω を L の拡大体とする. L から Ω への単射準同型写像の集合 H に対して,

$$L^H = \{x \in L \mid \text{任意の } \sigma \in H \text{ に対して } \sigma(x) = x\}$$

を H の (L における) **不変体**という (H の元が準同型写像であることを用いれば, 不変体 L^H は L の部分体であることが確かめられる).

以下, 多くの場合, H は代数拡大 L/K の自己同型群 $\text{Aut}(L/K)$ の部分群である. 次の補題は, 不変体の定義からすぐに示すことができる.

補題 10.5 L/K を体の拡大とする.

- (1) L/K の任意の中間体 M に対して, $M \subset L^{\text{Aut}(L/M)}$ が成り立つ.
- (2) $\text{Aut}(L/K)$ の任意の部分群 H に対して, $H \subset \text{Aut}(L/L^H)$ が成り立つ.

定理 10.6 代数拡大 L/K がガロアであるためには, $K = L^{\text{Aut}(L/K)}$ であることが必要十分である.

証明 必要性: $M = L^{\text{Aut}(L/K)}$ とおくと, 前補題 (1) から $K \subset M$ である. そこで, L/K がガロア, すなわち分離的かつ正規であることを仮定して, $M \subset K$ を導く. そのために $\alpha \in M$ を任意にとる. M の定義から, 任意の $\sigma \in \text{Aut}(L/K)$ に対して $\sigma(\alpha) = \alpha$ であるが, L/K は正規なので, 定理 9.1 の性質 (iii) を用いれば, $\text{Conj}(\alpha, K) = \{\alpha\}$ が得られる. さらに, α は K 上分離的だから, 定理 8.4 より

$$[K(\alpha) : K] = |\text{Conj}(\alpha, K)| = 1, \quad \therefore K(\alpha) = K$$

よって $\alpha \in K$ となるから, $M \subset K$ が導かれた.

十分性: $K = L^{\text{Aut}(L/K)}$ を仮定し, 任意の $\alpha \in L$ に対して,

$$(\spadesuit) \quad |\text{Conj}(\alpha, K)| = [K(\alpha) : K], \quad \text{Conj}(\alpha, K) \subset L$$

を確かめればよい. なぜなら, 前者の等式と定理 8.4 から L/K の分離性が, 後者の包含関係と定理 9.1 の性質 (iv) から L/K の正規性が導かれるからである. いま,

$$B_\alpha = \{ \sigma(\alpha) \mid \sigma \in \text{Aut}(L/K) \}$$

とおけば, $B_\alpha \subset L$ であり, 系 6.12 より

$$(\heartsuit) \quad B_\alpha \subset \{ \sigma(\alpha) \mid \sigma \in \text{Aut}(\overline{K}/K) \} = \text{Conj}(\alpha, K),$$

よって,

$$(\diamondsuit) \quad |B_\alpha| \leq |\text{Conj}(\alpha, K)| \leq [K(\alpha) : K]$$

が成り立つ. とくに, B_α は有限集合であり, L 上の多項式

$$f_\alpha(X) = \prod_{\beta \in B_\alpha} (X - \beta)$$

を定義することができる. ここで, 任意の $\sigma \in \text{Aut}(L/K)$ に対して

$$f_\alpha^\sigma(X) = \prod_{\beta \in B_\alpha} (X - \sigma(\beta)) = \prod_{\gamma \in \sigma(B_\alpha)} (X - \gamma)$$

だが, $\text{Aut}(L/K)$ が群であることに注意すれば, $\sigma(B_\alpha) = B_\alpha$, よって $f_\alpha^\sigma(X) = f_\alpha(X)$ であることがわかる. すなわち $f_\alpha(X)$ の係数は $L^{\text{Aut}(L/K)} = K$ に属する; $f_\alpha(X) \in K[X]$. さらに $f_\alpha(\alpha) = 0$ であるから, 補題 3.5 より

$$[K(\alpha) : K] \leq \deg f_\alpha(X) = |B_\alpha|.$$

よって, $(\heartsuit)$ の包含関係と $(\diamondsuit)$ の不等号はすべて等号に置き換えられ,

$$\text{Conj}(\alpha, K) = B_\alpha \subset L, \quad |\text{Conj}(\alpha, K)| = [K(\alpha) : K],$$

すなわち $(\spadesuit)$ が確かめられた. □

系 10.7 L/K をガロア拡大としそのガロア群を G とする. M を L/K の中間体とすると, L/M はガロア拡大でそのガロア群 $\text{Gal}(L/M)$ は G の部分群であり, さらに $L^{\text{Gal}(L/M)} = M$ が成り立つ.

証明 L/K の分離性から L/M が分離的であること (定理 8.11), また, L/K の正規性から L/M が正規拡大であること (定理 9.13) がわかるから, L/M はガロア拡大である. 後半は前定理から導かれる. $\square$

定理 10.8 L/K を有限次ガロア拡大としそのガロア群を G とする. H を $\text{Gal}(L/K)$ の部分群とすると, L^H は L/K の中間体, したがって L/L^H はガロア拡大であり, さらに $\text{Gal}(L/L^H) = H$ が成り立つ.

証明 $M = L^H$ とおく. L/M がガロア拡大であることは, 系 10.7 で示されている. 補題 10.5 (2) より $H \subset \text{Gal}(L/M)$ であり, このことと定理 10.3 を用いて

$$|H| \leq |\text{Gal}(L/M)| = |\text{Aut}(L/M)| = [L : M].$$

一方, 原始元定理 (定理 8.7) より $L = M(\alpha)$ をみたす $\alpha \in L$ がとれる. そこで, L 上の多項式

$$g_\alpha(X) = \prod_{\sigma \in H} (X - \sigma(\alpha))$$

を考えると, H が群であることから, 任意の $\sigma \in H$ に対して $g_\alpha^\sigma(X) = g_\alpha(X)$ であり, $g_\alpha(X)$ の係数は $L^H = M$ に属することがわかる; $g_\alpha(X) \in M[X]$. さらに $g_\alpha(\alpha) = 0$ なので

$$[L : M] \leq \deg g_\alpha(X) = |H|.$$

したがって, 上の不等式と合わせて $|H| = |\text{Gal}(L/M)|$ であり, よって $H = \text{Gal}(L/M)$ を得る. $\square$

定理 10.9 (ガロア理論の基本定理) 有限次ガロア拡大 L/K に対して, そのガロア群を G とする. $\mathcal{M}_{L/K}$ を L/K の中間体全体の集合, $\mathcal{H}_G$ を G の部分群全体の集合とする;

$$\mathcal{M}_{L/K} = \{M \mid M \text{ は } L/K \text{ の中間体}\}, \quad \mathcal{H}_G = \{H \mid H \text{ は } G \text{ の部分群}\}.$$

このとき, 二つの写像

$$\mathcal{M}_{L/K} \longrightarrow \mathcal{H}_G, \quad M \mapsto \text{Gal}(L/M)$$

$$\mathcal{H}_G \longrightarrow \mathcal{M}_{L/K}, \quad H \mapsto L^H$$

は互いに逆の全単射である.

証明 写像に名前を付けて, $\Phi: \mathcal{M}_{L/K} \rightarrow \mathcal{H}_G$ および $\Psi: \mathcal{H}_G \rightarrow \mathcal{M}_{L/K}$ とする. このとき, 任意の $M \in \mathcal{M}_{L/K}$, $H \in \mathcal{H}_G$ に対して

$$\Psi(\Phi(M)) = M, \quad \Phi(\Psi(H)) = H$$

を示せばよいが, これらはそれぞれ

$$L^{\text{Gal}(L/M)} = M, \quad \text{Gal}(L/L^H) = H$$

のことであり, 系 10.7, 定理 10.8 ですでに示されている. $\square$

定義 10.10 有限次ガロア拡大 L/K に対してそのガロア群を G とする;

$$G = \text{Gal}(L/K).$$

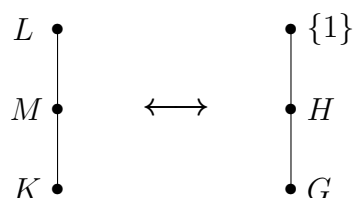
L/K の中間体 M と G の部分群 H の間に,

$$H = \text{Gal}(L/M)$$

あるいは, これと同値な

$$M = L^H$$

の関係があるとき, M と H は互いに対応するという. この対応を**ガロア対応**という. とくに K は G に対応し, L は $\text{id}_L (= L$ 上の恒等写像) だけを元にもつ群 (単位群) に対応する. 今後, 単位群を簡単に $\{1\}$ と略記することにする.



定義 10.11 L/K をガロア拡大, そのガロア群を G とする.

- (1) G が巡回群のとき, L/K を**巡回拡大**という.
- (2) G がアーベル群のとき, L/K を**アーベル拡大**という.
- (3) G が可解群のとき, L/K を**可解拡大**という.

例 10.12 (1) 素数次ガロア拡大は巡回拡大である. なぜなら, 素数位数の有限群は巡回群だから.

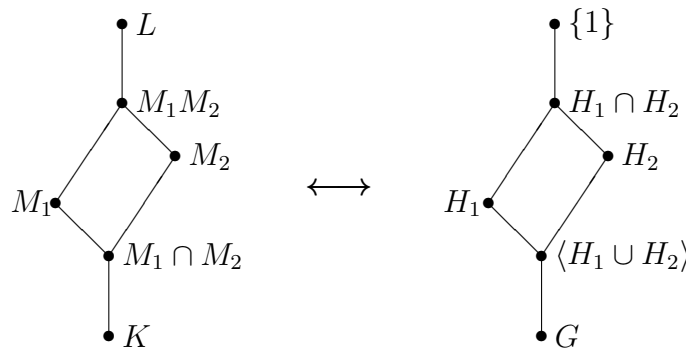
(2) 次数 5 以下のガロア拡大はアーベル拡大である. なぜなら, 位数が 5 以下の有限群はすべてアーベル群だから.

(3) 次数 60 未満のガロア拡大は可解拡大である. なぜなら, 位数が 60 未満の有限群はすべて可解群だから.

§11. ガロア対応

定理 11.1 L/K を有限次ガロア拡大とし, そのガロア群を G とする. いま, L/K の中間体 M_1, M_2 がそれぞれ G の部分群 H_1, H_2 に対応しているとする.

- (1) $M_1 \subset M_2$ と $H_1 \supset H_2$ は同値である.
- (2) 合成体 $M_1 M_2$ に対応する部分群は $H_1 \cap H_2$ である.
- (3) $M_1 \cap M_2$ に対応する部分群は $H_1 \cup H_2$ で生成される G の部分群である.



証明 (1) まず $M_1 \subset M_2$ を仮定する. $\sigma \in H_2 = \text{Gal}(L/M_2)$ を任意にとると,

$$\sigma(x) = x \quad (\forall x \in M_2) \quad \text{より} \quad \sigma(x) = x \quad (\forall x \in M_1), \quad \therefore \sigma \in \text{Gal}(L/M_1) = H_1$$

よって $H_2 \subset H_1$ を得る. 逆に $H_2 \subset H_1$ を仮定する. $x \in M_1 = L^{H_1}$ を任意にとると,

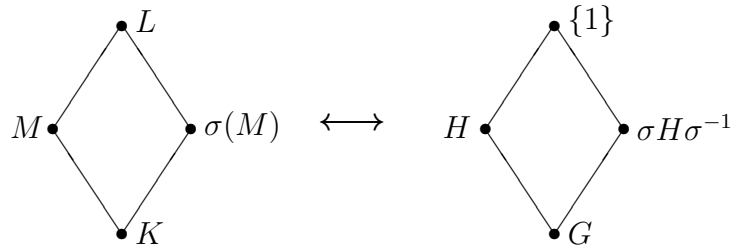
$$\sigma(x) = x \quad (\forall \sigma \in H_1) \quad \text{より} \quad \sigma(x) = x \quad (\forall \sigma \in H_2), \quad \therefore x \in L^{H_2} = M_2$$

よって $M_1 \subset M_2$ を得る.

(2) $M_1 M_2$ は M_1, M_2 を含む最小の体だから, (1) より, 対応する部分群は H_1, H_2 に含まれる最大の部分群 $H_1 \cap H_2$ である.

(3) $M_1 \cap M_2$ は M_1, M_2 に含まれる最大の体だから, (1) より, 対応する部分群は H_1, H_2 を含む最小の群であり, それは $H_1 \cup H_2$ で生成される G の部分群である. $\square$

定理 11.2 L/K を有限次ガロア拡大とし, そのガロア群を G とする. M を L/K の中間体, H を M に対応する G の部分群とする. また, $\sigma \in G$ とする. このとき, $\sigma(M)$ は L/K の中間体であり, 対応する G の部分群は $\sigma H \sigma^{-1}$ である.



証明 L/K は正規なので $\sigma(L) = L$, よって $K \subset \sigma(M) \subset L$ となるから $\sigma(M)$ は L/K の中間体である. また, $M = L^H$ より, $\alpha \in L$ に対して

$$\alpha \in M \iff \tau(\alpha) = \alpha \quad (\forall \tau \in H).$$

したがって,

$$\begin{aligned} \beta \in \sigma(M) &\iff \sigma^{-1}(\beta) \in M \iff \tau(\sigma^{-1}(\beta)) = \sigma^{-1}(\beta) \quad (\forall \tau \in H) \\ &\iff (\sigma\tau\sigma^{-1})(\beta) = \beta \quad (\forall \tau \in H) \iff \rho(\beta) = \beta \quad (\forall \rho \in \sigma H \sigma^{-1}) \end{aligned}$$

よって, 中間体 $\sigma(M)$ は部分群 $\sigma H \sigma^{-1}$ に対応する. $\square$

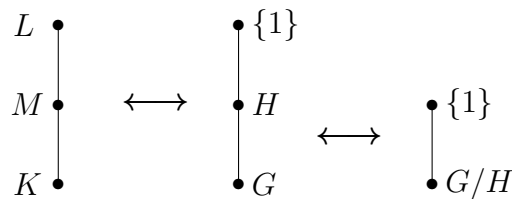
定理 11.3 L/K を有限次ガロア拡大とし, そのガロア群を G とする. M を L/K の中間体, H を M に対応する G の部分群とする. このとき, M/K がガロア拡大であるためには, H が G の正規部分群であることが必要十分である. またこのとき M/K のガロア群は G/H と同型である. 詳しくは, 制限写像

$$G = \text{Gal}(L/K) \longrightarrow \text{Gal}(M/K), \quad \sigma \mapsto \sigma|_M$$

から自然に同型

$$G/H = \text{Gal}(L/K) / \text{Gal}(L/M) \cong \text{Gal}(M/K)$$

が引き起こされる.



証明 L/K がガロア拡大なので, とくに M/K は分離的である. したがって, M/K がガロアであるためには, 正規であること, すなわち, 任意の $\sigma \in G$ に対して $\sigma(M) = M$ が成り立つことが必要十分である. 前定理を用いれば,

$$\sigma(M) = M \iff \sigma H \sigma^{-1} = H$$

であるが, 右の等式が任意の $\sigma \in G$ に対して成り立つことは, H が G の正規部分群であることを示している. 後半は, 準同型定理から導かれる. $\square$

系 11.4 L/K を有限次ガロア拡大, M をその中間体とする.

- (1) L/K がアーベル拡大ならば, L/M , M/K はともにアーベル拡大である.
- (2) L/K が巡回拡大ならば, L/M , M/K はともに巡回拡大である.
- (3) L/K が可解拡大ならば, L/M も可解拡大である. さらに M/K がガロア拡大 (すなわち $\text{Gal}(L/M)$ が $\text{Gal}(L/K)$ の正規部分群) ならば, M/K も可解拡大である.

証明 H を群 G の部分群とする. G がアーベル群ならば, H はアーベル群かつ G の正規部分群であって, 剰余群 G/H もアーベル群である. このことと前定理から (1) が得られる. また, アーベル群を巡回群としても同様のことがいえるから (2) も成り立つ. (3) は, G が可解群のとき H も可解群であり, さらに H が G の正規部分群ならば剰余群 G/H も可解群になることから導かれる. $\square$

定理 11.5 体の拡大 Ω/K の中間体 M_1, M_2 がともに K 上の有限次ガロア拡大体であるとする.

- (1) M_1M_2 および $M_1 \cap M_2$ はともに K 上ガロアである.
- (2) $\text{Gal}(M_1M_2/K)$ は直積 $\text{Gal}(M_1/K) \times \text{Gal}(M_2/K)$ の部分群に同型である.
- (3) $M_1 \cap M_2 = K$ ならば, 自然な同型

$$\text{Gal}(M_1M_2/K) \cong \text{Gal}(M_1/K) \times \text{Gal}(M_2/K)$$

が存在する.

証明 (1) は, 定理 8.13 から分離性が, 定理 9.14 から正規性が導かれることからわかる. (2) と (3) を示すために, 準同型写像

$$\Gamma : \text{Gal}(M_1M_2/K) \longrightarrow \text{Gal}(M_1/K) \times \text{Gal}(M_2/K), \quad \sigma \mapsto (\sigma|_{M_1}, \sigma|_{M_2})$$

を考える. いま, $\sigma \in \text{Ker } \Gamma$ ならば, $\sigma|_{M_1} = \text{id}_{M_1}$, $\sigma|_{M_2} = \text{id}_{M_2}$ だから, $\sigma|_{M_1M_2} = \text{id}_{M_1M_2}$, したがって $\text{Ker } \Gamma = \{\text{id}_{M_1M_2}\} = \{1\}$, すなわち Γ は単射であり (2) が得られた. 次に, $G = \text{Gal}(M_1M_2/K)$ とおき, M_1, M_2 に対応する G の部分群を H_1, H_2 とする. M_1, M_2 は K 上ガロアだから, 定理 11.3 より, H_1, H_2 は G の正規部分群で, 自然な同型

$$\text{Gal}(M_1/K) \cong G/H_1, \quad \text{Gal}(M_2/K) \cong G/H_2$$

が得られる. したがって, 上で定義した単射準同型写像 Γ は

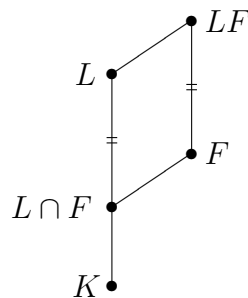
$$\Gamma : G \longrightarrow G/H_1 \times G/H_2$$

と書き換えることができる. ここで, H_1, H_2 の正規性から, $H_1 \cup H_2$ で生成される群は

$$H_1H_2 = \{h_1h_2 \mid h_1 \in H_1, h_2 \in H_2\}$$

と一致する. 一方, 定理 11.1 (2) より, $H_1 \cap H_2$ は $M_1 M_2$ に対応するから単位群である; $H_1 \cap H_2 = \{1\}$. よって, $H_1 H_2$ は直積群 $H_1 \times H_2$ と同型であり, さらに $M_1 \cap M_2$ に対応していることが定理 11.1 (3) からわかる. そこで, とくに $M_1 \cap M_2 = K$ の場合を考えると, $G = H_1 H_2 \cong H_1 \times H_2$ であって, G の位数と $G/H_1 \times G/H_2$ の位数は等しくなる. したがって, Γ は同型写像であり (3) が確かめられた. $\square$

定理 11.6 L/K が有限次ガロア拡大ならば, K 上の任意の拡大体 F に対して, LF/F はガロア拡大であり, そのガロア群は $\text{Gal}(L/(L \cap F))$ と同型である. とくに $\text{Gal}(LF/F)$ は $\text{Gal}(L/K)$ の部分群と同型である.



証明 L/K は分離拡大なので, L の任意の元は K 上分離的だから, F 上でも分離的, したがって命題 8.10 等を用いれば, LF/F は分離拡大である. 一方, 定理 9.15 より LF は F 上正規でもあるから, LF/F はガロア拡大である. 定理の後半を示すために, $M = L \cap F$ とおき, 準備として

$$[L : M] = [LF : F]$$

が成り立つことを確かめよう. L/K は有限次分離拡大だから, 原始元定理 (定理 8.7) より, $L = K(\alpha)$ となるような $\alpha \in L$ がとれる. $f(X)$ を α の K 上の最小多項式, $g(X)$ を α の F 上の最小多項式とする. $f(X) \in F[X]$ と考えれば, $f(X)$ は $g(X)$ で割り切れることがわかるから, $B \subset \text{Conj}(\alpha, K)$ が存在して,

$$g(X) = \prod_{\beta \in B} (X - \beta)$$

と書くことができる. ここで, L/K は正規であるから $B \subset \text{Conj}(\alpha, K) \subset L$, したがって, $g(X)$ の係数は $L \cap F = M$ に属する. さらに, $g(X)$ は F 上既約だから M 上でも既約, よって α の M 上の最小多項式となるから, $L = M(\alpha)$, $LF = F(\alpha)$ に注意すれば,

$$[L : M] = [M(\alpha) : M] = \deg g = [F(\alpha) : F] = [LF : F]$$

が得られた. さて, 準同型写像

$$\Delta : \text{Gal}(LF/F) \longrightarrow \text{Gal}(L/M), \quad \sigma \mapsto \sigma|_L$$

を考える ($M \subset F$ なので定義可能). いま, $\sigma \in \text{Ker } \Delta$ とすると $\sigma|_L = \text{id}_L$ だが, もともと σ は F 上の写像なので $\sigma|_F = \text{id}_F$, したがって $\sigma = \text{id}_{LF}$ であり, $\text{Ker } \Delta = \{\text{id}_{LF}\} = \{1\}$, よって Δ は単射である. さらに, 定理 10.3 と上で示した $[LF : F] = [L : M]$ から, $\text{Gal}(LF/F)$ と $\text{Gal}(L/M)$ の位数は等しいので, Δ は同型写像であることが導かれる. $\square$

§12. ガロア対応の例

例 12.1 ($\mathbf{Q}$ 上の 2 次拡大) $\mathbf{Q}$ 上の 2 次拡大体 L は $\mathbf{Q}$ 上ガロアであり, $\alpha \notin \mathbf{Q}$ をみたす任意の $\alpha \in L$ をとれば, $L = \mathbf{Q}(\alpha)$ である. α の $\mathbf{Q}$ 上の最小多項式を

$$f(X) = X^2 + bX + c \quad (b, c \in \mathbf{Q})$$

とすると, α は

$$\frac{-b + \sqrt{b^2 - 4c}}{2}, \quad \frac{-b - \sqrt{b^2 - 4c}}{2}$$

のどちらかであり, どちらであっても $L = \mathbf{Q}(\sqrt{b^2 - 4c})$ である. 有理数 $b^2 - 4c$ の分母を s とすれば, $s^2(b^2 - 4c) \in \mathbf{Z}$ かつ $L = \mathbf{Q}(\sqrt{s^2(b^2 - 4c)})$ でもあるから,

$$L = \mathbf{Q}(\sqrt{m}) \quad (m \in \mathbf{Z})$$

と表すことができる. ここで, もし m が平方数 l^2 で割れて $m = l^2 m'$ ならば $L = \mathbf{Q}(\sqrt{m'})$ とできる. そこで, はじめから m は平方因子をもたない, つまり

$$m = -1 \text{ または } \pm p_1 p_2 \dots p_r \quad (p_i \text{ は相異なる素数})$$

の形をした整数であるとしてよい (このような整数は square-free な整数と呼ばれる).

さて, $\sqrt{m}$ の $\mathbf{Q}$ 上の共役元は, $\sqrt{m}, -\sqrt{m}$ なので, 定理 6.11 より, 2 つの同型写像, すなわち $\text{Gal}(L/\mathbf{Q})$ の元で

$$\sqrt{m} \mapsto \sqrt{m}, \quad \sqrt{m} \mapsto -\sqrt{m}$$

をみたすものがそれぞれ存在する. 前者は恒等写像 id_L である. 後者を σ とすると, $\sigma(\sqrt{m}) = -\sqrt{m}$, より詳しく

$$\sigma : L \longrightarrow L, \quad a + b\sqrt{m} \mapsto a - b\sqrt{m} \quad (a, b \in \mathbf{Q})$$

となっている. ここで,

$$\sigma^2(a + b\sqrt{m}) = \sigma(a - b\sqrt{m}) = a - b(-\sqrt{m}) = a + b\sqrt{m}$$

より $\sigma^2 = \text{id}_L$ が成り立っている. 以上をまとめて, 2 次拡大 $L/\mathbf{Q}$ のガロア群として位数 2 の巡回群

$$\text{Gal}(L/\mathbf{Q}) = \langle \sigma \rangle = \{1, \sigma\}$$

が得られたことになる (ただし, $\text{id}_L = 1$ と略記した).

例 12.2 ($\mathbf{Q}$ 上の巡回拡大でない 4 次アーベル拡大) $\mathbf{Q}$ 上の拡大体

$$L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$$

を考える. $\alpha = \sqrt{2} + \sqrt{3}$ とおけば $L = \mathbf{Q}(\alpha)$ と書ける (例 2.4 参照). $\sqrt{2}, \sqrt{3}$ の $\mathbf{Q}$ 上の共役元は, それぞれ $\pm\sqrt{2}, \pm\sqrt{3}$ だから, α の $\mathbf{Q}$ 上の共役元は $\pm\sqrt{2} \pm \sqrt{3}$ (復号任意) のどれかである. 一方,

$$|\text{Conj}(\alpha, \mathbf{Q})| = [L : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = 4$$

より

$$\text{Conj}(\alpha, \mathbf{Q}) = \left\{ \sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3} \right\}$$

でなければならない. よって,

$$\text{Conj}(\alpha, \mathbf{Q}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\alpha) = L$$

がいえて, $L/\mathbf{Q}$ は正規拡大であることがわかる. したがって $L/\mathbf{Q}$ はガロア拡大である (多項式 $(X^2 - 2)(X^2 - 3)$ の $\mathbf{Q}$ 上の最小分解体であることからわかる). G をガロア群とする; $G = \text{Gal}(L/\mathbf{Q})$. $L/\mathbf{Q}$ の中間体

$$M_2 = \mathbf{Q}(\sqrt{2}), \quad M_3 = \mathbf{Q}(\sqrt{3})$$

に対応する G の部分群を H_2, H_3 とする. すなわち

$$H_2 = \text{Gal}(L/M_2), \quad H_3 = \text{Gal}(L/M_3),$$

または, これらと同値だが

$$M_2 = L^{H_2}, \quad M_3 = L^{H_3}$$

が成り立っている.

$$[L : M_2] = \frac{[L : \mathbf{Q}]}{[M_2 : \mathbf{Q}]} = \frac{4}{2} = 2, \quad [L : M_3] = \frac{[L : \mathbf{Q}]}{[M_3 : \mathbf{Q}]} = \frac{4}{2} = 2$$

より, H_2, H_3 はどちらも位数 2 の群, したがって巡回群である. そこで, それらの生成元をそれぞれ $\tau, \sigma \in G$ とする;

$$H_2 = \langle \tau \rangle, \quad H_3 = \langle \sigma \rangle.$$

このとき $\sqrt{2} \in M_2 = L^{H_2}$ より $\tau(\sqrt{2}) = \sqrt{2}$ が成り立つが, もし $\tau(\sqrt{3}) = \sqrt{3}$ でもあるとすると, L 全体が H_2 で不変になるから, $M_2 = L^{H_2} = L$ となって矛盾する. よって $\tau(\sqrt{3}) = -\sqrt{3}$ でなければならない. H_3 についても同様に考えて,

$$\begin{aligned} \sigma(\sqrt{2}) &= -\sqrt{2}, & \sigma(\sqrt{3}) &= \sqrt{3}, \\ \tau(\sqrt{2}) &= \sqrt{2}, & \tau(\sqrt{3}) &= -\sqrt{3}, \end{aligned}$$

したがって

$$\sigma(\alpha) = -\sqrt{2} + \sqrt{3}, \quad \tau(\alpha) = \sqrt{2} - \sqrt{3}$$

を得る. ここで, $\sigma \neq \tau$ はあきらかだが,

$$\begin{aligned} \sigma\tau(\alpha) &= \sigma(\tau(\alpha)) = \sigma(\sqrt{2} - \sqrt{3}) = -\sqrt{2} - \sqrt{3}, \\ \tau\sigma(\alpha) &= \tau(\sigma(\alpha)) = \tau(-\sqrt{2} + \sqrt{3}) = -\sqrt{2} - \sqrt{3} \end{aligned}$$

より, $\sigma\tau = \tau\sigma$ が成り立つ. したがって G はアーベル群である. また, $\sigma\tau$ は σ とも τ とも異なる G の元である. G の位数が体次数 $[L:\mathbf{Q}] = 4$ と一致することに注意すれば,

$$G = \{1, \sigma, \tau, \sigma\tau\} = \langle \sigma, \tau \rangle$$

と表され, 位数 4 のアーベル群であることがわかる. さらに G は位数 4 の元をもたないから巡回群ではない. 実際, G は位数 2 の巡回群の直積 $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ と同型である. (加法群 $\mathbf{Z}/2\mathbf{Z}$ は位数 2 の巡回群 (生成元は $\bar{1} = 1 + 2\mathbf{Z}$) であり, 同型写像

$$\varphi: G \longrightarrow \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

が

$$\varphi(\sigma) = (\bar{1}, \bar{0}), \quad \varphi(\tau) = (\bar{0}, \bar{1})$$

によって与えられる.)

例 12.3 ($\mathbf{Q}$ 上の 6 次非アーベル拡大) α を $X^3 - 5$ の実数根とし, ω を 1 の原始 3 乗根とする ($\omega = e^{\frac{2\pi i}{3}}$ と思ってよい). アイゼンシュタインの定理より, $X^3 - 5$ は $\mathbf{Q}$ 上既約, したがって α の $\mathbf{Q}$ 上の最小多項式である. さらに

$$X^3 - 5 = (X - \alpha)(X - \alpha\omega)(X - \alpha\omega^2)$$

より $\text{Conj}(\alpha, \mathbf{Q}) = \{\alpha, \alpha\omega, \alpha\omega^2\}$ であって, $X^3 - 5$ の $\mathbf{Q}$ 上の最小分解体 L は

$$L = \mathbf{Q}(\alpha, \alpha\omega, \alpha\omega^2) = \mathbf{Q}(\alpha, \omega)$$

で与えられる. $L/\mathbf{Q}$ のガロア群を $G = \text{Gal}(L/\mathbf{Q})$ とおく. いま, 2つの中間体

$$K = \mathbf{Q}(\alpha), \quad F = \mathbf{Q}(\omega)$$

について

$$[K:\mathbf{Q}] = 3, \quad [F:\mathbf{Q}] = [\mathbf{Q}(\sqrt{-3}):\mathbf{Q}] = 2$$

に注意する (後者は ω が $X^2 + X + 1$ の根, すなわち $(-1 \pm \sqrt{-3})/2$ であることからわかる). このことから, $[L:\mathbf{Q}] = 6$, したがって G の位数は 6 である. K, F に対応する G の部分群をそれぞれ H, N とする;

$$\begin{aligned} K &= L^H, & H &= \text{Gal}(L/K), \\ F &= L^N, & N &= \text{Gal}(L/F). \end{aligned}$$

このとき,

$$|H| = [L : K] = \frac{[L : \mathbf{Q}]}{[K : \mathbf{Q}]} = \frac{6}{3} = 2, \quad |N| = [L : F] = \frac{[L : \mathbf{Q}]}{[F : \mathbf{Q}]} = \frac{6}{2} = 3,$$

したがって, H は位数 2 の巡回群, N は位数 3 の巡回群である. それぞれの生成元を τ, σ とする;

$$H = \langle \tau \rangle = \{1, \tau\}, \quad N = \langle \sigma \rangle = \{1, \sigma, \sigma^2\}.$$

ここで, $\tau(\omega) = \bar{\omega} = \omega^2$ である. 実際, そうでないとすると $\tau(\omega) = \omega$ だが, $\alpha \in K$ より $\tau(\alpha) = \alpha$ でもあるから, $L = \mathbf{Q}(\alpha, \omega)$ が H の不変体となって矛盾する. 一方, $\sigma(\alpha) = \alpha$ とすると, 今度は L が N の不変体となって矛盾するから, $\sigma(\alpha) = \alpha\omega$ または $\alpha\omega^2$ である. 後者の場合,

$$\sigma^2(\alpha) = \sigma(\alpha\omega^2) = \sigma(\alpha)\sigma(\omega)^2 = \alpha\omega^2\omega^2 = \alpha\omega^4 = \alpha\omega$$

であって, かつ $N = \langle \sigma^2 \rangle$ でもあるから, σ^2 をあらためて σ とおくことによって

$$\begin{aligned} \sigma(\alpha) &= \alpha\omega, & \sigma(\omega) &= \omega, \\ \tau(\alpha) &= \alpha, & \tau(\omega) &= \omega^2 \end{aligned}$$

であるとしてよい. このとき,

$$\begin{aligned} \tau\sigma(\alpha) &= \tau(\alpha\omega) = \alpha\omega^2, & \sigma^2\tau(\alpha) &= \sigma^2(\alpha) = \alpha\omega^2, \\ \tau\sigma(\omega) &= \tau(\omega) = \omega^2, & \sigma^2\tau(\omega) &= \sigma^2(\omega^2) = \omega^2 \end{aligned}$$

より $\tau\sigma = \sigma^2\tau$ が示される. 次に, 定理 11.2 より,

$$\begin{aligned} \sigma(K) &= \mathbf{Q}(\sigma(\alpha)) = \mathbf{Q}(\alpha\omega) \text{ に対応する部分群は } \sigma H \sigma^{-1} = \langle \sigma\tau\sigma^{-1} \rangle, \\ \sigma^2(K) &= \mathbf{Q}(\sigma^2(\alpha)) = \mathbf{Q}(\alpha\omega^2) \text{ に対応する部分群は } \sigma^2 H \sigma^{-2} = \langle \sigma^2\tau\sigma^{-2} \rangle. \end{aligned}$$

さらに, $\tau^2 = \sigma^3 = 1$ と $\tau\sigma = \sigma^2\tau$ を使えば,

$$\sigma\tau\sigma^{-1} = \sigma^2\tau, \quad \sigma^2\tau\sigma^{-2} = \sigma\tau$$

および

$$G = \langle \sigma, \tau \rangle = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

が成り立つことがわかる. したがって, G は 3 次対称群 S_3 と同型な非アーベル群である. $(G : N) = 2$ より N は G の正規部分群であり, F は $\mathbf{Q}$ 上のガロア拡大体である. これは $[F : \mathbf{Q}] = 2$ からわかる (命題 9.3 参照). 一方, $\text{Conj}(\alpha, \mathbf{Q}) \not\subset K = \mathbf{Q}(\alpha)$ より, K は $\mathbf{Q}$ 上ガロアではなく, したがって, H は G の正規でない部分群である. このことは, $\sigma\tau\sigma^{-1} = \sigma^2\tau \notin H$ から直接確かめられる.

§13. クンマー拡大

以下において扱う体はすべて C の部分体とする. また, 自然数 n に対して, $\zeta_n \in C$ を 1 の原始 n 乗根とする. すなわち, $\zeta_n \in C^\times$ であって, その位数が n であるとする ($\zeta_n = e^{2\pi i/n}$ であるとしてよい).

定理 13.1 n を自然数とし, K が 1 の原始 n 乗根 ζ_n を含むとする. $a \in K^\times$ に対して, $\alpha^n = a$ をみたす α を任意にひとつとり $L = K(\alpha)$ とおく.

- (1) L は $X^n - a$ の K 上の最小分解体である.
- (2) $X^n - a$ が K 上既約 (すなわち α の K 上の最小多項式) ならば, L/K は n 次巡回拡大であり, $\sigma(\alpha) = \zeta_n \alpha$ をみたす K 上の自己同型 σ によって $\text{Gal}(L/K)$ が生成される;

$$\text{Gal}(L/K) = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}.$$

- (3) $\alpha^l \in K$ である最小の自然数 l が存在し, この l に対して $X^l - \alpha^l$ は K 上既約である. この場合, l は n の約数であり, L/K は l 次巡回拡大である.

証明 $\zeta = \zeta_n$ と略記する.

(1) $X^n - a$ のすべての根は $\alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^{n-1}\alpha$ であるが, $\zeta \in K$ より最小分解体は $K(\alpha) = L$ と一致する (例 9.12 参照).

(2) L/K がガロア拡大であることは (1) よりわかる. $G = \text{Gal}(L/K)$ とおく. $X^n - a$ は α の K 上の最小多項式なので, $|G| = [L : K] = n$ である. さらに, $\zeta\alpha$ は α と共役なので, 定理 6.11 より, $\sigma(\alpha) = \zeta\alpha$ をみたす $\sigma \in G$ が存在する. このとき,

$$\sigma^2(\alpha) = \sigma(\zeta\alpha) = \zeta\sigma(\alpha) = \zeta \cdot \zeta\alpha = \zeta^2\alpha,$$

同様にして, $\sigma^j(\alpha) = \zeta^j\alpha$ が任意の $j \in \mathbf{Z}$ について成り立ち, とくに $\sigma^n(\alpha) = \zeta^n\alpha = \alpha$ より $\sigma^n = \text{id}_L (= 1)$ となる. よって $|G| = n$ に注意すれば,

$$G = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\} = \langle \sigma \rangle$$

を得る. とくに L/K は n 次巡回拡大である.

(3) 最小の l が存在することはあきらかであり, さらに l が n の約数であることを示すのも難しくない. いま, $\xi = \zeta^{n/l}$ とおけば, ξ は 1 の原始 l 乗根であり, $X^l - \alpha^l$ のすべての根は $\xi^i\alpha$ ($i = 0, \dots, l-1$) である. よって, もし $X^l - \alpha^l$ が K 上可約ならば, その既約因子 $g(X) \in K[X]$ は, $1 \leq d < l$ と $0 \leq i_1 < \dots < i_d \leq l-1$ を用いて

$$g(X) = (X - \xi^{i_1}\alpha) \cdots (X - \xi^{i_d}\alpha)$$

と表され, とくに, その定数項は $g(0) = \pm \xi^{i_1 + \dots + i_d} \alpha^d \in K$ となる. 一方, $\xi = \zeta^{n/l} \in K$ だから $\alpha^d \in K$ でなければならないが, これは l の最小性に矛盾する. L/K が l 次巡回拡大であることは (2) を援用すればわかる. $\square$

定義 13.2 前定理のようにして与えられる体の拡大 L/K を自然数 n に関する巡回クンマー拡大という. n に関する巡回クンマー拡大の合成を, n に関するクンマー拡大という. とくに, 有限次拡大 L/K が n に関するクンマー拡大であるとは, K が 1 の原始 n 乗根 ζ_n を含み, 有限個の $a_1, \dots, a_r \in K^\times$ について $\alpha_j^n = a_j$ をみたす α_j によって $L = K(\alpha_1, \dots, \alpha_r)$ と表されることである. n に関する有限次クンマー拡大は, しばしば $L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$ とも表される.

補題 13.3 (デデキント) Γ を乗法群とし, $\sigma_1, \dots, \sigma_n$ を Γ から $C^\times$ への相異なる準同型写像とする. このとき, $(c_1, \dots, c_n) \neq (0, \dots, 0)$ をみたす任意の $c_1, \dots, c_n \in C$ に対して

$$\sum_{i=1}^n c_i \sigma_i(\gamma) = c_1 \sigma_1(\gamma) + \dots + c_n \sigma_n(\gamma) \neq 0$$

をみたす $\gamma \in \Gamma$ が存在する.

証明 対偶, すなわち, $c_1, \dots, c_n \in C$ とするとき,

$$\forall \gamma \in \Gamma \text{ に対して } \sum_{i=1}^n c_i \sigma_i(\gamma) = 0 \implies c_1 = \dots = c_n = 0$$

を n に関する数学的帰納法によって示す. $n = 1$ のときはあきらかである. そこで, $n > 1$ として, $n - 1$ のときは成り立つと仮定し, 任意の $\gamma \in \Gamma$ について

$$(\spadesuit) \quad c_1 \sigma_1(\gamma) + c_2 \sigma_2(\gamma) + \dots + c_n \sigma_n(\gamma) = 0$$

とする. いま, $\sigma_1 \neq \sigma_n$ だから, $\sigma_1(\beta) \neq \sigma_n(\beta)$ であるような $\beta \in \Gamma$ がとれる. 等式 $(\spadesuit)$ の γ の代わりに $\beta\gamma$ を用いれば,

$$c_1 \sigma_1(\beta) \sigma_1(\gamma) + c_2 \sigma_2(\beta) \sigma_2(\gamma) + \dots + c_n \sigma_n(\beta) \sigma_n(\gamma) = 0.$$

これと, $(\spadesuit)$ に $\sigma_n(\beta)$ をかけたもの

$$c_1 \sigma_n(\beta) \sigma_1(\gamma) + c_2 \sigma_n(\beta) \sigma_2(\gamma) + \dots + c_n \sigma_n(\beta) \sigma_n(\gamma) = 0$$

の差を取れば, 最後の項 $c_n \sigma_n(\beta) \sigma_n(\gamma)$ が消去されて,

$$c_1 (\sigma_1(\beta) - \sigma_n(\beta)) \sigma_1(\gamma) + \dots + c_n (\sigma_{n-1}(\beta) - \sigma_n(\beta)) \sigma_{n-1}(\gamma) = 0$$

が任意の $\gamma \in \Gamma$ について成り立つ. よって, 帰納法の仮定と β の取り方から $c_1 = 0$ を得る. したがって $(\spadesuit)$ は

$$c_2 \sigma_2(\gamma) + \dots + c_n \sigma_n(\gamma) = 0$$

と書き換えられ, 再び帰納法の仮定より $c_2 = \dots = c_n = 0$ を得る. □

定理 13.4 n を自然数とし、体 K は 1 の原始 n 乗根 ζ_n を含むとする。もし L/K が n 次巡回拡大ならば、ある $a \in K^\times$ が存在して、 $L = K(\sqrt[n]{a})$ と表される。すなわち、 K 上の n 次巡回拡大は巡回クンマー拡大である。

証明 $\zeta = \zeta_n$ と略記する。 σ を $\text{Gal}(L/K)$ の生成元とする；

$$\text{Gal}(L/K) = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}, \quad \sigma^n = 1.$$

いま、 $\Gamma = L^\times$ 、 $\sigma_i = \sigma^{i-1}$ および $c_i = \zeta^{-(i-1)}$ ($i = 1, \dots, n$) として前補題を適用すれば、

$$\sum_{i=0}^{n-1} \zeta^{-i} \sigma^i(\gamma) = \gamma + \zeta^{-1} \sigma(\gamma) + \dots + \zeta^{-(n-1)} \sigma^{n-1}(\gamma) \neq 0$$

をみたす $\gamma \in L^\times$ が存在する。この和を α とすると、 $0 \neq \alpha \in L$ であって

$$\sigma(\alpha) = \sum_{i=0}^{n-1} \zeta^{-i} \sigma^{i+1}(\gamma) = \zeta \sum_{i=0}^{n-1} \zeta^{-(i+1)} \sigma^{i+1}(\gamma) = \zeta \alpha$$

が成り立ち、両辺を n 乗して $\sigma(\alpha^n) = \alpha^n$ を得る。 σ は $\text{Gal}(L/K)$ の生成元だから、 α^n は $\text{Gal}(L/K)$ の不変体 K に属する。すなわち $\alpha^n \in K$ である。ここで、系 6.12 より

$$\{\sigma^j(\alpha) \mid j = 0, 1, 2, \dots, n-1\} \subset \text{Conj}(\alpha, K)$$

だが、左辺は $\{\alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^{n-1}\alpha\}$ に等しく、 $\alpha \neq 0$ より n 個の元からなるので、

$$n \leq |\text{Conj}(\alpha, K)| \leq [K(\alpha) : K] \leq [L : K] = n,$$

よって、不等号はすべて等号であり、とくに $L = K(\alpha)$ が得られる。 $\square$

定理 13.5 n を自然数とし、体 K は 1 の原始 n 乗根 ζ_n を含むとする。このとき、 L/K が n に関する有限次クンマー拡大であるためには、 L/K が有限次アーベル拡大でガロア群のすべての元の位数が n の約数であることが必要十分である。

証明は、定理 13.1 と定理 13.4 を組み合わせればよい。後で引用されないので、ここでは証明を省略する。

定義 13.6 L/K を体の拡大とする。

- (1) $X^n - a$ ($a \in K^\times$) の形の K 上の既約多項式の根 α によって $L = K(\alpha)$ と表すことができるとき、 L/K を **2 項拡大** という。
- (2) 体の有限列 $K_0, K_1, \dots, K_m$ で、

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{m-1} \subset K_m = L$$

$$K_i/K_{i-1} \text{ は 2 項拡大 } (i = 1, 2, \dots, m)$$

をみたすものが存在するとき、 L/K を **ベキ根拡大** という。

定義 13.7 L/K を代数拡大とする. 中間体の有限列 $K_0, K_1, \dots, K_m$ で,

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{m-1} \subset K_m = L$$

$$K_i/K_{i-1} \text{ はアーベル拡大 } (i = 1, 2, \dots, m)$$

をみたすものがとれるとき, L/K を**冪アーベル拡大**という.

注意 定理 13.1 において, $X^n - a$ が K 上既約ならば L/K は 2 項拡大かつ巡回拡大であるが, たとえ既約でなくても, (3) より, やはり 2 項拡大かつ巡回拡大になる. したがって, 一般に有限次クンマー拡大はベキ根拡大でありかつアーベル (したがって冪アーベル) 拡大である.

補題 13.8 n を 1 より大きい自然数とする. 体 K に対して $K(\zeta_n)/K$ は n より低い次数のアーベル拡大である.

証明 $\zeta = \zeta_n$ と略す. 任意の $\sigma \in \text{Aut}(\overline{K}/K)$ に対して $\sigma(\zeta)$ も 1 の原始 n 乗根だから, とくに $\sigma(\zeta) \in K(\zeta)$, よって $K(\zeta)/K$ はガロア拡大である. そのガロア群を G とおく. $\sigma \in G$ に対して, $\sigma(\zeta) = \zeta^j$ をみたす整数 j が n を法として一意的に定まる. また, 上述のように ζ^j は 1 の原始 n 乗根だから, j, n は互いに素である. よって, 写像

$$G \longrightarrow (\mathbf{Z}/n\mathbf{Z})^\times, \quad \sigma \mapsto \bar{j}$$

が定義できることがわかる. この写像が単射準同型であることを確かめるのは難しくない. よって, G は $(\mathbf{Z}/n\mathbf{Z})^\times$ の部分群に同型, とくにアーベル群であり,

$$[K(\zeta) : K] = |G| \leq |(\mathbf{Z}/n\mathbf{Z})^\times| = \varphi(n) < n.$$

ここで, φ はオイラー関数である. □

定理 13.9 ベキ根拡大 L/K に対して, 有限次冪アーベル拡大 L'/K で $L \subset L'$ をみたすものが存在する.

証明 L/K の中間体の列

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{m-1} \subset K_m = L$$

$$K_i/K_{i-1} \text{ は 2 項拡大 } (i = 1, 2, \dots, m)$$

が存在する. ここで, K_{i-1} 上の既約多項式 $X^{n_i} - a_i$ の根 α_i によって $K_i = K_{i-1}(\alpha_i)$ と表すことができる. そこで, n を $n_1, \dots, n_m$ の公倍数とし, ζ を 1 の原始 n 乗根として, $M_i = K_i(\zeta)$ ($i = 0, 1, \dots, m$) とおく. $i = 1, \dots, m$ に対して, M_{i-1} は 1 の原始 n_i 乗根をもっているから, $M_i = M_{i-1}(\alpha_i)$ は M_{i-1} 上の巡回クンマー拡大, したがって巡回拡大である. 一方, 補題 13.8 より, $M_0 = K(\zeta)$ は K 上のアーベル拡大なので, $M_m = L(\zeta)$ は K 上有限次冪アーベル拡大である. □

上の定理において, ベキ根拡大と有限次冪アーベル拡大の役割を入れ替えても正しいことが次節で示される (定理 14.2). すなわち, これらの拡大は“本質的”に同等であると考えることができる.

§14. 可解性

この節でも、前節同様、扱う体はすべて C の部分体とする.

補題 14.1 有限次アーベル拡大 L/K に対して、中間体の列 $K_1, \dots, K_r$ で、

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{r-1} \subset K_r = L$$

$$K_i/K_{i-1} \text{ は巡回拡大 } (i = 1, 2, \dots, r)$$

をみたすものが存在する.

証明 L/K の次数に関する数学的帰納法によって示す. $[L:K] = 1$ すなわち $L = K$ のときは自明だから, $[L:K] > 1$ として $G = \text{Gal}(L/K)$ とおく. $1 \neq \sigma \in G$ をひとつとって $H = \langle \sigma \rangle$ とし, 対応する L/K の中間体を M とすると, $\text{Gal}(L/M) = H$ は巡回群だから L/M は巡回拡大である. 一方, 系 11.4 (2) より M/K はアーベル拡大である. しかも, $H \neq \{1\}$ より $[M:K] < [L:K]$ だから, 帰納法の仮定より各拡大が巡回拡大である中間体の列 $K = K_0 \subset K_1 \subset \cdots \subset K_s = M$ がとれる. これと $M \subset L$ を合わせれば証明が完了する. $\square$

定理 14.2 有限次冪アーベル拡大 L/K に対して、ベキ根拡大 L'/K で $L \subset L'$ をみたすものが存在する.

証明 L/K の次数に関する数学的帰納法による. $[L:K] = 1$ のときはあきらかだから, $n = [L:K] > 1$ とする. いま, L/K は冪アーベル拡大だから, 前補題を何度か適用することにより, 中間体の列 $K_1, \dots, K_r$ で、

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{r-1} \subset K_r = L$$

$$K_i/K_{i-1} \text{ は巡回拡大 } (i = 1, 2, \dots, r)$$

をみたすものが存在する. 各 $i = 1, 2, \dots, r$ について $n_i = [K_i:K_{i-1}]$ とすると, それらの最小公倍数 m は n の約数である. ζ を 1 の原始 m 乗根とすれば, 補題 13.8 より, $K(\zeta)/K$ はアーベル拡大で次数は m 未満, したがって n 未満である. よって, 帰納法の仮定が適用でき, ベキ根拡大 M/K で $K(\zeta) \subset M$ をみたすものがとれる. $M_i = K_i M$ とおけば, $M_i = K_i M_{i-1}$ だから, 定理 11.6 より M_i/M_{i-1} はガロア拡大でそのガロア群 $\text{Gal}(M_i/M_{i-1})$ は $\text{Gal}(K_i/K_{i-1})$ の部分群と同型である. よって M_i/M_{i-1} は巡回拡大でその次数 m_i は n_i の約数であり m の約数でもある. したがって M_{i-1} は 1 の原始 m_i 乗根を含み, 定理 13.4 が適用できて, M_i/M_{i-1} は巡回クンマー拡大, よって 2 項拡大となる. このことから M_r/M_0 すなわち LM/M はベキ根拡大であることがわかり, M/K がベキ根拡大であることと合わせて定理が証明された. $\square$

定義 14.3 α を K 上代数的な元とする. $\alpha \in L$ をみたすベキ根拡大 L/K が存在するとき, α は K 上ベキ根によって表されるという.

定義 14.4 $f(X) \in K[X]$ とする. $f(X)$ の任意の根が K 上ベキ根によって表されるとき, 方程式 $f(X) = 0$ は K 上ベキ根によって解ける, または K 上ベキ根によって可解であるという.

例 14.5 体 K 上のすべての2次方程式は K 上ベキ根によって解ける. なぜなら, すべての2次式 $f(X) = X^2 + bX + c$ は

$$f(X) = \left(X + \frac{b}{2}\right)^2 - \left(\frac{b^2}{4} - c\right)$$

と変形できるからである.

例 14.6 体 K に対して, 1 のベキ根は K 上ベキ根によって表される. この事実は当たり前のように思えるが, $n > 1$ のとき2項式 $X^n - 1$ は K 上既約ではないので, 定義から直接には導けない. 証明は, 補題 13.8 および定理 14.2 を用いて与えられる (定理 14.7). なお, $n = 3, 5$ の場合は以下を参照せよ.

(1) 1 の原始3乗根 $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$ について, $L = \mathbf{Q}(\omega)$ とおく. $\omega^3 = 1$ かつ $\omega \neq 1$ より $\omega^2 + \omega + 1 = 0$ だから,

$$\omega = \frac{-1 \pm \sqrt{-3}}{2},$$

よって, $L = \mathbf{Q}(\sqrt{-3})$ であって $L/\mathbf{Q}$ は2項拡大, したがって, ω は $\mathbf{Q}$ 上ベキ根によって表される.

(2) ζ を 1 の原始5乗根とすると, $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$. これを ζ^2 で割って

$$\zeta^2 + \zeta + 1 + \frac{1}{\zeta} + \frac{1}{\zeta^2} = 0.$$

そこで, $\eta = \zeta + \frac{1}{\zeta}$ とおけば, $\eta^2 = \zeta^2 + \frac{1}{\zeta^2} + 2$ だから

$$\eta^2 + \eta - 1 = 0, \quad \therefore \eta = \frac{-1 \pm \sqrt{5}}{2}.$$

一方, $\zeta^2 - \eta\zeta + 1 = 0$ より

$$\zeta = \frac{\eta \pm \sqrt{\eta^2 - 4}}{2}$$

であるから, 2項拡大の列

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(\sqrt{5}, \sqrt{\eta^2 - 4})$$

が得られ, $\zeta \in \mathbf{Q}(\sqrt{5}, \sqrt{\eta^2 - 4})$. このことから, ζ は $\mathbf{Q}$ 上ベキ根によって表されることがわかる.

定理 14.7 (ガウス) n を自然数とし, ζ を 1 の原始 n 乗根とすると, 任意の体 K に対して ζ は K 上ベキ根で表される.

証明 補題 13.8 から $K(\zeta)/K$ はアーベル拡大であり, 定理 14.2 より, ベキ根拡大 L/K で $K(\zeta) \subset L$ をみたすものがとれる. とくに ζ は K 上ベキ根で表される. $\square$

いま, L/K を有限次ガロア拡大としそのガロア群を G とする. さらに L/K が冪アーベル拡大でもあるとすると, 中間体の列

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{m-1} \subset K_m = L$$

$$K_i/K_{i-1} \text{ はアーベル拡大 } (i = 1, 2, \dots, m)$$

に対応して, G の部分群の列

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m = \{1\}$$

$$G_i \text{ は } G_{i-1} \text{ の正規部分群で } G_{i-1}/G_i \text{ はアーベル群 } (i = 1, 2, \dots, m)$$

がとれる. このような部分群列が存在するとき, G は**可解群**とよばれるのであった. すなわち, 冪アーベルであるガロア拡大とは可解拡大のことに他ならない. よって, 定理 14.2 から次の定理を得る.

定理 14.8 有限次可解拡大 L/K に対して, ベキ根拡大 L'/K で $L \subset L'$ をみたすものが存在する.

一方で, 与えられた有限次冪アーベル拡大 L/K に対して, 原始元定理により $L = K(\alpha)$ と表したとき, L/K の正規閉包 (いまの場合, L を含む K 上の最小のガロア拡大体) L' は, 命題 9.17 より

$$L' = K(\text{Conj}(\alpha, K)) = \prod_{\beta \in \text{Conj}(\alpha, K)} K(\beta)$$

で与えられる. 定理 11.5 (2) を使えば, 数学的帰納法により, K 上の有限個の冪アーベル拡大体の合成体が冪アーベル拡大体となることが示せるから, L'/K は可解拡大である. したがって, 定理 13.9 から次の定理が帰結される.

定理 14.9 ベキ根拡大 L/K に対して, 有限次可解拡大 L'/K で $L \subset L'$ をみたすものが存在する.

以上で, この講義の最終目標である定理の証明の準備がすべて整った.

定理 14.10 (ガロア) $f(X) \in K[X]$ の K 上の最小分解体を L とする. 方程式 $f(X) = 0$ が K 上ベキ根によって解けるための必要十分条件は L/K が可解拡大であることである.

証明 L/K が可解拡大ならば, 定理 14.8 から, $f(X)$ のすべての根が K 上ベキ根によって表されることが直ちにわかる. 逆を示すために, $f(X)$ の任意の根 α が K 上ベキ根によって表されるとする. このとき, ベキ根拡大 L_α/K が存在して $\alpha \in L_\alpha$ をみたす. 定理 14.9 を用いれば, $L_\alpha \subset L'_\alpha$ をみたす有限次可解拡大 L'_α/K がとれる. そこで, $f(X)$ のすべての根 α にわたる合成体

$$\tilde{L} = \prod_{\alpha} L'_\alpha$$

を考える. いま, K 上のガロア拡大の合成はガロアであり K 上の有限個の冪アーベル拡大の合成も冪アーベルだから, $\tilde{L}$ は K 上可解拡大である. 最後に, $\tilde{L}/K$ の中間体である L は K 上ガロアだから, 系 11.4 (3) より, L/K は可解拡大であることがわかる. $\square$

定理 14.11 $f(X)$ を $\mathbb{Q}$ 上の 5 次既約多項式とする. $f(X)$ が実根をちょうど 3 個もつならば, 方程式 $f(X) = 0$ は $\mathbb{Q}$ 上ベキ根によって解けない.

証明 $f(X)$ の $\mathbb{Q}$ 上の最小分解体を L とし, $L/\mathbb{Q}$ のガロア群を G とする. G は $f(X)$ の 5 つの根の置換群と考えられるので, 5 次対称群 S_5 の部分群とみなすことができる. ここで, $f(X)$ のひとつの根 α に対して $\mathbb{Q}(\alpha)$ は $L/\mathbb{Q}$ の中間体だから, G の位数は $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ で割り切れる. したがって G は位数 5 の元をもつ. このことから, 置換群としての G は長さ 5 の巡回置換をもつことが示せる. 一方, 複素共役を対応させる写像 $C \rightarrow C, z \mapsto \bar{z}$ を L に制限したものを $\tau \in G$ とおけば, L がちょうど 2 個の虚根をもつことから, τ は互換とみなすことができる. 互換および長さ 5 の巡回置換をもつ S_5 の部分群は S_5 と一致することは, 群論の一般論から証明できる (§15 補遺の補題 15.3 参照). したがって $G = S_5$ であるが, S_5 は可解群ではないので $L/\mathbb{Q}$ は可解拡大ではない. よって, 定理 14.10 より $f(X) = 0$ は $\mathbb{Q}$ 上ベキ根によって解けない. $\square$

上の定理の条件をみたす 5 次既約多項式として, たとえば $f(X) = X^5 - 5X - 1$ があげられる. 実際, 既約であることは $f(X+1)$ にアイゼンシュタインの定理を素数 5 に関して適用すればよい. 実根の個数が 3 つであることは微積分学の簡単な計算で確かめられる. よって, $f(X) = 0$ は $\mathbb{Q}$ 上ベキ根によって解けない.

定理 14.12 (アーベル) $\mathbb{Q}$ 上の 5 次方程式には, 四則とベキ根によって表される「解の公式」は存在しない.

証明 もし存在すれば, 有理数係数のどんな 5 次方程式の解も $\mathbb{Q}$ 上ベキ根で表されることになる. しかし, 上に述べたように $\mathbb{Q}$ 上ベキ根によって解けない 5 次方程式が存在するから矛盾である. $\square$

§15. 補遺

次の命題は、例 7.9 の最後の方、および、補題 8.5 の証明で使われている。

命題 15.1 体 K の乗法群 $K^\times$ の有限部分群は巡回群である。

証明 A を $K^\times$ の有限部分群とし、 A に属する位数最大の元 a をひとつとる。 a で生成される巡回群 $\langle a \rangle$ が A に一致すること確かめればよい。そこで、 $\langle a \rangle$ に属さない $b \in A$ が存在するとして矛盾を導く。 a, b の位数をそれぞれ m, n とする。いま、素数 p について

$$m = p^e m', \quad n = p^f n', \quad \text{ただし, } p \text{ は } m' n' \text{ を割り切らない}$$

とすると、 $a^{p^e}, b^{n'}$ の位数はそれぞれ m', p^f でこれらは互いに素だから、積 $a^{p^e} b^{n'}$ の位数は $p^f m'$ である。よって、 m の最大性より

$$p^f m' \leq m = p^e m', \quad \therefore f \leq e$$

となる。これが任意の素数 p について成り立つから、 m は n の倍数であることがわかる。 b の位数は n であったから、とくに b は多項式 $X^m - 1$ の根である。一方、 a の位数は m であったから、 $m+1$ 個の元

$$b, 1, a, a^2, \dots, a^{m-1} \in K^\times$$

はすべて多項式 $X^m - 1$ の根となるが、体 K において m 次式は m 個より多くの根をもたないはずだから矛盾である。 $\square$

次に、分離拡大に関する重要な命題 8.10 および定理 8.11 の証明において鍵となった補題の証明を与える。

補題 15.2 (補題 8.9 再掲) 体 K 上代数的である α, β が、 $\beta \in K(\alpha)$ をみたすならば、

$$|\text{Conj}(\alpha, K)| = |\text{Conj}(\alpha, K(\beta))| |\text{Conj}(\beta, K)|$$

が成り立つ。

証明 ふたつの写像

$$F : \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K) \longrightarrow \text{Conj}(\alpha, K)$$

$$G : \text{Conj}(\alpha, K) \longrightarrow \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K)$$

を定義し、それらが互いに逆写像であること、すなわち $F \circ G$ と $G \circ F$ がそれぞれ恒等写像であることを確かめればよい。そのために、まず $\delta \in \text{Conj}(\beta, K)$ に対して、定理 6.11

より, $\sigma(\beta) = \delta$ をみたす $\sigma \in \text{Aut}(\overline{K}/K)$ が存在することに注意する. このような σ を各 δ に対して 1 つずつ選んで固定し σ_δ と表すことにする;

$$\sigma_\delta \in \text{Aut}(\overline{K}/K), \quad \sigma_\delta(\beta) = \delta \in \text{Conj}(\beta, K).$$

(1) F の定義: $\gamma \in \text{Conj}(\alpha, K(\beta))$ ならば, γ と α は $K(\beta)$ 上共役であるから, K 上でももちろん共役, よって $\text{Conj}(\gamma, K) = \text{Conj}(\alpha, K)$ が成り立つ. さらに, $\delta \in \text{Conj}(\beta, K)$ に対して, $\sigma_\delta \in \text{Aut}(\overline{K}/K)$ が上のようにして定まり, $\sigma_\delta(\gamma) \in \text{Conj}(\gamma, K) = \text{Conj}(\alpha, K)$ であるから,

$$F : \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K) \longrightarrow \text{Conj}(\alpha, K), \quad (\gamma, \delta) \mapsto \sigma_\delta(\gamma)$$

が定義できる.

(2) G の定義: $\varepsilon \in \text{Conj}(\alpha, K)$ に対して定理 6.11 を適用すれば, $\tau(\alpha) = \varepsilon$ をみたす $\tau \in \text{Aut}(\overline{K}/K)$ が存在する. このとき $\tau(\beta)$ の値は τ の選び方によらず ε のみから定まる (実際, $\tau' \in \text{Aut}(\overline{K}/K)$ も $\tau'(\alpha) = \varepsilon$ をみたすならば, $(\tau^{-1} \circ \tau')(\alpha) = \alpha$ だから, $\tau^{-1} \circ \tau'$ は $K(\alpha)$ 上で恒等写像であり, さらに $\beta \in K(\alpha)$ だから, $(\tau^{-1} \circ \tau')(\beta) = \beta$ すなわち $\tau'(\beta) = \tau(\beta)$ を得る). また, $\tau(\beta) \in \text{Conj}(\beta, K)$ に注意すれば, $\sigma_{\tau(\beta)} \in \text{Aut}(\overline{K}/K)$ が ε のみから定まるともわかる. ここで, 上の σ_δ の定義から $\sigma_{\tau(\beta)}(\beta) = \tau(\beta)$, すなわち $\sigma_{\tau(\beta)}^{-1}(\tau(\beta)) = \beta$ だから, $\sigma_{\tau(\beta)}^{-1} \circ \tau \in \text{Aut}(\overline{K}/K(\beta))$. よって

$$\sigma_{\tau(\beta)}^{-1}(\varepsilon) = \left(\sigma_{\tau(\beta)}^{-1} \circ \tau \right) (\alpha) \in \text{Conj}(\alpha, K(\beta))$$

であり

$$G : \text{Conj}(\alpha, K) \longrightarrow \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K), \quad \varepsilon \mapsto \left(\sigma_{\tau(\beta)}^{-1}(\varepsilon), \tau(\beta) \right)$$

が定義される.

(3) $F \circ G$ が恒等写像であることの証明: $\varepsilon \in \text{Conj}(\alpha, K)$ に対して, $\tau(\alpha) = \varepsilon$ をみたす $\tau \in \text{Aut}(\overline{K}/K)$ をとると

$$F(G(\varepsilon)) = F\left(\sigma_{\tau(\beta)}^{-1}(\varepsilon), \tau(\beta)\right) = \sigma_{\tau(\beta)}\left(\sigma_{\tau(\beta)}^{-1}(\varepsilon)\right) = \varepsilon$$

よって $F \circ G$ は $\text{Conj}(\alpha, K)$ 上の恒等写像である.

(4) $G \circ F$ が恒等写像であることの証明: $(\gamma, \delta) \in \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K)$ に対して, $F(\gamma, \delta) = \sigma_\delta(\gamma)$ である. いま γ に対して, $\rho(\alpha) = \gamma$ をみたす $\rho \in \text{Aut}(\overline{K}/K(\beta))$ が存在する. この ρ を用いると, $\sigma_\delta(\rho(\alpha)) = \sigma_\delta(\gamma)$ より, $\tau(\alpha) = \sigma_\delta(\gamma)$ をみたす $\tau \in \text{Aut}(\overline{K}/K)$ として $\tau = \sigma_\delta \circ \rho$ をとることができる. さらに $\rho(\beta) = \beta$ なので, $\tau(\beta) = \sigma_\delta(\rho(\beta)) = \sigma_\delta(\beta) = \delta$ となるから

$$G(F(\gamma, \delta)) = G(\sigma_\delta(\gamma)) = \left(\sigma_{\tau(\beta)}^{-1}(\sigma_\delta(\gamma)), \tau(\beta) \right) = \left(\sigma_\delta^{-1}(\sigma_\delta(\gamma)), \delta \right) = (\gamma, \delta)$$

よって $G \circ F$ は $\text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K)$ 上の恒等写像である. □

最後に, 対称群の生成系に関する補題を紹介する. $\mathbb{Q}$ 上ベキ根によって解けない 5 次方程式の実例を与えた定理 14.11 の証明に, この補題が使われている.

補題 15.3 n を 3 以上の自然数とする. n 次対称群 S_n の部分群 G が以下のいずれかを満たすならば, $G = S_n$ が成り立つ.

- (1) G は互換 $(1\ 2), (1\ 3), \dots, (1\ n)$ を含む.
- (2) G は長さ 2, $n-1$, n の巡回置換を少なくともひとつずつ含む.
- (3) n は素数で, G は互換および長さ n の巡回置換を少なくともひとつずつ含む.

証明 (1) $2 \leq i < j \leq n$ なる任意の i, j について,

$$(1\ i)(1\ j)(1\ i) = (i\ j)$$

が成り立つから, G はすべての互換を含む. S_n の任意の元は互換の積で表すことができるから, $G = S_n$ を得る.

(2) G は $(i\ j), (2\ 3 \cdots n)$ を含むとしてよい. さらに G は長さ n の巡回置換 σ を含むが, $\sigma = (1 \cdots i \cdots)$ と書いたとき, $1, i$ の間隔が d であれば $\sigma^d(1) = i$ となる. いま, $\sigma^d(k) = j$ とすると, $k \neq 1$ かつ $\sigma^{-d}(i\ j)\sigma^d = (1\ k)$ であり, さらに

$$(2\ 3 \cdots n)(1\ k)(2\ 3 \cdots n)^{-1} = \begin{cases} (1\ k+1) & (k = 2, \dots, n-1), \\ (1\ 2) & (k = n) \end{cases}$$

と計算され, (1) に帰着する.

(3) G は $(i\ j), \sigma = (1\ 2 \cdots n)$ を含むとしてよい. このとき, $\sigma^{j-i}(i) = j$ が成り立つが, n は素数だから σ^{j-i} も長さ n の巡回置換であり, $\sigma^{j-i} = (i\ j \cdots)$ なる形に書かれる. これと $(i\ j)$ との積 $(i\ j)(i\ j \cdots) = (j \cdots)$ は長さ $n-1$ の巡回置換 (下線の部分が同じ) だから (2) に帰着する. □

索引

あ

アーベル拡大	40
アーベルの定理	56

え

延長	17
----	----

か

可解拡大	40
拡大体	5
ガロア拡大	37
ガロア群	37
ガロア対応	40
ガロアの定理	56
ガロア理論の基本定理	39

き

基本対称式	3
共役	23
共役元	23

く

クロネッカーの定理	18
クンマー拡大	50

け

原始元	5
原始元定理	31

こ

合成体	16
-----	----

さ

最小多項式	11
最小分解体	33

し

自己同型群	23
自己同型写像	23
次数	6
重根	29
シュタイニッツの定理	22
巡回拡大	40
巡回クンマー拡大	50
上の準同型写像	17

せ

正規	33
正規拡大	33
正規閉包	36
制限	17

た

対称式	3
対称式の基本定理	4
代数拡大	13
代数学の基本定理	21
代数的	9, 13
代数的閉体	21
代数的閉包	21
単根	29
単純拡大	5

ち

中間体	5
超越拡大	13
超越的	9, 13

つ

ツォルンの補題	22, 23
---------	--------

て

デデキントの定理	50
添加した体	5

と

同型	17
同型写像	17

に

2 項拡大	51
-------	----

ひ

標数	25
----	----

ふ

フェルマーの定理	27
不変体	37
フロベニウス写像	28
分離拡大	31
分離多項式	29
分離的	29–31

へ

ベキ根拡大	51
ベキ根によって	54

む

無限次拡大	6
-------	---

ゆ

有限次拡大	6
有限体	25

る

冪アーベル拡大	52
---------	----