

ガロア理論入門（体と群と方程式）

大阿久 俊則

目 次

1	体とその拡大	2
2	有理数係数多項式の既約性	9
3	分解体	13
4	有限次拡大と体準同型	16
5	群についての復習	17
6	ガロア拡大とガロア群	20
7	ガロア理論の基本定理（ガロア対応）	24
8	1 の n 乗根	32
9	2 項方程式と巡回拡大	34
10	3 次方程式のガロア群と根の公式	37
11	可解群	41
12	方程式のべき根による可解性	45
13	5 次方程式のガロア群の例と根の公式の不可能性	46
14	円分体	47

はじめに

代数方程式（2 次方程式，3 次方程式，...）の解（正式には根 (root) という）を求めることは 1800 年頃までは代数学の最も重要な問題と考えられていた．2 次方程式の根の公式

は少なくとも 830 年頃にはアラビア人に知られていた (代数学を表す algebra はアラビア語に由来する) . 3 次方程式の根の公式は 1530 年頃イタリアのタルタリア (Tartaglia) やカルダノ (Cardano) らによって発見され, 更にそのすぐ後にはカルダノの弟子フェラーリ (Ferrari) によって 4 次方程式の根の公式も見出された .

その後約 300 年に渡って 5 次方程式の根の公式を求めることが代数学の中心的な問題となったが誰も見出すことができなかった . そして, 群の考え方を取り入れたラグランジュ (Lagrange, 1736–1813) , ルフィニ (Ruffini, 1765–1822) らの研究を経て最終的に 1826 年にノルウェーのアーベル (Abel, 1802–1829) によって 5 次以上の方程式の根の公式は不可能である (存在しない) ことが証明された . 彼に因んで可換群はアーベル群とも呼ばれる .

一方, ガウス (Gauss, 1777–1855) は 1799 年に代数方程式の根が複素数の範囲で必ず存在すること (代数学の基本定理) を証明した . ただし根が存在しても, それを具体的に表せるかどうかは別問題である .

5 次以上の代数方程式の根の公式は存在しないが, 個々の方程式の根を (四則演算と根号を用いて) 具体的に表せる場合もある . フランスのガロア (Évariste Galois, 1811–1832) は 1832 年の遺稿の中で, 与えられた方程式の根が四則演算と根号を用いて表示できるための必要十分条件を, 方程式に付随した群 (Galois 群と呼ばれる) の性質を用いて与えた . そのために体とその拡大の概念を導入した . これがガロア理論の原型である . 体の拡大と群との対応を記述することがガロア理論の本質であり, 代数方程式の可解性の問題は (歴史的には重要であったが現在では) その応用の 1 つに過ぎない .

この講義では, ガロア理論の基本的な部分を群, 環, 体などの現代の代数学の言葉を用いて解説する . 体としては複素数体の部分体 (古典的な場合と呼ばれる) を主に扱う .

なお, 「環と加群の基礎」の内容, 特に単項イデアル整域 (PID) についての事項は既知として自由に用いるので, 必要に応じて参照してください .

1 体とその拡大

まず環と体の定義を復習しておこう .

定義 1.1 集合 R が環 (ring) であるとは, 2 つの 2 項演算 (加法と乗法)

$$R \times R \ni (a, b) \mapsto a + b \in R, \quad R \times R \ni (a, b) \mapsto ab \in R,$$

が定義され次の性質を満たすことである .

- (1) 任意の $a, b, c \in R$ に対して $(a + b) + c = a + (b + c)$ が成立する (加法の結合法則)
- (2) 任意の $a, b \in R$ に対して $a + b = b + a$ が成立する (加法の交換法則)
- (3) R の元 0_R が存在して, 任意の $a \in R$ に対して $a + 0_R = a$ が成立する (0_R を加法についての単位元といい, 通常は単に 0 で表す.)
- (4) R の任意の元 a に対してある $b \in R$ が存在して $a + b = 0$ が成立する . このとき $b = -a$ と表し a の加法についての逆元という .

- (5) 任意の $a, b, c \in R$ に対して $(ab)c = a(bc)$ が成立する (乗法の結合法則)
- (6) R のある元 1_R が存在して, 任意の $a \in R$ に対して $a1_R = 1_Ra = a$ が成立する (1_R を乗法についての単位元といい, 通常は 1 で表す.)
- (7) 任意の $a, b, c \in R$ に対して $a(b+c) = ab+ac$, $(a+b)c = ac+bc$ が成立する (分配法則)

$a, b \in R$ に対して, $a - b = a + (-b)$ と定義する. さらに次の条件が成立するとき R は可換環 (commutative ring) であるという.

- (8) 任意の $a, b \in R$ に対して $ab = ba$ が成立する (乗法の交換法則)

定義 1.2 K が 0 以外の元を含む可換環であって, 0 と異なる K の任意の元 a に対して $ab = ba = 1$ を満たす $b \in K$ が存在するとき, K を体 (field) という. このとき $b = a^{-1}$ と表し, a の乗法についての逆元という.

たとえば $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である. これらをそれぞれ有理数体, 実数体, 複素数体という. K と L を体とする. 写像 $\sigma: K \rightarrow L$ が環としての準同型であるとき, すなわち

- (1) $\sigma(a+b) = \sigma(a) + \sigma(b)$ ($\forall a, b \in K$)
- (2) $\sigma(ab) = \sigma(a)\sigma(b)$ ($\forall a, b \in K$)
- (3) $\sigma(1_K) = 1_L$ ($1_K, 1_L$ はそれぞれ K, L における乗法の単位元)

を満たすとき, σ を体準同型という. もし $ab = 1$ であれば $\sigma(a)\sigma(b) = \sigma(ab) = 1$ であるから, $\sigma(a^{-1}) = \sigma(a)^{-1}$ が成立する.

体準同型 σ の核 $\text{Ker } \sigma = \{a \in K \mid \sigma(a) = 0\}$ は K のイデアルであるが, 体 K のイデアルは $\{0\}$ または K のいずれかであり, $\sigma(1) = 1$ より σ は 0 写像ではないから, $\text{Ker } \sigma = \{0\}$, 従って σ は単射 (1 対 1 写像) である. 体準同型が全単射であるとき体同型という. 特に体 K から K への体同型のことを K の自己同型という.

例 1.1 複素数 $z = x + iy$ ($x, y \in \mathbb{R}$) に対して共役複素数 $\bar{z} = x - iy$ を対応させる写像 $\sigma: \mathbb{C} \ni z \mapsto \bar{z} \in \mathbb{C}$ は複素数体 $\mathbb{C}$ の自己同型であり, $\mathbb{R}$ の元を固定する. すなわち, 任意の $x \in \mathbb{R}$ に対して $\sigma(x) = \bar{x} = x$ である. また, $\sigma^2 = \sigma \circ \sigma$ (写像の合成) は $\mathbb{C}$ から $\mathbb{C}$ への恒等写像 $\text{id}_{\mathbb{C}}$ となる.

定義 1.3 (多項式環) K を体, $x_1, \dots, x_n$ を不定元 (文字) とするとき, 非負整数 $m_1, \dots, m_n$ に対して $x_1^{m_1} \cdots x_n^{m_n}$ という式を単項式という. 有限個の単項式の K 係数の 1 次結合で表される式を K 係数の多項式という. K 係数の多項式の全体を $K[x_1, \dots, x_n]$ と表す. これは自然な加法と乗法により可換環となり, K 上の n 変数多項式環とよばれる.

体上の 1 変数多項式環は単項イデアル整域 (PID) である (「環と加群の基礎」参照).

定義 1.4 L が体であって, L の部分集合 K が L と同じ演算によって体であるとき, K を L の部分体 (subfield), L を K の拡大体 (extension field) という. このとき簡単のため $L \supset K$ は体の拡大であるという. $L \supset K$ を L/K と略記することもある.

たとえば, $\mathbb{Q}$ と $\mathbb{R}$ は $\mathbb{C}$ の部分体, $\mathbb{C}$ は $\mathbb{R}$ と $\mathbb{Q}$ の拡大体, $\mathbb{R}$ は $\mathbb{Q}$ の拡大体である.

補題 1.1 L を体とする. ある (添字) 集合 Λ があって, 任意の $\lambda \in \Lambda$ について L の部分体 K_λ が対応しているとすると, これらの共通部分 $K := \bigcap_{\lambda \in \Lambda} K_\lambda$ は L の部分体である.

証明: $a, b \in K$ とすると, 任意の $\lambda \in \Lambda$ について $a, b \in K_\lambda$ であり K_λ は体であるから, $a+b \in K_\lambda, ab \in K_\lambda$ である. さらに $a \neq 0$ ならば $a^{-1} \in K_\lambda$ である. 以上により $a+b, ab$ は K に属し, $a \neq 0$ ならば a^{-1} も K に属する. $\square$

L を体 K の拡大体として, $\alpha_1, \dots, \alpha_n \in L$ とする. このとき K と $\alpha_1, \dots, \alpha_n$ を含むような L の部分体のうち最小のものが存在する. 実際 K と $\alpha_1, \dots, \alpha_n$ を含むような L のすべての部分体を考え, それらの共通部分をとればよい. この体を $K(\alpha_1, \dots, \alpha_n)$ と表して, K に $\alpha_1, \dots, \alpha_n$ を添加した体, または K 上 $\alpha_1, \dots, \alpha_n$ で生成される体という. 特に $n=1$ のとき, $K(\alpha_1)$ を K の単純拡大 (体) という.

補題 1.2 $L \supset K$ を体の拡大, $\alpha_1, \dots, \alpha_n \in L$ とすると,

$$K(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f, g \in K[x_1, \dots, x_n], g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$$

が成立する. ここで $K[x_1, \dots, x_n]$ は不定元 $x_1, \dots, x_n$ についての K 係数多項式の全体を表す.

証明: 右辺の集合を K' とおくと, K' が体であることは容易に確かめられる. $f(x_1, \dots, x_n) = x_i, g(x_1, \dots, x_n) = 1$ とすれば $\alpha_i \in K'$ であることもわかるから, $K(\alpha_1, \dots, \alpha_n) \subset K'$ である. 一方, $f(\alpha_1, \dots, \alpha_n)/g(\alpha_1, \dots, \alpha_n)$ は K のいくつかの元 (多項式 f, g の係数) と $\alpha_1, \dots, \alpha_n$ から加減乗除を何回か行ったものであるから, $K(\alpha_1, \dots, \alpha_n)$ に属さなければならない. よって $K(\alpha_1, \dots, \alpha_n) = K'$ である. $\square$

例 1.2 体の拡大 $\mathbb{C} \supset \mathbb{Q}$ において $\mathbb{Q}(\sqrt{2})$ を考えよう. 上の補題によって

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{f(\sqrt{2})}{g(\sqrt{2})} \mid f, g \in \mathbb{Q}[x], g(\sqrt{2}) \neq 0 \right\}$$

であるが, $(\sqrt{2})^2 = 2 \in \mathbb{Q}$ であるから, f と g は 1 次式であるとしてよい. すなわち

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a\sqrt{2} + b}{c\sqrt{2} + d} \mid a, b, c, d \in \mathbb{Q}, c\sqrt{2} + d \neq 0 \right\}$$

となる. さらに $c = d = 0$ でなければ $\pm c\sqrt{2} + d \neq 0$ であり, 分母を有理化すると

$$\frac{1}{c\sqrt{2} + d} = \frac{-c\sqrt{2} + d}{-2c^2 + d^2}$$

となるから、結局

$$\mathbb{Q}(\sqrt{2}) = \{a\sqrt{2} + b \mid a, b \in \mathbb{Q}\}$$

であることがわかる。 $\sqrt{2}$ は有理数ではないから、 $a\sqrt{2} + b$ という表示は一意的である。

補題 1.3 $L \supset K$ を体の拡大、 $\alpha, \beta \in L$ とすると、 $K(\alpha, \beta) = K(\alpha)(\beta) = K(\beta)(\alpha)$ が成立する。

証明: $K(\alpha)(\beta)$ は α, β と K を含む体であるから、 $K(\alpha)(\beta) \supset K(\alpha, \beta)$ が成立する。一方、 $K(\alpha, \beta)$ は $K(\alpha)$ と β を含むから、 $K(\alpha, \beta) \supset K(\alpha)(\beta)$ が成立する。従って $K(\alpha)(\beta) = K(\alpha, \beta)$ である。□

$L \supset K$ を体の拡大とすると、 L を K 上のベクトル空間とみなすことができる。実際、 L における加法は L の体としての加法であり、 $\alpha \in L$ と $c \in K$ に対して $c\alpha$ (L における積) を α のスカラー (c) 倍とみなせばよい。これがベクトル空間の公理をみたすことは容易に確認できる。このとき L の K 上のベクトル空間としての次元を $[L : K]$ で表して、 L の K 上の (または拡大 $L \supset K$ の) (拡大) 次数と呼ぶ。次数は自然数または無限大である。特に次数が有限である (無限大でない) とき、 $L \supset K$ は有限次拡大 (finite extension) であるという。 $[L : K] = n$ であるとき、 $L \supset K$ は n 次拡大であるともいう。

例 1.3 $\mathbb{C}$ の任意の元 α は実数 a, b によって $a + bi = a1 + bi$ と一通りに表されるから、 1 と i は $\mathbb{C}$ を $\mathbb{R}$ 上のベクトル空間とみなしたときの基底である。従って $[\mathbb{C} : \mathbb{R}] = 2$ である。

$L \supset K$ を体の拡大とする。 $\alpha \in L$ に対して

$$I(\alpha) := \{f \in K[x] \mid f(\alpha) = 0\}$$

は 1 変数多項式環 $K[x]$ のイデアルであることが容易にわかる。このイデアルが $\{0\}$ でないとき、すなわち $I(\alpha)$ が 0 でない多項式を含むとき、 α は K 上代数的 (algebraic) であるという。 $K[x]$ は単項イデアル整域 (PID) であるから、このとき $I(\alpha)$ の元のうちモニック (最高次の係数が 1) で次数最小のもの $f_\alpha(x)$ がただ 1 つ存在して、 $I(\alpha)$ は $f_\alpha(x)$ の倍元の全体となる。この $f_\alpha(x)$ のことを α の K 上の最小多項式 (minimal polynomial) という。

命題 1.1 (1) α の K 上の最小多項式 f_α は $K[x]$ の既約元である。

(2) 逆に $f(x)$ が $K[x]$ の既約元かつモニックであり $f(\alpha) = 0$ を満たせば $f(x) = f_\alpha(x)$ である。

証明: (1) $f_\alpha = gh$ を満たす 1 次以上の $g, h \in K[x]$ が存在したとすると、 $0 = f_\alpha(\alpha) = g(\alpha)h(\alpha)$ より $g(\alpha) = 0$ または $h(\alpha) = 0$ が成立するから g または h は $I(\alpha)$ に属しその次数は $\deg f_\alpha$ より小だから f_α の定義に反する。

(2) $K[x]$ におけるモニックな既約多項式 $f(x)$ が $f(\alpha) = 0$ を満たせば $f \in I(\alpha) = K[x]f_\alpha$ であるから f は f_α で割り切れるが、 f は既約だから f は f_α の定数倍でなければならない。 f も f_α もモニックであるから $f = f_\alpha$ でなければならない。□

なお, $I(\alpha) = \{0\}$ のときは α は K 上超越的 (transcendental) であるという (この講義では超越的な場合は扱わない.)

例 1.4 虚数単位 $i = \sqrt{-1} \in \mathbb{C}$ の $\mathbb{R}$ 上の最小多項式は $f(x) = x^2 + 1$ である. 実際, i の $\mathbb{R}$ 上の最小多項式を $g(x)$ とすると, $f(i) = 0$ より $f(x)$ は $g(x)$ の倍元だから $f(x) = g(x)$ でなければ $g(x)$ は 1 次式であり $g(x) = ax + b$ ($a, b \in \mathbb{R}$) と書ける. このとき $0 = g(i) = b + ia$ であるが, 複素数の定義より, これは $a = b = 0$ を意味するから $g(x) = 0$ となり矛盾である. 以上により $f(x) = g(x)$ が示された.

例 1.5 $\sqrt{2} \in \mathbb{R}$ の $\mathbb{Q}$ 上の最小多項式は $f(x) = x^2 - 2$ である. 実際, $\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式を $g(x)$ とすると, $f(\sqrt{2}) = 0$ より $f(x)$ は $g(x)$ の倍元だから $f(x) = g(x)$ でなければ $g(x)$ は 1 次式であり $g(x) = ax + b$ ($a, b \in \mathbb{Q}$) と書ける. このとき $0 = g(\sqrt{2}) = a\sqrt{2} + b$ であるが, もし $a \neq 0$ ならば $\sqrt{2} = -b/a$ となり $\sqrt{2}$ が無理数であることに反する. 従って $a = b = 0$ すなわち $g(x) = 0$ となり矛盾である. 以上により $f(x) = g(x)$ が示された.

定理 1.1 $L \supset K$ を体の拡大として, $\alpha \in L$ は K 上代数的であると仮定する. α の K 上の最小多項式を f_α とする. $\deg f_\alpha = n$ とすると, $1, \alpha, \dots, \alpha^{n-1}$ が $K(\alpha)$ の K ベクトル空間としての基底となる. 特に $K(\alpha) = K[\alpha] := \{f(\alpha) \mid f(x) \in K[x]\}$ であり,

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

が成立する. さらに, $K(\alpha)$ は剰余環 (体) $K[x]/K[x]f_\alpha$ に体として同型である.

証明: $K[x]$ から L への写像 φ を

$$\varphi(f) = f(\alpha) \quad (f = f(x) \in K[x])$$

により定義する. φ が環準同型であり, $\text{Ker } \varphi = I(\alpha)$ であることは容易にわかる. また φ の像は

$$K[\alpha] := \{f(\alpha) \mid f(x) \in K[x]\}$$

である. 環準同型定理により, 環同型

$$\bar{\varphi} : K[x]/I(\alpha) \xrightarrow{\sim} K[\alpha]$$

であって, 任意の $f \in K[x]$ について $\bar{\varphi}([f]) = \varphi(f)$ を満たすものが存在する. ここで $[f]$ は f の $K[x]/I(\alpha)$ における同値類を表す. $I(\alpha) = K[x]f_\alpha$ であり, f_α は $K[x]$ の素元であるから, $I(\alpha)$ は単項イデアル整域 $K[x]$ の $\{0\}$ と異なる素イデアル, 従って極大イデアルである. よって $K[x]/I(\alpha)$ は体であるから, それと環として同型な $K[\alpha]$ も体となる. $g \in K[x]$ が $g(\alpha) \neq 0$ を満たせば, $g(\alpha) \in K[\alpha] \setminus \{0\}$ より $1/g(\alpha) \in K(\alpha)$ も $K[\alpha]$ の元となる. 従って $K(\alpha) = K[\alpha]$ である.

任意の $f \in K[x]$ に対して $q, r \in K[x]$ が存在して

$$f = qf_\alpha + r, \quad \deg r < n = \deg f_\alpha$$

となる. $r(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ ($c_k \in K$) とすると,

$$f(\alpha) = q(\alpha)f_\alpha(\alpha) + r(\alpha) = r(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

より, $1, \alpha, \dots, \alpha^{n-1}$ は K ベクトル空間 $K(\alpha)$ を張る. 一方,

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0, \quad c_0, c_1, \dots, c_{n-1} \in K$$

とすると, $r(x) := c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ は $I(\alpha)$ に属し $\deg r < n = \deg f_\alpha$ であるから, 多項式として $r = 0$, すなわち $c_0 = c_1 = \cdots = c_{n-1} = 0$ でなければならない. $\square$

例 1.6 $\alpha = \sqrt[3]{2} \in \mathbb{C}$ とおく. (α は 3 乗すると 2 になるような実数である.) $f(x) = x^3 - 2$ は $\mathbb{Q}[x]$ において既約であることを示そう. $f(x)$ が既約でないと仮定すると $f(x)$ はある 1 次式 $x - c$ ($c \in \mathbb{Q}$) で割り切れる. 互いに素な整数 p, q によって $c = p/q$ とおくと, $f(p/q) = 0$ より $p^3 = 2q^3$ を得る. よって p は偶数でなければならないから $p = 2k$ ($k \in \mathbb{Z}$) とおける. このとき $8k^3 = 2q^3$ すなわち $4k^3 = q^3$ より q も偶数となるが, これは矛盾である. 以上により $f(x)$ は $\mathbb{Q}$ 上既約であることが示された. 従って $f(x)$ は α の最小多項式であるから, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 3$ であり, $\mathbb{Q}$ 上のベクトル空間として

$$\mathbb{Q}(\alpha) = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\alpha^2 = \{c_0 + c_1\alpha + c_2\alpha^2 \mid c_0, c_1, c_2 \in \mathbb{Q}\}$$

が成り立ち, $1, \alpha, \alpha^2$ は $\mathbb{Q}$ 上 1 次独立である.

命題 1.2 $L \supset K$ が体の有限次拡大であれば L の任意の元 α は K 上代数的であり, α の K 上の最小多項式の次数は $[L : K]$ 以下である.

証明: $\alpha \in L$ とする. $n = [L : K]$ とすると, $1, \alpha, \dots, \alpha^n$ は K 上 1 次従属であるから, 0 でない高々 n 次の多項式 $f(x) \in K[x]$ があって, $f(\alpha) = 0$ となる. よって α は K 上代数的である. α の最小多項式は $f(x)$ を割り切るから, その次数は $\deg f \leq n$ 以下である. $\square$

定理 1.2 $L \supset K$ と $K \supset F$ が共に体の有限次拡大であれば, $L \supset F$ も有限次拡大であり,

$$[L : F] = [L : K][K : F]$$

証明: L の K ベクトル空間としての基底を $\alpha_1, \dots, \alpha_n$, K の F ベクトル空間としての基底を $\beta_1, \dots, \beta_m$ とするとき, $\alpha_j\beta_k$ ($1 \leq j \leq n, 1 \leq k \leq m$) が L の F ベクトル空間としての基底であることを示そう. α を L の任意の元とすると, K の元 $c_1, \dots, c_n$ が存在して $\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$ と表される. また c_j ($1 \leq j \leq n$) に対してある $c_{j1}, \dots, c_{jm} \in F$ が存在して

$$c_j = c_{j1}\beta_1 + \cdots + c_{jm}\beta_m$$

と表される. 以上をまとめると

$$\alpha = \sum_{j=1}^n \sum_{k=1}^m c_{jk} \alpha_j \beta_k$$

となるから $\alpha_j \beta_k$ ($1 \leq j \leq n, 1 \leq k \leq m$) は L を張る．ここで，

$$\sum_{j=1}^n \sum_{k=1}^m c_{jk} \alpha_j \beta_k = \sum_{j=1}^n \left(\sum_{k=1}^m c_{jk} \beta_k \right) \alpha_j = 0$$

と仮定すると， $\alpha_1, \dots, \alpha_n$ が K 上 1 次独立であることから

$$\sum_{k=1}^m c_{jk} \beta_k = 0 \quad (1 \leq j \leq n)$$

となる． $\beta_1, \dots, \beta_m$ が F 上 1 次独立であることから $c_{jk} = 0$ を得る．よって $\alpha_j \beta_k$ ($1 \leq j \leq n, 1 \leq k \leq m$) は F 上 1 次独立である．以上により $[L : F] = nm = [L : K][K : F]$ を得る．
□

系 1.1 $L \supset K$ が体の拡大であり， $\alpha_1, \dots, \alpha_n \in L$ がすべて K 上代数的ならば $K(\alpha_1, \dots, \alpha_n) \supset K$ は有限次拡大である．

証明: α_k は K 上代数的だから $K(\alpha_1, \dots, \alpha_{k-1})$ 上でも代数的である．従って有限次拡大の列

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset K(\alpha_1, \dots, \alpha_n)$$

に上の定理を適用すればよい．□

定理 1.3 体の拡大 $L \supset K$ について，次の 2 条件は同値である．

- (1) $L \supset K$ は有限次拡大である．
- (2) K 上代数的な有限個の L の元 $\alpha_1, \dots, \alpha_n$ があって， $L = K(\alpha_1, \dots, \alpha_n)$ が成立する．

証明: (1) $\Rightarrow$ (2): $L \supset K$ は有限次拡大であると仮定して (2) が成立することを $[L : K]$ についての帰納法で示す． $[L : K] = 1$ のときは $L = K$ であるから (2) は $n = 0$ で成立する． $[L : K] > 1$ として， $\alpha \in L \setminus K$ を任意にとる．このとき $L \supset K(\alpha) \not\subseteq K$ であり，定理 1.2 より

$$[L : K(\alpha)] = [L : K] / [K(\alpha) : K] < [L : K]$$

であるから，帰納法の仮定により $K(\alpha)$ 上代数的な L の元 $\beta_1, \dots, \beta_m$ が存在して

$$L = K(\alpha)(\beta_1, \dots, \beta_m) = K(\alpha, \beta_1, \dots, \beta_m)$$

となる．命題 1.2 より $\beta_1, \dots, \beta_m$ は K 上代数的であるから (2) が示された．

(2) $\Rightarrow$ (1) は系 1.1 より従う．□

例 1.7 体の拡大 $\mathbb{C} \supset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \supset \mathbb{Q}$ を考える. $\alpha := \sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式は $f(x) = x^2 - 2$ であり, $\sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式は $g(x) = x^2 - 3$ である.

$\sqrt{3}$ は $\mathbb{Q}(\sqrt{2})$ に属さないことを示そう. もし $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ とすると, ある有理数 a, b が存在して $\sqrt{3} = a\sqrt{2} + b$ と表される. 両辺を 2 乗して整理すると

$$2ab\sqrt{2} = 3 - 2a^2 - b^2$$

となり $\sqrt{2}$ は有理数でないから, $ab = 0$ でなければならない. $a = 0$ とすると, $\sqrt{3} = \pm b \in \mathbb{Q}$ となって矛盾である. $b = 0$ とすると, $3 = 2a^2$ となる. $a = \frac{p}{q}$ ($p, q \in \mathbb{Z}$ は互いに素) と表すと, $2p^2 = 3q^2$ となる. これから q は偶数であることがわかるので, $q = 2k$ ($k \in \mathbb{Z}$) とおくと, $p^2 = 6k^2$, 従って p も偶数でなければならない. これは p と q が互いに素であることに反する. 以上により, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ であることが示された.

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ より $\sqrt{3}$ の $\mathbb{Q}(\sqrt{2})$ 上の最小多項式の次数は 2 以上である. これと $g(\sqrt{3}) = 0$ から $\sqrt{3}$ の $\mathbb{Q}(\sqrt{2})$ 上の最小多項式も $g(x) = x^2 - 3$ である. 以上により

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

である. 定理 1.2 の証明より, $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ が $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の $\mathbb{Q}$ 上の基底となる.

例 1.8 $i = \sqrt{-1}$ として, 拡大体 $\mathbb{Q}(i, \sqrt{2})$ の $\mathbb{Q}$ 上の拡大次数を求めよう. $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\sqrt{2})(i)$ と定理 1.2 より

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})]$$

が成立する. $f(x) = x^2 + 1$ とおくと $f(i) = 0$ であるが, $f(x) = 0$ は実根を持たないことと $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ より $f(x)$ は i の $\mathbb{Q}(\sqrt{2})$ 上の最小多項式でもある. よって $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2$ であるから, $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$ を得る. 定理 1.2 の証明より $1, \sqrt{2}, i, \sqrt{2}i$ が $\mathbb{Q}(i, \sqrt{2})$ の $\mathbb{Q}$ 上の基底である.

問題 1.1 次の各々の複素数 α の $\mathbb{Q}$ 上の最小多項式と拡大次数 $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ を求めよ.

$$(1) \quad \alpha = \sqrt{5} + 1 \qquad (2) \quad \alpha = \frac{-1 + \sqrt{-3}}{2} \qquad (3) \quad \alpha = \sqrt[3]{4}$$

問題 1.2 $i = \sqrt{-1}$ とするとき, 拡大体 $\mathbb{Q}(i, \sqrt[3]{2})$ の $\mathbb{Q}$ 上の拡大次数 $[\mathbb{Q}(i, \sqrt[3]{2}) : \mathbb{Q}]$ を求めよ.

問題 1.3 $i = \sqrt{-1}$ とするとき, 拡大体 $\mathbb{Q}(i\sqrt{2}, \sqrt{3})$ の $\mathbb{Q}$ 上の拡大次数 $[\mathbb{Q}(i\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ を求めよ. また $\mathbb{Q}(i\sqrt{2}, \sqrt{3})$ の $\mathbb{Q}$ ベクトル空間としての基底を一組求めよ.

2 有理数係数多項式の既約性

一般に K を体とするとき, K 係数多項式 $f \in K[x]$ が K 上既約であるとは, f が $K[x]$ の既約元 (= 素元) であることと定義する. 前節でも見たように, f が K 上既約である

かどうかを判定することは重要な問題であるが、一般には困難である。ここでは $K = \mathbb{Q}$ の場合に、既約性の判定法 (十分条件) を 2 つ与える。

$f \in \mathbb{Q}[x]$ とする。 f にある自然数 ($\mathbb{Q}[x]$ の単元) を掛けることにより、 $f \in \mathbb{Z}[x]$ としても一般性を失わないことに注意する。 f の次数 $\deg f$ が 1 であれば f は既約である。 $\deg f$ が 2 または 3 のときは、 f が既約でないことと、 f がある 1 次多項式で割り切れることとが同値である。さらにこれは、剰余定理により $f(a) = 0$ を満たす有理数 $a \in \mathbb{Q}$ が存在することと同値である。これは以下のように有限の手続きで判定できる。

定義 2.1 0 でない整数係数多項式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad (n \geq 0, a_i \in \mathbb{Z}, a_n \neq 0)$$

に対して、 f の係数 $a_0, a_1, \dots, a_n$ のうち 0 と異なるもの全体の最大公約数を f の内容 (content) といい $\text{cont}(f)$ で表す。 f が原始多項式 (primitive polynomial) であるとは、 f の内容 $\text{cont}(f)$ が 1 となることである。

たとえば $f(x) = 3x^2 - 6x + 4$ のとき $\text{cont}(f) = 1$ であるから、 f は原始多項式である。 $f(x) = 3x^2 - 6x + 9$ のとき $\text{cont}(f) = 3$ であるから、 f は原始多項式ではないが、 $f(x) = 3(x^2 - 2x + 3)$ となり $x^2 - 2x + 3$ は原始多項式である。

補題 2.1 (Gauss の補題) $f, g \in \mathbb{Z}[x]$ とする。 f と g が原始多項式ならば fg も原始多項式である。

証明:

$$\begin{aligned} f &= a_n x^n + \cdots + a_1 x + a_0 \quad (a_n \neq 0), & g &= b_m x^m + \cdots + b_1 x + b_0 \quad (b_m \neq 0) \\ fg &= c_{n+m} x^{n+m} + \cdots + c_1 x + c_0 \end{aligned}$$

とする。 fg が原始多項式でないと仮定すると、ある素数 p があって $c_0, c_1, \dots, c_{n+m}$ はすべて p の倍数となる。 f と g は原始多項式だから、 f と g 各々の係数で p の倍元ではないものが存在する。すなわち、非負整数 k と l が存在して、

$$p \nmid a_k \text{ かつ } (j > k \Rightarrow p \mid a_j), \quad p \nmid b_l \text{ かつ } (j > l \Rightarrow p \mid b_j),$$

が成立する。このとき fg の x^{k+l} の係数 c_{k+l} は

$$c_{k+l} = a_k b_l + a_{k+1} b_{l-1} + a_{k+2} b_{l-2} + \cdots + a_{k-1} b_{l+1} + a_{k-2} b_{l+2} + \cdots$$

となり、右辺の第 1 項以外はすべて p の倍数である。一方 a_k も b_l も p の倍数ではなく、 p は素数だから $a_k b_l$ は p の倍数ではない。よって c_{k+l} は p の倍数ではない。これは矛盾であるから fg は原始多項式である。□

命題 2.1 $g \in \mathbb{Z}[x]$ を原始多項式とする。 $f \in \mathbb{Z}[x]$ が $\mathbb{Q}[x]$ において g の倍元であれば f は $\mathbb{Z}[x]$ においても g の倍元である。

証明: $f(x)$ が $\mathbb{Q}[x]$ において $g(x)$ の倍元であれば, $f(x) = g(x)h(x)$ を満たす $h(x) \in \mathbb{Q}[x]$ が存在する. 原始多項式 $h_0(x) \in \mathbb{Z}[x]$ と $a, b \in \mathbb{Z}$ ($b \neq 0$) が存在して $h(x) = (a/b)h_0(x)$ と表せる. このとき $\mathbb{Z}[x]$ において $bf(x) = ah_0(x)g(x)$ が成立する. Gauss の補題により $h_0(x)g(x)$ は原始多項式であるから, 両辺の内容を比較して $b \operatorname{cont}(f) = a$ を得る. 特に a は b の倍数であるから $c := a/b$ は整数である. 従って $h(x) = ch_0(x)$ は $\mathbb{Z}[x]$ に属するから $f(x) = ch_0(x)g(x)$ は $\mathbb{Z}[x]$ においても $g(x)$ の倍元である. $\square$

命題 2.2 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ ($a_i \in \mathbb{Z}$, $n \in \mathbb{N}$, $a_n \neq 0$, $a_0 \neq 0$) を $\mathbb{Z}[x]$ の原始多項式とする. もし有理数 r が $f(r) = 0$ を満たせば, $r = a/b$ かつ $a|a_0$, $b|a_n$ を満たす整数 a, b が存在する (特に $a_n = 1$ ならば $r \in \mathbb{Z}$ かつ r は a_0 の約数である.)

証明: 互いに素な整数 a, b によって $r = a/b$ と表すと, $b(x - r) = bx - a$ は $\mathbb{Q}[x]$ において $f(x)$ の約元であり, $\mathbb{Z}[x]$ における原始多項式でもあるから, 上の命題によって $bx - a$ は $\mathbb{Z}[x]$ において $f(x)$ の約元である. 従ってある $n-1$ 次多項式 $q(x) \in \mathbb{Z}[x]$ が存在して $f(x) = (bx - a)q(x)$ と表せる. 両辺の x^n の係数と定数項を比較して結論を得る. $\square$

この命題によって $f \in \mathbb{Z}[x]$ が 2 次または 3 次であれば, f の $\mathbb{Q}[x]$ における既約分解 (因数分解) を求めることができる. (4 次以上でも可能な場合もある.)

例 2.1 $f(x) = 2x^3 - 3x^2 - 11x + 6$ が有理数の根 a をもし持てば, a は $\pm 1, \pm 2, \pm 3, \pm 6, \pm 1/2, \pm 3/2$ のいずれかである. たとえば $f(-2) = 0$ となるので $f(x)$ を $x+2$ で割り算して $f(x) = (x+2)(2x^2 - 7x + 3)$ を得る. さらに同様に $2x^2 - 7x + 3 = (x-3)(2x-1)$ と分解できるので $\mathbb{Q}[x]$ における既約分解 $f(x) = (x+2)(x-3)(2x-1)$ を得る (各因子は整数係数多項式であることに注意.)

例 2.2 $f(x) = x^3 + 2x + 1$ の有理数根がもしあれば ± 1 のどちらかであるが, $f(\pm 1) \neq 0$ であるから $f(x)$ は $\mathbb{Q}$ 上既約である. 従って α を $f(\alpha) = 0$ を満たす複素数 (の一つ) とすれば, $f(x)$ は α の $\mathbb{Q}$ 上の最小多項式であり, $\mathbb{Q}(\alpha)$ は $\mathbb{Q}$ の 3 次拡大である.

4 次以上の多項式の場合は, たとえば

$$f(x) = x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 + x + 1)(x^2 - x + 1)$$

より f は $\mathbb{Q}$ 上既約でないが, $x^2 \pm x + 1$ は $\mathbb{Q}$ 上既約なので, f は有理数係数の 1 次式では割り切れない.

次のアイゼンシュタイン (Eisenstein) の判定法は, 既約性の十分条件を与える.

定理 2.1 (Eisenstein の判定法) 2 次以上の整数係数多項式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad (n \geq 2, a_i \in \mathbb{Z}, a_n \neq 0)$$

に対して, ある素数 p が存在して

$$p \nmid a_n, \quad p|a_i \quad (0 \leq i \leq n-1), \quad p^2 \nmid a_0$$

が成立すれば, $f(x)$ は $\mathbb{Q}$ 上既約である.

証明: $f(x)$ が $\mathbb{Q}$ 上既約でないとは定すると, 命題 2.1 によって 1 次以上の $g(x), h(x) \in \mathbb{Z}[x]$ が存在して $f(x) = g(x)h(x)$ が成立する.

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0, \quad h(x) = c_{n-m} x^{n-m} + c_{n-m-1} x^{n-m-1} + \cdots + c_0$$

とする. $\bar{a}_i$ を $a_i \in \mathbb{Z}$ の体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ における同値類として, $\bar{f}(x) \in \mathbb{F}_p[x]$ を

$$\bar{f}(x) = \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + \cdots + \bar{a}_1 x + \bar{a}_0$$

によって定義する. $\bar{g}(x), \bar{h}(x) \in \mathbb{F}_p[x]$ も同様に定義する. $\mathbb{Z} \ni c \mapsto \bar{c} \in \mathbb{F}_p$ が環準同型であることと $f(x) = g(x)h(x)$ より

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x) = (\bar{b}_m x^m + \cdots + \bar{b}_0)(\bar{c}_{n-m} x^{n-m} + \cdots + \bar{c}_0)$$

が成立する. 一方, 仮定により $\mathbb{F}_p[x]$ において $\bar{f}(x) = \bar{a}_n x^n$ かつ $\bar{a}_n \neq \bar{0}$ であるから, $\bar{g}(x)$ と $\bar{h}(x)$ は $\mathbb{F}_p[x]$ において x^n を割り切る. 従って $\bar{g}(x) = \bar{b}_m x^m$, $\bar{h}(x) = \bar{c}_{n-m} x^{n-m}$ である. 特に $g(x)$ と $h(x)$ の定数項は共に p の倍数であるから, $f(x) = g(x)h(x)$ の定数項 a_0 は p^2 の倍数でなければならないが, これは仮定に反する. 以上により $f(x)$ は $\mathbb{Q}$ 上既約である. $\square$

例 2.3 n を 2 以上の自然数とする. 整数 a はある素数 p の倍数であるが p^2 の倍数ではないとすると, $x^n - a$ は $\mathbb{Q}$ 上既約である. 特に任意の素数 p について $x^n \pm p$ は $\mathbb{Q}$ 上既約である. 従って $x^n - p$ は $\sqrt[n]{p}$ の最小多項式であり, $\mathbb{Q}(\sqrt[n]{p})$ は $\mathbb{Q}$ の n 次拡大である.

問題 2.1 次の多項式は $\mathbb{Q}$ 上既約かどうか判定し, 既約でなければ $\mathbb{Q}[x]$ における既約 (素元) 分解を求めよ.

- (1) $x^3 + x + 1$ (2) $x^3 + x^2 + x + 1$ (3) $x^4 + 12x^2 + 8x + 6$
 (4) $(x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1$ (ヒント: 展開する)
 (5) $x^4 + x^3 + x^2 + x + 1$ (ヒント: (4) を用いる) (6) $x^6 - 1$

問題 2.2 $x^4 + 1$ が $\mathbb{Q}$ 上既約であることを次の方針で証明せよ (あるいは別の方法で証明してもよい.)

- (1) $i = \sqrt{-1}$ を虚数単位として $\alpha = \frac{1+i}{\sqrt{2}}$ とおくと $\alpha^4 + 1 = 0$ が成立することを示せ.
 (2) α の $\mathbb{Q}(i)$ 上の最小多項式を求めよ.
 (3) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ を求めよ.
 (4) $x^4 + 1$ は α の $\mathbb{Q}$ 上の最小多項式であること, 従って $\mathbb{Q}$ 上既約であることを示せ.

3 分解体

定義 3.1 体 L が代数閉体 (algebraically closed field) であるとは, $L[x]$ の既約元 (= 素元) の全体と 1 次多項式の全体が一致することである. 言い換えれば ($L[x]$ は PID 従って UFD なので), $L[x]$ の 0 でない任意の元は $L[x]$ に属する 1 次多項式の積で表せることである.

次の事実は「複素関数論 II」で証明する.

定理 3.1 (代数学の基本定理) 複素数体 $\mathbb{C}$ は代数閉体である.

任意の体 (たとえば $\mathbb{F}_p$) に対して, それを部分体として含むような代数閉体が存在することを証明することもできるが抽象的な議論が必要になるので, 以下では簡単のため, 体はすべて複素数体 $\mathbb{C}$ の部分体であると仮定する.

補題 3.1 K を $\mathbb{C}$ の部分体とすると, K は有理数体 $\mathbb{Q}$ を部分体として含む.

証明: K は $0, 1, -1$ を含むから, 加法により K は $\mathbb{Z}$ を含むことがわかる. 任意の自然数 n に対してその逆元 $r \in K$ が存在する. このとき $\mathbb{C}$ において $nr = 1$ であるから, $r = n^{-1} = 1/n$ である. よって $1/n$ は K に属するから $\mathbb{Q} \subset K$ である. $\square$

定義 3.2 $\mathbb{C}$ の部分体 K と定数でない $f \in K[x]$ に対して, f の $\mathbb{C}$ における根を $\alpha_1, \dots, \alpha_n$ とするとき, $K(\alpha_1, \dots, \alpha_n)$ のことを f の K 上の (最小) 分解体 (splitting field) という.

例 3.1 $x^2 - 2$ の $\mathbb{Q}$ 上の最小分解体は 2 次拡大 $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ である ($\mathbb{C}[x]$ において $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ と分解され, $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ であるから.)

例 3.2 $x^3 - 2$ の $\mathbb{Q}$ 上の最小分解体 L を求めよう. $r, \theta \in \mathbb{R}$, $r > 0$ として $z = re^{i\theta} = r(\cos \theta + i \sin \theta)$ ($i = \sqrt{-1}$) とおくと

$$z^3 = r^3(\cos 3\theta + i \sin 3\theta) = 2 = 2(\cos 0 + i \sin 0)$$

が成り立つためには $r^3 = 2$ かつ $3\theta = 2n\pi$ ($\exists n \in \mathbb{Z}$) が必要十分である. よって

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

とおけば, $z^3 = 2$ を満たす複素数は $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ の 3 つであることがわかる. 従って $\mathbb{C}[x]$ において

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$$

と分解される. $\omega = \sqrt[3]{2}\omega^2(\sqrt[3]{2}\omega)^{-1}$ であるから,

$$L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$$

となる. Eisenstein の判定法より $f(x) = x^3 - 2$ は $\mathbb{Q}$ 上既約であるから $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式であり, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ である. ω は実数ではなく $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ であるから, ω の $\mathbb{Q}(\sqrt[3]{2})$ 上の最小多項式の次数は 2 以上である. 一方 $g(x) = x^2 + x + 1$ とすれば

$$g(\omega) = \omega^2 + \omega + 1 = \frac{\omega^3 - 1}{\omega - 1} = 0$$

であるから, $g(x)$ が ω の $\mathbb{Q}(\sqrt[3]{2})$ 上の最小多項式であり, $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$ である. 以上により $[L : \mathbb{Q}] = 6$ であり, $1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega$ が L の $\mathbb{Q}$ ベクトル空間としての基底である ($1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[3]{3}i, \sqrt[3]{2}\sqrt[3]{3}i, \sqrt[3]{4}\sqrt[3]{3}i$ でもよい.)

例 3.3 $x^4 - 4 = (x^2 + 2)(x^2 - 2)$ の $\mathbb{Q}$ 上の最小分解体は $L = \mathbb{Q}(\sqrt{2}, i\sqrt{2}) = \mathbb{Q}(\sqrt{2}, i)$ である. $[L : \mathbb{Q}] = 4$ であり, $1, \sqrt{2}, i, \sqrt{2}i$ が L の $\mathbb{Q}$ 上の基底である.

命題 3.1 K を $\mathbb{C}$ の部分体, $f(x) \in K[x]$ とする. $f(x)$ が $K[x]$ の既約元 (= 素元) ならば, $f(x)$ の $\mathbb{C}$ における根はすべて相異なる.

証明: $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$ ($c_k \in K, c_n \neq 0$) とする. $f(x)$ の導関数 $f'(x) = n c_n x^{n-1} + \cdots + c_1$ の次数は $n-1 < n = \deg f$ であり, $f(x)$ は既約だから, $f(x)$ と $f'(x)$ は $K[x]$ において互いに素である. よって $f(x)$ と $f'(x)$ の生成するイデアルは $K[x]$ 全体となるから,

$$a(x)f(x) + b(x)f'(x) = 1 \quad (1)$$

を満たす $a(x), b(x) \in K[x]$ が存在する. 一方, $f(x)$ の $\mathbb{C}[x]$ における既約 (素元) 分解を

$$f(x) = c_n (x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k} \quad (\alpha_1, \dots, \alpha_k \text{ は相異なる複素数})$$

とすると,

$$\begin{aligned} f'(x) &= m_1 c_n (x - \alpha_1)^{m_1-1} \cdots (x - \alpha_k)^{m_k} + \cdots \\ &\quad + m_j c_n (x - \alpha_1)^{m_1} \cdots (x - \alpha_j)^{m_j-1} \cdots (x - \alpha_k)^{m_k} \\ &\quad + \cdots + m_k c_n (x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k-1} \end{aligned}$$

であり, x に α_j を代入すると, 右辺の第 j 番目の項以外は 0 になるから, もし $m_j \geq 2$ ならば $f'(\alpha_j) = f(\alpha_j) = 0$ となる. よって式 (1) に $x = \alpha_j$ を代入すると $0 = 1$ となり矛盾である. 従って $k = n$ かつ $m_1 = \cdots = m_k = 1$ でなければならない. $\square$

定理 3.2 K と L を複素数体 $\mathbb{C}$ の部分体とする. $L \supset K$ が有限次拡大であれば単純拡大である. すなわち, ある $\alpha \in L$ が存在して $L = K(\alpha)$ となる. α は K 上代数的である.

証明: (1) $\alpha, \beta \in \mathbb{C}$ が K 上代数的であるとする. 適当な $c \in K$ を選ぶと $K(\alpha, \beta) = K(\alpha + c\beta)$ が成立する (従って単純拡大である) ことを示す.

$f_\alpha(x), f_\beta(x) \in K[x]$ をそれぞれ α, β の K 上の最小多項式とする. $\mathbb{C}[x]$ において

$$f_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n), \quad f_\beta(x) = (x - \beta_1) \cdots (x - \beta_m) \quad (\alpha_j, \beta_k \in \mathbb{C})$$

と1次式の積に分解される．命題 3.1 より $\alpha_1, \dots, \alpha_n$ は相異なり， $\beta_1, \dots, \beta_m$ も相異なる．順番を入れ替えて $\alpha = \alpha_1, \beta = \beta_1$ としてよい． K は $\mathbb{Q}$ を含むから無限集合であり，

$$c \neq -\frac{\alpha - \alpha_j}{\beta - \beta_k} = -\frac{\alpha_1 - \alpha_j}{\beta_1 - \beta_k} \quad (1 \leq \forall j \leq n, 2 \leq \forall k \leq m)$$

を満たすような $c \in K$ を選ぶことができる．このような c を1つ選んで $\gamma = \alpha + c\beta$ とおく．このとき $K(\gamma) = K(\alpha, \beta)$ となることを示せばよい．

そのために，まず $\beta \in K(\gamma)$ を示そう． β の $K(\gamma)$ 上の最小多項式を $h(x)$ とする． $g(x) = f_\alpha(\gamma - cx)$ とおくと $g(x)$ は $K(\gamma)[x]$ に属し， $g(\beta) = f_\alpha(\gamma - c\beta) = f_\alpha(\alpha) = 0$ であるから， $g(x)$ は $h(x)$ の倍元である．また， $f_\beta(\beta) = 0$ かつ $f_\beta(x) \in K[x] \subset K(\gamma)[x]$ より $f_\beta(x)$ も $h(x)$ の倍元である．一方，複素数 z について

$$g(z) = 0 \Leftrightarrow f_\alpha(\gamma - cz) = 0 \Leftrightarrow \gamma - cz = \alpha_j \quad (1 \leq \exists j \leq n)$$

であるから，もし $g(\beta_k) = 0$ ($2 \leq \exists k \leq m$) とすると，ある j があって， $\gamma - c\beta_k = \alpha + c\beta - c\beta_k = \alpha_j$ すなわち $c = -\frac{\alpha - \alpha_j}{\beta - \beta_k}$ となり， c の選び方に反する．従って $g(\beta_k) \neq 0$

($2 \leq \forall k \leq m$) である． $h(x)$ は $K(\gamma)[x]$ において $f_\beta(x)$ と $g(x)$ の共約元だから，結局 $h(x)$ の $\mathbb{C}$ における根は $\beta = \beta_1$ のみである． $h(x)$ は $K(\gamma)[x]$ で既約であり命題 3.1 より根はすべて相異なるので， $h(x) = x - \beta$ である． $h(x) \in K(\gamma)[x]$ であったから， β は $K(\gamma)$ に属する．従って $\alpha = \gamma - c\beta$ も $K(\gamma)$ に属するから， $K(\alpha, \beta) \subset K(\gamma)$ である．一方 $\gamma = \alpha + c\beta \in K(\alpha, \beta)$ より $K(\gamma) \subset K(\alpha, \beta)$ も成立する．以上により $K(\alpha, \beta) = K(\gamma)$ が示された．

(2) 一般の場合: 定理 1.3 により， K 上代数的な L の元 $\alpha_1, \dots, \alpha_n$ が存在して

$$L = K(\alpha_1, \dots, \alpha_n)$$

となる． $n \geq 2$ であれば (1) より， K 上代数的な $\beta \in L$ があって $K(\alpha_1, \alpha_2) = K(\beta)$ が成り立つ．従って， $L = K(\beta, \alpha_3, \dots, \alpha_n)$ となる．以下同様にして生成元の個数を減らして1つにすることができる．□

例 3.4 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ を考える． $c := 1$ は0とも $-\frac{\sqrt{2} - (-\sqrt{2})}{\sqrt{3} - (-\sqrt{3})} = -\frac{\sqrt{2}}{\sqrt{3}}$ とも異なるから定理 3.2 の証明から， $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ が成立する．このことは， $\alpha := \sqrt{2} + \sqrt{3}$ とおけば

$$\alpha^{-1} = \sqrt{3} - \sqrt{2}, \quad \sqrt{3} = \frac{1}{2}(\alpha + \alpha^{-1}), \quad \sqrt{2} = \frac{1}{2}(\alpha - \alpha^{-1})$$

が $\mathbb{Q}(\alpha)$ に属することからもわかる． α の $\mathbb{Q}$ 上の最小多項式を求めよう．

$$\alpha^2 = 5 + 2\sqrt{6}, \quad (\alpha^2 - 5)^2 = 24$$

より $f(x) = x^4 - 10x^2 + 1$ は $f(\alpha) = 0$ を満たす． $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}$ の4次拡大であったから，この $f(x)$ が α の $\mathbb{Q}$ 上の最小多項式である．

問題 3.1 次の多項式の $\mathbb{Q}$ 上の分解体を求めよ (なるべく簡単な表示を求めよ.) また分解体の $\mathbb{Q}$ 上の拡大次数を求めよ.

$$(1) \quad x^2 + x - 1 \quad (2) \quad x^4 - 1 \quad (3) \quad x^6 - 1 \quad (4) \quad x^3 - 8 \quad (5) \quad x^4 + 4$$

問題 3.2 $i = \sqrt{-1}$ とするとき $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$ が成立することを示せ. また $\sqrt{2} + i$ の $\mathbb{Q}$ 上の最小多項式を求めよ (ヒント: $\alpha = \sqrt{2} + i$ として, α^{-1} を用いて $\sqrt{2}$ と i が $\mathbb{Q}(\alpha)$ に属することを示すとよい.)

4 有限次拡大と体準同型

$\mathbb{C} \supset L \supset K$ を体の拡大とする. 体準同型 $\sigma : L \rightarrow \mathbb{C}$ が K 上の体準同型であるとは, $\sigma(a) = a$ がすべての $a \in K$ について成立することである. このとき, L と $\mathbb{C}$ を K 上のベクトル空間とみなすと, σ を L から $\mathbb{C}$ への K 線形写像とみなすこともできる. 実際, $\alpha \in L$ と $c \in K$ に対して $\sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\sigma(\alpha)$ が成立する. (L から $\mathbb{C}$ への任意の K 線形写像が K 上の体準同型になるわけではない.)

$\sigma : L \rightarrow \mathbb{C}$ を K 上の体準同型とすると, 多項式 $f = f(x) = c_n x^n + \cdots + c_1 x + c_0 \in L[x]$ に対して, 多項式 $\sigma(f) \in \mathbb{C}[x]$ を

$$\sigma(f)(x) := \sigma(c_n)x^n + \cdots + \sigma(c_1)x + \sigma(c_0)$$

によって定義する. これにより環準同型 $\sigma : L[x] \rightarrow \mathbb{C}[x]$ が定まる. 任意の $\alpha \in L$ に対して

$$\begin{aligned} \sigma(f)(\sigma(\alpha)) &= \sigma(c_n)\sigma(\alpha)^n + \cdots + \sigma(c_1)\sigma(\alpha) + \sigma(c_0) \\ &= \sigma(c_n\alpha^n + \cdots + c_1\alpha + c_0) = \sigma(f(\alpha)) \end{aligned}$$

が成立する. 特に $f(x) \in K[x]$ ならば $\sigma(f) = f$ より, $f(\sigma(\alpha)) = \sigma(f(\alpha))$ が成立する.

定理 4.1 K を $\mathbb{C}$ の部分体, $\alpha \in \mathbb{C}$ を K 上代数的な元として, α の K 上の最小多項式を $f_\alpha(x)$ とする. $f_\alpha(x)$ の $\mathbb{C}[x]$ における既約分解を

$$f_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_1 = \alpha, \alpha_2, \dots, \alpha_n \in \mathbb{C}$$

とする. このとき各 $j = 1, \dots, n$ に対して, $K(\alpha)$ から $\mathbb{C}$ への K 上の体準同型 σ_j であって, $\sigma_j(\alpha) = \alpha_j$ をみたすものがただ 1 つ存在する. さらに $K(\alpha)$ から $\mathbb{C}$ への K 上の体準同型はこれらの n 個のみである.

証明: $n = 1$ のときは $K(\alpha) = K$ であるから K 上の体準同型は恒等写像のみであり定理は成立する. よって $n \geq 2$ としてよい. 命題 3.1 により $\alpha_1, \dots, \alpha_n$ は相異なる. $1 \leq j \leq n$ とする. $f_\alpha(x)$ は α_j の K 上の最小多項式でもあるから, $I(\alpha_j) = I(\alpha)$ であり, 定理 1.1 により体同型

$$\psi_j : K[x]/I(\alpha) = K[x]/I(\alpha_j) \xrightarrow{\sim} K[\alpha_j] = K(\alpha_j) \subset \mathbb{C}$$

が存在する．従って $\psi_j \circ \psi_1^{-1} : K(\alpha_1) \rightarrow K(\alpha_j)$ は体同型である．定理 1.1 の証明からわかるように， $a, b \in K$ のとき $\psi_j([ax + b]) = a\alpha_j + b$ であるから，

$$\psi_j \circ \psi_1^{-1}(\alpha_1) = \psi_j([x]) = \alpha_j, \quad \psi_j \circ \psi_1^{-1}(b) = \psi_j([b]) = b \quad (\forall b \in K)$$

が成立する．従って $\sigma_j := \psi_j \circ \psi_1^{-1}$ を $K(\alpha)$ から $K(\alpha_j) \subset \mathbb{C}$ への体準同型とみなせば， σ_j は K 上の体準同型であり， $\sigma_j(\alpha) = \alpha_j$ を満たす．

逆に $\sigma : K(\alpha) \rightarrow \mathbb{C}$ を K 上の任意の体準同型とする．

$$f_\alpha(\sigma(\alpha)) = \sigma(f_\alpha(\alpha)) = \sigma(0) = 0$$

であるから， $\sigma(\alpha)$ は $f_\alpha(x)$ の根であり， $\sigma(\alpha) = \alpha_j$ ($1 \leq j \leq n$) となる． $K(\alpha) = K[\alpha]$ の任意の元はある多項式 $g(x) \in K[x]$ によって $g(\alpha)$ と表される．このとき

$$\sigma(g(\alpha)) = g(\sigma(\alpha)) = g(\alpha_j)$$

となる．一方

$$\psi_j(g(\alpha)) = g(\psi_j(\alpha)) = g(\alpha_j)$$

も成立するから， $\sigma = \psi_j$ である．□

例 4.1 ($\mathbb{Q}(\sqrt{2})$) $\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ であるから， $\mathbb{Q}$ 上の体準同型 $\sigma : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{C}$ であって $\sigma(\sqrt{2}) = -\sqrt{2}$ をみたすものが存在する． $a, b \in \mathbb{Q}$ に対して

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

$\mathbb{Q}(\sqrt{2})$ から $\mathbb{C}$ への $\mathbb{Q}$ 上の準同型は，この σ と埋め込み写像 $\text{id} : \mathbb{Q} \rightarrow \mathbb{C}$ の 2 つである．

例 4.2 ($\mathbb{Q}(\sqrt[3]{2})$) $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^3 - 2$ であり， $\mathbb{C}[x]$ において

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2), \quad \omega = \frac{-1 + \sqrt{3}i}{2}$$

と既約分解されたから (例 3.2)， $\mathbb{Q}(\sqrt[3]{2})$ から $\mathbb{C}$ への $\mathbb{Q}$ 上の体準同型は 3 つある．1 つは埋め込み写像であり，あとの 2 つ σ, τ はそれぞれ $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ ， $\tau(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$ を満たす． $\sigma(\mathbb{Q}(\sqrt[3]{2}))$ と $\tau(\mathbb{Q}(\sqrt[3]{2}))$ は $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ には含まれないことに注意する．

5 群についての復習

定義 5.1 集合 G が群 (group) であるとは，2 項演算

$$G \times G \ni (\sigma, \tau) \longmapsto \sigma\tau \in G$$

が定義されていて，

$$(1) \quad (\sigma_1\sigma_2)\sigma_3 = \sigma_1(\sigma_2\sigma_3) \quad (\forall \sigma_1, \sigma_2, \sigma_3 \in G)$$

- (2) ある $e \in G$ が存在して $e\sigma = \sigma e = \sigma$ が任意の $\sigma \in G$ について成立する (e を G の単位元 (identity element) という.)
- (3) 任意の $\sigma \in G$ に対して $\sigma\tau = \tau\sigma = e$ を満たす $\tau \in G$ が存在する (このとき $\tau = \sigma^{-1}$ と表して σ の逆元と呼ぶ.)

が成立することである.

群 G が可換群 (commutative group) またはアーベル群 (abelian group) であるとは, $\sigma\tau = \tau\sigma$ が任意の $\sigma, \tau \in G$ について成り立つことである. G がアーベル群であるとき演算 $\sigma\tau$ を加法の形で $\sigma + \tau$ と表すこともある (単位元は 0 で表す.) このとき G を加法群ともいう. たとえば n を任意の自然数とすると環 $\mathbb{Z}/n\mathbb{Z}$ は加法に関してアーベル群である.

G が有限集合であるとき, G を有限群といい, G の元の個数 $|G| = \sharp G$ を G の位数 (order) という.

以下, 群 G は有限群であるとする. $\sigma \in G$ に対して, $\sigma^n = e$ となるような最小の非負整数 n のことを σ の位数 (order) という. 群 G のある元 σ の位数が $n = |G|$ に等しいとき, G を巡回群 (cyclic group) という. このとき σ のことを G の生成元 (generator) といい $G = \langle \sigma \rangle$ と表す. このとき $e, \sigma, \dots, \sigma^{n-1}$ は相異なるので $G = \{e, \sigma, \dots, \sigma^{n-1}\}$ となることがわかる. 特に, 巡回群はアーベル群である. たとえば $\bar{1} \in \mathbb{Z}/n\mathbb{Z}$ の (加法に関する) 位数は $n = |\mathbb{Z}/n\mathbb{Z}|$ であるから $\mathbb{Z}/n\mathbb{Z}$ は巡回群である. 位数 (元の個数) が素数の群は巡回群である.

G と G' を群とすると, 写像 $\varphi: G \rightarrow G'$ が群準同型 (group homomorphism) であるとは, $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$ が任意の $\sigma, \tau \in G$ について成立することである. さらに φ が全単射であるとき φ は群同型 (group isomorphism), または G と G' は群として同型であるという.

群 G の部分集合 H が G の部分群であるとは, H が e を含み G と同じ演算で群となっていることである. このとき H の位数は G の位数の約数である. さらに, 群 G の部分群 H が G の正規部分群 (normal subgroup) であるとは, 任意の $\sigma \in H$ と任意の $\tau \in G$ に対して $\tau\sigma\tau^{-1} \in H$ となることである. 特に, アーベル群の任意の部分群は正規部分群である.

H を群 G の正規部分群とすると, 剰余群 (quotient group) G/H が次のように定義できる. G/H は剰余類 $\sigma H = \{\sigma h \mid h \in H\}$ ($\sigma \in H$) のうち相異なるものの全体であり, $(\sigma H)(\tau H) = (\sigma\tau)H$ により G/H の 2 項演算が定義できて群となる. 単位元は $eH = H$ である. また G/H の位数は $|G|/|H|$ である.

S を n 個の元からなる集合とすると S から S への全単射の全体を S_n と表す. S_n の元を (S の) 置換 (permutation) という. $\sigma, \tau \in S_n$ に対して $\sigma\tau = \sigma \circ \tau$ (合成写像) と定義すると群となる. 単位元は恒等写像 $\text{id} = \text{id}_S$ である. この群を n 次対称群 (symmetric group) といい S_n と表す. S_n の位数は $n!$ である. $S = \{1, 2, \dots, n\}$ としても一般性を失わない. $\sigma \in S_n$ を

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

と表す．列は自由に移動してもよい．また動かさない元に対応する列は省略してもよい．このとき任意の $\tau \in S_n$ に対して

$$\tau\sigma\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \cdots & \tau(n) \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \cdots & \tau(\sigma(n)) \end{pmatrix}$$

となることが容易にわかる．

$n_1, \dots, n_r$ を S の相異なる元とすると

$$(n_1 \ n_2 \ \cdots \ n_r) := \begin{pmatrix} n_1 & n_2 & \cdots & n_{r-1} & n_r \\ n_2 & n_3 & \cdots & n_r & n_1 \end{pmatrix}$$

を長さ r の巡回置換 (cyclic permutation) という．特に長さ 2 の巡回置換を互換 (transposition) という．任意の置換はいくつかの互換の積で表され，互換の個数の偶奇は分解のしかたによらないことを示すことができる．偶数個の互換の積で表されるような置換を偶置換，奇数個の互換の積で表されるような置換を奇置換という． S_n の元のうち偶置換の全体 A_n は S_n の正規部分群となる． A_n を n 次の交代群 (alternating group) という． A_n の位数は $n!/2$ である．

任意の置換は，共通成分を含まないような巡回置換の積 (合成) として (順序を除いて一意的に) 表すことができる．これをサイクル分解という．たとえば

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (1 \ 3)(2 \ 4 \ 5)$$

このとき，任意の $\tau \in S_n$ ($n \geq 5$) に対して

$$\tau\sigma\tau^{-1} = (\tau(1) \ \tau(3))(\tau(2) \ \tau(4) \ \tau(5))$$

も同じ型のサイクル分解を持つ．一般の場合も同様である．

G を群， A を集合とする．写像

$$G \times A \ni (\sigma, a) \longmapsto \sigma(a) \in A$$

が定義されていて (すなわち G の元を A から A への写像とみなす)， $\sigma(\tau(a)) = (\sigma\tau)(a)$ ， $e(a) = a$ が任意の $\sigma, \tau \in G$ と $a \in A$ について成立するとき，これを G の A への作用 (action)，または G が A に作用しているという． $a \in A$ に対して A の部分集合

$$O(a) := \{\sigma(a) \mid \sigma \in G\}$$

を a の G 軌道 (G -orbit) という． A はいくつかの G 軌道の互いに交わらない和集合となる． A 全体が 1 つの G 軌道である，すなわち $A = O(a)$ となるような $a \in A$ が存在するとき， G は A に推移的に作用しているという．このとき，任意の $b, c \in A$ に対して $c = \sigma(b)$ となるような $\sigma \in G$ が存在する．実際このとき， $b = \sigma_1(a)$ ， $c = \sigma_2(a)$ を満たす $\sigma_1, \sigma_2 \in G$ が存在する． $c = \sigma_2(a) = \sigma_2(\sigma_1^{-1}(b)) = (\sigma_2\sigma_1^{-1})(b)$ より $\sigma = \sigma_2\sigma_1^{-1}$ とすればよい．たとえば， S_n は集合 $\{1, 2, \dots, n\}$ に (写像として) 推移的に作用している． $n \geq 3$ ならば A_n も $\{1, 2, \dots, n\}$ に推移的に作用する．

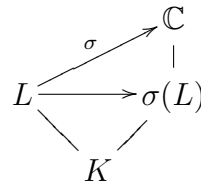
6 ガロア拡大とガロア群

定義 6.1 $\mathbb{C} \supset L \supset K$ を体の拡大とする. このとき $L \supset K$ がガロア拡大 (Galois extension) または正規拡大 (normal extension) であるとは, L が $K[x]$ に属するある多項式 (既約でなくてもよい) の K 上の (最小) 分解体になっていることである. このとき L は K のガロア拡大であるとも言う.

たとえば例 3.1 と例 3.3 により, $\mathbb{Q}(\sqrt{2})$ と $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$ は共に $\mathbb{Q}$ のガロア拡大である.

一般に, $L \supset K$ がガロア拡大であれば, 定理 1.3 により $L \supset K$ は有限次拡大であり, 命題 1.2 により L の任意の元 α は K 上代数的である (すなわち α の K 上の最小多項式が存在する).

命題 6.1 $L \supset K$ をガロア拡大として, $\sigma: L \rightarrow \mathbb{C}$ を K 上の体準同型とする.



- (1) σ は L から L への K 上の体同型となる. すなわち $\sigma(L) = L$ が成立する.
- (2) L が $f(x) \in K[x]$ の分解体であるとき, $f(x)$ の相異なる根を $\alpha_1, \dots, \alpha_n$ とすると, 集合として

$$\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\} = \{\alpha_1, \dots, \alpha_n\}$$

が成立する. すなわち σ は集合 $\{\alpha_1, \dots, \alpha_n\}$ の置換を引き起こす. さらに, $\sigma(\alpha_j) = \alpha_j$ がすべての $j = 1, \dots, n$ について成立すれば $\sigma = \text{id}_L$ である.

証明: L は $f(x) \in K[x]$ の分解体であるとして, $f(x)$ の相異なる根を $\alpha_1, \dots, \alpha_n$ とすると, $L = K(\alpha_1, \dots, \alpha_n)$ である. $\sigma: L \rightarrow \mathbb{C}$ を K 上の体準同型とすると, $1 \leq j \leq n$ のとき $f(\sigma(\alpha_j)) = \sigma(f(\alpha_j)) = \sigma(0) = 0$ であるから, ある $k(j) \in \{1, \dots, n\}$ があって, $\sigma(\alpha_j) = \alpha_{k(j)}$ となる. σ は体準同型であるから単射であり, $\alpha_{k(1)}, \dots, \alpha_{k(n)}$ は相異なる. 従って集合として $\{\alpha_{k(1)}, \dots, \alpha_{k(n)}\} = \{\alpha_1, \dots, \alpha_n\}$ である. よって σ は $\{\alpha_1, \dots, \alpha_n\}$ の置換を引き起こす.

これを用いて $\sigma(L) \subset L$ を示そう. $\alpha \in L$ とすると, 補題 1.2 により, K の元を係数とする n 変数多項式 $g(x_1, \dots, x_n)$ と $h(x_1, \dots, x_n)$ が存在して

$$\alpha = \frac{h(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}$$

と表される. g と h の係数は K の元であり σ は K の元を固定するから,

$$\sigma(\alpha) = \frac{\sigma(h(\alpha_1, \dots, \alpha_n))}{\sigma(g(\alpha_1, \dots, \alpha_n))} = \frac{h(\sigma(\alpha_1), \dots, \sigma(\alpha_n))}{g(\sigma(\alpha_1), \dots, \sigma(\alpha_n))} = \frac{h(\alpha_{k(1)}, \dots, \alpha_{k(n)})}{g(\alpha_{k(1)}, \dots, \alpha_{k(n)})}$$

が成立し, $\sigma(\alpha)$ は $K(\alpha_1, \dots, \alpha_n) = L$ に属する. よって $\sigma(L) \subset L$ が示された. ここで, $\sigma(\alpha_j) = \alpha_j$ がすべての $j = 1, \dots, n$ について成立すると仮定すると, 上の等式より $\sigma(\alpha) = \alpha$ が成立することがわかるから, $\sigma = \text{id}_L$ である.

σ は K 上の有限次元ベクトル空間 L から $\sigma(L)$ の上への K 線形写像ともみなせ, 体準同型であるから単射である. 従って σ は L から $\sigma(L)$ への K ベクトル空間としての同型写像である. よって L と $\sigma(L)$ の K ベクトル空間としての次元は同じである. これと $\sigma(L) \subset L$ より $\sigma(L) = L$ が従う. よって σ は L から L への同型写像である. $\square$

例 6.1 上の命題と例 4.2 から $\mathbb{Q}(\sqrt[3]{2})$ は $\mathbb{Q}$ のガロア拡大ではないことがわかる ($\mathbb{Q}(\sqrt[3]{2})$ から $\mathbb{C}$ への体準同型であって像が $\mathbb{Q}(\sqrt[3]{2})$ に含まれないものが存在するから.) 一方, $\omega = \frac{-1 + \sqrt{3}i}{2}$ とすると, $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ は $x^3 - 2$ の $\mathbb{Q}$ 上の分解体であるから $\mathbb{Q}$ のガロア拡大である.

定義 6.2 $L \supset K$ をガロア拡大とするとき, L から L への K 上の体同型の全体が写像の合成を演算としてなす群のことを拡大 $L \supset K$ の (あるいは L の K 上の) ガロア群 (Galois group) といい, $\text{Gal}(L/K)$ で表す. 単位元は L から L への恒等写像 $\text{id}_L : L \ni \alpha \mapsto \alpha \in L$ である. L が $f(x) \in K[x]$ の分解体であるとき, $\text{Gal}(L/K)$ のことを多項式 $f(x)$ の K 上のガロア群とも呼ぶ.

補題 6.1 $L \supset K$ をガロア拡大とする. L の元 $\alpha_1, \dots, \alpha_n$ によって $L = K(\alpha_1, \dots, \alpha_n)$ と表示されると仮定する. このとき $G = \text{Gal}(L/K)$ の元 σ は $\sigma(\alpha_j)$ ($j = 1, \dots, n$) から一意的に定まる. すなわち $\sigma, \tau \in G$ が

$$\sigma(\alpha_j) = \tau(\alpha_j) \quad (1 \leq \forall j \leq n)$$

を満たせば G の元として $\sigma = \tau$ である.

証明: β を L の任意の元とすると, 補題 1.2 によって $\beta = \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}$ となるような n 変数多項式 $f, g \in K[x_1, \dots, x_n]$ が存在する. $\sigma \in G$ とすると f と g の係数が K の元であり, σ は K の元を固定するから,

$$\sigma(\beta) = \frac{\sigma(f(\alpha_1, \dots, \alpha_n))}{\sigma(g(\alpha_1, \dots, \alpha_n))} = \frac{f(\sigma(\alpha_1), \dots, \sigma(\alpha_n))}{g(\sigma(\alpha_1), \dots, \sigma(\alpha_n))}$$

が成立する. 従って $\sigma(\beta)$ は $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ から 4 則演算によって一意的に定まる. $\square$

ガロア拡大が単純拡大で表されていればガロア群は次のように決まる.

定理 6.1 $L \supset K$ はガロア拡大であって, $L = K(\alpha)$ ($\alpha \in L$) とする. $f(x) \in K(x)$ を α の K 上の最小多項式として, $\alpha = \alpha_1, \dots, \alpha_n$ をその根とする. このとき, 各 $j = 1, \dots, n$ に対して, $\sigma_j(\alpha) = \alpha_j$ を満たすような $\sigma_j \in \text{Gal}(L/K)$ がただ 1 つ存在して

$$\text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$$

となる. 特に任意の $j = 1, \dots, n$ について α_j は L に属し, 従って L は $f(x)$ の K 上の分解体である.

証明: $1 \leq j \leq n$ のとき, 定理 4.1 により, $\sigma_j(\alpha) = \alpha_j$ をみたすような $L = K(\alpha)$ から $\mathbb{C}$ への K 準同型 σ_j があり, これらが L から $\mathbb{C}$ への K 上の体準同型のすべてである. 命題 6.1 により σ_j は L の K 上の自己同型であるから $\text{Gal}(L/K)$ に属する. 以上により $G(L/K) = \{\sigma_1, \dots, \sigma_n\}$ である. 特に $\alpha_j = \sigma_j(\alpha)$ は L に属する. 従って $K(\alpha) \subset K(\alpha_1, \dots, \alpha_n) \subset L$ であるが仮定より $K(\alpha) = L$ だから $L = K(\alpha_1, \dots, \alpha_n)$ が成立する. $\square$

定理 6.2 $L \supset K$ をガロア拡大とすると, $|\text{Gal}(L/K)| = [L : K]$ が成立する. すなわち, ガロア群の位数は拡大次数に等しい.

証明: 定理 3.2 により, K 上代数的な $\alpha \in L$ が存在して $L = K(\alpha)$ が成立する. α の K 上の最小多項式を $f(x)$ としてその次数を n とすると, 定理 1.1 より $[L : K] = n$ である. 一方, 定理 6.1 より $|\text{Gal}(L/K)| = n$ が成立する. $\square$

例 6.2 整数 m は平方因子を含まない (素数の 2 乗で割り切れない) 2 以上の自然数であるか, または負であるとして体の拡大 $\mathbb{Q}(\sqrt{m}) \supset \mathbb{Q}$ を考える. $m > 0$ のときは, m を割り切る素数の 1 つを p とすると, m は p^2 では割り切れないから, Eisenstein の判定法により $x^2 - m$ は $\mathbb{Q}$ 上既約である. また $m < 0$ のときは $c^2 = m$ を満たす有理数 c は存在しないから $x^2 - m$ は $\mathbb{Q}$ 上既約である. 以上により, $f(x) = x^2 - m$ が $\alpha := \sqrt{m}$ の $\mathbb{Q}$ 上の最小多項式である. このとき $\mathbb{C}[x]$ において $x^2 - m = (x - \alpha)(x + \alpha)$ と既約分解されるから, $L := \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, -\alpha)$ は $x^2 - m$ の $\mathbb{Q}$ 上の分解体であり, $\mathbb{Q}(\sqrt{m}) \supset \mathbb{Q}$ はガロア拡大である. 定理 6.1 により $\sigma(\sqrt{m}) = -\sqrt{m}$ を満たす $\sigma \in \text{Gal}(L/\mathbb{Q})$ が存在して, $\text{Gal}(L/\mathbb{Q}) = \{\text{id}_L, \sigma\}$ である. この群は 2 次巡回群 $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ に同型である.

次の命題によってガロア群を適当な次数の対称群の部分群とみなすことができる.

命題 6.2 $L \supset K$ をガロア拡大としてそのガロア群を $G := \text{Gal}(L/K)$ とする. L が $f(x) \in K[x]$ の分解体であるとして, $A = \{\alpha_1, \dots, \alpha_n\}$ を $f(x)$ の相異なる根全体の集合とする. このとき, G の元 σ は, 定義域を A に制限すると A の置換, すなわち A から A への全単射を引き起こす. これを $\sigma|_A$ で表す. $\sigma|_A$ を n 次対称群 S_n の元とみなすと, 対応

$$G \ni \sigma \longmapsto \sigma|_A \in S_n$$

は単射群準同型である. これによって G を S_n の部分群とみなすことができる. 特に $|G|$ は $n!$ の約数である.

証明: 命題 6.1 の (2) により, $\sigma \in G$ の A への制限 (定義域 L を A に制限した写像) $\sigma|_A$ は A の置換であるから S_n の元とみなせる. 対応 $\sigma \longmapsto \sigma|_A$ が G から S_n の群準同型であること, すなわち $\sigma, \tau \in G$ に対して $(\sigma \circ \tau)|_A = (\sigma|_A) \circ (\tau|_A)$ が成立することは写像の合成と制限の定義より明らかである. この準同型が単射であることを示すため, $\sigma|_A$ が恒等写像であると仮定すると, 命題 6.1 の (2) より $\sigma = \text{id}_L$ である. よって準同型 $\sigma \mapsto \sigma|_A$ は単射である. $\square$

例 6.3 $f(x) = x^3 - 2$ の分解体 L の $\mathbb{Q}$ 上のガロア群 $G = \text{Gal}(L/\mathbb{Q})$ を求めよう.

$$L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

であり, $[L:\mathbb{Q}] = 6$ であった (例 3.2) から G の位数は 6 である. また, $L[x]$ において

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$$

と既約分解されるから, 命題 6.2 より, G は $f(x)$ の根の集合 $A = \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$ への作用によって 3 次対称群 S_3 の部分群とみなせるが, $|G| = 6 = |S_3|$ であるから, G は S_3 に同型である.

補題 6.2 $L \supset K$ をガロア拡大とする. $\alpha \in L$ と 1 次以上の多項式 $f(x) \in K[x]$ が $f(\alpha) = 0$ を満たせば, $\text{Gal}(L/K)$ の任意の元 σ について $f(\sigma(\alpha)) = 0$ が成立する.

証明: σ は $f(x)$ の係数を固定するから $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$ が成立する. $\square$

例 6.4 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}$ のガロア群を求めよう. L は $(x^2 - 2)(x^2 - 3)$ の $\mathbb{Q}$ 上の分解体であるから, $L \supset \mathbb{Q}$ はガロア拡大である. 例 1.6 により拡大次数は 4 である. $\sigma \in G := \text{Gal}(L/\mathbb{Q})$ とする. $\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^2 - 2$ であり $\mathbb{C}[x]$ において $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ と分解されるから, 補題 6.2 によって $\sigma(\sqrt{2}) = \pm\sqrt{2}$ でなければならない. 同様に $\sigma(\sqrt{3}) = \pm\sqrt{3}$ でなければならない. このとき $\sigma(-\sqrt{2}) = -\sigma(\sqrt{2})$ かつ $\sigma(-\sqrt{3}) = -\sigma(\sqrt{3})$ であるから, $A = \{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}$ とすると, $\sigma|_A$ は $\sigma(\sqrt{2})$ と $\sigma(\sqrt{3})$ から一意的に決まり, 4 通りの可能性しかない. 一方, $|G| = [L:\mathbb{Q}] = 4$ であり, 命題 6.2 によって制限写像 $G \ni \sigma \mapsto \sigma|_A$ は単射であるから, 実際にこの 4 通りの A の置換を引き起こす $\sigma \in G$ が存在する. すなわち,

$$\begin{aligned} \sigma_2(\sqrt{2}) &= -\sqrt{2}, & \sigma_2(\sqrt{3}) &= \sqrt{3}, & \sigma_3(\sqrt{2}) &= \sqrt{2}, & \sigma_3(\sqrt{3}) &= -\sqrt{3}, \\ \sigma_4(\sqrt{2}) &= -\sqrt{2}, & \sigma_4(\sqrt{3}) &= -\sqrt{3}, \end{aligned}$$

を満たすような $\sigma_2, \sigma_3, \sigma_4 \in G$ がそれぞれただ 1 つ存在して $G = \{\sigma_1 = \text{id}_L, \sigma_2, \sigma_3, \sigma_4\}$ となる. $\sqrt{2}$ と $\sqrt{3}$ への作用を見ることにより

$$\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = \text{id}_L, \quad \sigma_2\sigma_3 = \sigma_3\sigma_2 = \sigma_4, \quad \sigma_2\sigma_4 = \sigma_4\sigma_2 = \sigma_3, \quad \sigma_3\sigma_4 = \sigma_4\sigma_3 = \sigma_2$$

となることが確かめられるので, G はアーベル群であり, 加法群 $(\mathbb{Z}/\mathbb{Z}2) \oplus (\mathbb{Z}/\mathbb{Z}2)$ に同型である. たとえば $\sigma_2 \leftrightarrow (\bar{1}, \bar{0})$, $\sigma_3 \leftrightarrow (\bar{0}, \bar{1})$ と対応させればよい.

	σ_1	σ_2	σ_3	σ_4
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$

問題 6.1 $x^3 - 3$ の $\mathbb{Q}$ 上の分解体のガロア群を求めよ.

問題 6.2 $\mathbb{Q}(i\sqrt{2}, \sqrt{3})$ の $\mathbb{Q}$ 上のガロア群を求めよ.

問題 6.3 $x^4 + 1$ の $\mathbb{Q}$ 上の分解体を L として $G = \text{Gal}(L/\mathbb{Q})$ とおく .

- (1) $i = \sqrt{-1}$ を虚数単位として $\alpha = \frac{1+i}{\sqrt{2}}$ とおくと

$$x^4 + 1 = (x - \alpha)(x - i\alpha)(x + \alpha)(x + i\alpha)$$

が成立し, $L = \mathbb{Q}(\alpha)$ であることを示せ .

- (2) $[L : \mathbb{Q}]$ を求めよ (問題 2.2 を参照) .

- (3) $\sigma(\alpha)$ が $\alpha, i\alpha, -\alpha, -i\alpha$ にそれぞれ等しくなるような $\sigma \in G$ を $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ とする . これらが引き起こす $A = \{\alpha, i\alpha, -\alpha, -i\alpha\}$ の置換を求めよ (ヒント: $\alpha^2 = i$ に注意する) .

- (4) G は S_4 のどのような部分群に同型となるか?

7 ガロア理論の基本定理 (ガロア対応)

定義 7.1 体の拡大 $L \supset K$ に対して, $L \supset F \supset K$ を満たす L の部分体 F のことを拡大 $L \supset K$ の中間体 (intermediate field) という . 特に L と K も中間体である .

たとえば体の拡大 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}$ の中間体は L と $\mathbb{Q}$ 以外に $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$ がある . 例 6.4 の記号を用いると $L \supset \mathbb{Q}$ のガロア群は

$$G := \text{Gal}(L/\mathbb{Q}) = \{\sigma_1 = \text{id}_L, \sigma_2, \sigma_3, \sigma_4\} \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$$

であった . 例 1.6 により L の任意の元 α は $a, b, c, d \in \mathbb{Q}$ によって

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

と一意的に表され, 例 6.4 の表と $\sqrt{6} = \sqrt{2}\sqrt{3}$ より

$$\begin{aligned} \sigma_1(\alpha) &= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, & \sigma_2(\alpha) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}, \\ \sigma_3(\alpha) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}, & \sigma_4(\alpha) &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \end{aligned}$$

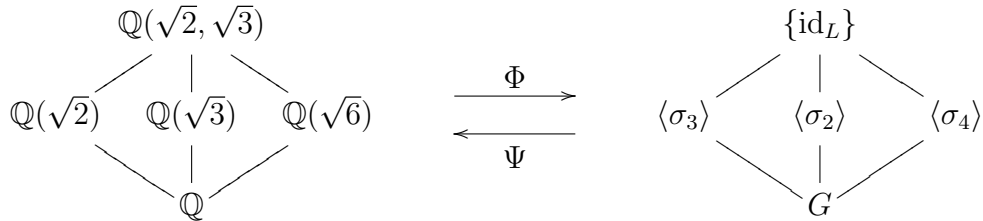
となることに注意すると, $\mathbb{Q}(\sqrt{2})$ は σ_3 で動かないような L の元の集合であり, $\mathbb{Q}(\sqrt{3})$ は σ_2 で動かないような L の元の集合であり, $\mathbb{Q}(\sqrt{6})$ は σ_4 で動かないような L の元の集合であることがわかる . たとえば σ_3 の生成する G の部分群は $H_3 := \langle \sigma_3 \rangle = \{\text{id}_L, \sigma_3\}$ であるから, $\mathbb{Q}(\sqrt{2})$ は H_3 のすべての元で動かないような L の元の集合である . すなわち

$$\mathbb{Q}(\sqrt{2}) = \{\alpha \in L \mid \sigma(\alpha) = \alpha \quad (\forall \sigma \in H_3)\}$$

が成立する . 逆に, $\mathbb{Q}(\sqrt{2})$ のすべての元を固定するような G の元の全体が H_3 である . すなわち

$$H_3 = \{\sigma \in G \mid \sigma(\alpha) = \alpha \quad (\forall \alpha \in \mathbb{Q}(\sqrt{2}))\}$$

が成立する． G の位数は 4 であるから， $\{\text{id}_L\}$ と G 以外の G の部分群は位数 2 であり， $\langle \sigma_2 \rangle, \langle \sigma_3 \rangle, \langle \sigma_4 \rangle$ のいずれかである．このように，拡大 $L \supset \mathbb{Q}$ の中間体とガロア群 G の部分群が 1 対 1 に対応している (定理 7.1)．これをガロア対応という．下の図の左は中間体の包含関係 (上が大きい) を表し，右は G の部分群の包含関係 (下が大きい) を表している．



なお， G はアーベル群であるから，部分群はすべて正規部分群である．これは $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$ がすべて $\mathbb{Q}$ のガロア拡大であることに対応している (定理 7.2)．

さて，一般に $L \supset K$ をガロア拡大として， F をその中間体とする． $G := \text{Gal}(L/K)$ の部分集合 H を

$$H = \{\sigma \in G \mid \sigma(\alpha) = \alpha \quad (\forall \alpha \in F)\}$$

で定義する． H は G の部分群である．実際， id_L は H に属し， $\sigma, \tau \in H$ ならば任意の $\alpha \in F$ に対して $(\sigma \circ \tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \alpha$, $\sigma^{-1}(\alpha) = \alpha$ が成立するから， $\sigma \circ \tau$ と σ^{-1} も H に属する．

このとき， $L \supset F$ はガロア拡大であって， $H = \text{Gal}(L/F)$ が成立する．実際， L はある $f \in K[x]$ の K 上の分解体であるから， f の根を $\alpha_1, \dots, \alpha_n$ とすれば

$$L = K(\alpha_1, \dots, \alpha_n)$$

であるが， $\alpha_1, \dots, \alpha_n \in L$ と $K \subset F \subset L$ より

$$L = K(\alpha_1, \dots, \alpha_n) \subset F(\alpha_1, \dots, \alpha_n) \subset L$$

となるから， $L = F(\alpha_1, \dots, \alpha_n)$ は f の F 上の分解体である． $\text{Gal}(L/F)$ は L から L への K 上の体準同型のうち F のすべての元を固定するものの全体であるから， H と一致する．そこで写像 Φ を

$$\Phi : \{L \supset K \text{ の中間体} \} \ni F \longmapsto \Phi(F) = \text{Gal}(L/F) \in \{G \text{ の部分群} \}$$

によって定義する．特に $\Phi(K) = G$ である．

逆に G の部分群 H に対して L の部分集合 F を

$$F = L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha \quad (\forall \sigma \in H)\}$$

で定義して H の固定体 (fixed field) または不変体と呼ぶ． $K \subset F \subset L$ であり，任意の $\sigma \in H$ と $\alpha, \beta \in F$ に対して

$$\begin{aligned} \sigma(\alpha \pm \beta) &= \sigma(\alpha) \pm \sigma(\beta) = \alpha \pm \beta, & \sigma(\alpha\beta) &= \sigma(\alpha)\sigma(\beta) = \alpha\beta, \\ \sigma(\alpha/\beta) &= \sigma(\alpha)/\sigma(\beta) = \alpha/\beta \quad (\beta \neq 0) \end{aligned}$$

が成立するから, $\alpha + \beta, \alpha\beta, \alpha/\beta$ も F に属する. よって F は $L \supset K$ の中間体である. そこで, 写像 $\Psi(H)$ を

$$\Psi: \{G \text{ の部分群} \} \ni H \mapsto \Psi(H) = L^H \in \{L \supset K \text{ の中間体} \}$$

と定義する. 定義より $\Psi(\{\text{id}_L\}) = L$ である.

以下では, この2つの写像 Φ と Ψ が互いに逆写像になっていることを示す. Φ と Ψ によるガロア拡大の中間体とガロア群の部分群との対応をガロア対応という.

命題 7.1 $L \supset K$ を有限次拡大, $\sigma: K \rightarrow \mathbb{C}$ を体準同型とする. このとき, 体準同型 $\tilde{\sigma}: L \rightarrow \mathbb{C}$ であって, 任意の $a \in K$ に対して $\tilde{\sigma}(a) = \sigma(a)$ を満たすものが存在する. この $\tilde{\sigma}$ を σ の L への拡張 (extension) という.

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\sigma}} & \mathbb{C} \\ | & \nearrow \sigma & \\ K & & \end{array}$$

証明: 定理 3.2 によって, K 上代数的な $\alpha \in L$ が存在して $L = K(\alpha)$ となる. α の K 上の最小多項式を $f_\alpha(x)$ とする. $\sigma: K \rightarrow \sigma(K)$ は体同型であるから, 環同型 $\sigma: K[x] \rightarrow \sigma(K)[x]$ を引き起こす. よって, $\sigma(f_\alpha)$ は $\sigma(K)[x]$ の既約元である. $\sigma(f_\alpha)$ の $\mathbb{C}$ における根の1つを β とすると, $\sigma(f_\alpha)$ は β の $\sigma(K)$ 上の最小多項式である. 従って定理 1.1 により2つの体同型

$$\varphi: K[x]/K[x]f_\alpha \xrightarrow{\sim} K(\alpha), \quad \varphi': \sigma(K)[x]/\sigma(K)[x]\sigma(f_\alpha) \xrightarrow{\sim} \sigma(K)(\beta)$$

が存在する. 一方 σ は体同型

$$\bar{\sigma}: K[x]/K[x]f_\alpha \xrightarrow{\sim} \sigma(K)[x]/\sigma(K)[x]\sigma(f_\alpha)$$

を引き起こす. $\tilde{\sigma} := \varphi' \circ \bar{\sigma} \circ \varphi^{-1}$ は $K(\alpha)$ から $\sigma(K)(\beta)$ への体同型である. $g(x) \in K[x]$ の $K[x]/K[x]f_\alpha$ における同値類を $[g(x)]$ と書くと $\varphi([g(x)]) = g(\alpha)$ であつたから, 特に $a \in K$ を定数多項式とみなせば $\varphi([a]) = a$ である. φ' についても同様だから, 任意の $a \in K$ に対して

$$\tilde{\sigma}(a) = \varphi'(\bar{\sigma}(\varphi^{-1}(a))) = \varphi'(\bar{\sigma}([a])) = \varphi'([\sigma(a)]) = \sigma(a)$$

が成立する. $\tilde{\sigma}$ を $K(\alpha)$ から $\mathbb{C}$ への体準同型とみなせばよい. $\square$

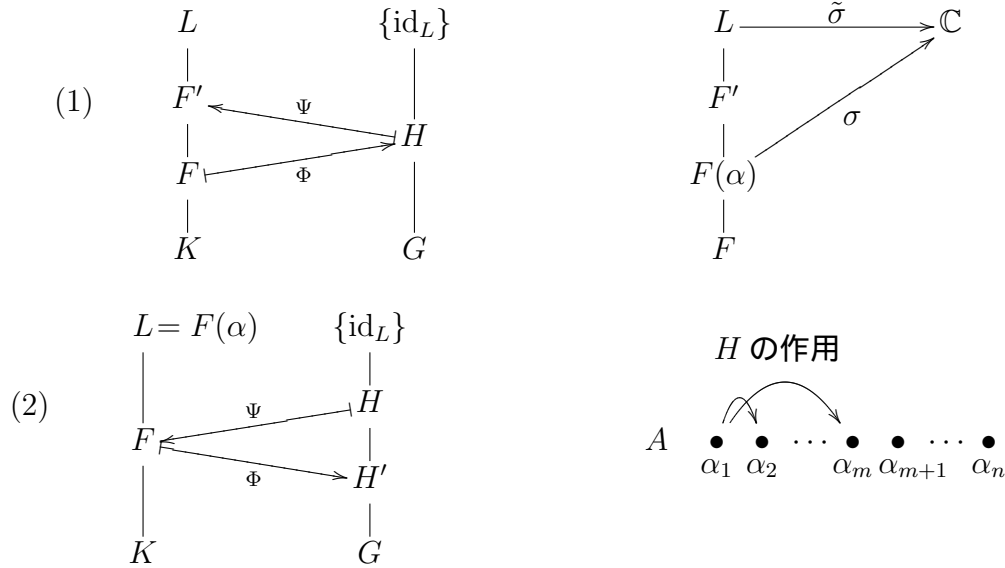
定理 7.1 $L \supset K$ をガロア拡大とすると Φ と Ψ は全単射であり互いに逆写像である.

証明: (1) F を拡大 $L \supset K$ の中間体, $H = \Phi(F)$ とするとき, $\Psi(H) = F$ であることを示す.

$$F' := \Psi(H) = L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha \quad (\forall \sigma \in H)\}$$

は体の拡大 $L \supset K$ の中間体である. H の定義より任意の $\alpha \in F$ と任意の $\sigma \in H$ について $\sigma(\alpha) = \alpha$ であるから, $F \subset F'$ が成り立つ. $F' \neq F$ と仮定して, $\alpha \in F' \setminus F$ とすると,

$F' \supset F(\alpha) \not\subseteq F$ である. α は F 上代数的であり F には属さないから, α の F 上の最小多項式 $f_\alpha(x)$ の次数 n は 2 以上である. $f_\alpha(x)$ の根を $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ とすると, 定理 4.1 によって, F 上の体準同型 $\sigma : F(\alpha) \rightarrow \mathbb{C}$ であって $\sigma(\alpha) = \alpha_2 \neq \alpha$ を満たすものが存在する. 命題 7.1 により σ の L への拡張 $\tilde{\sigma}$ が存在する. $L \supset K$ はガロア拡大であるから, $\tilde{\sigma}$ は L の K 上の自己同型, すなわち $G = \text{Gal}(L/K)$ の元であるが, σ が F 上の体準同型であったから, $\tilde{\sigma}$ は F の元を固定する. すなわち $\tilde{\sigma} \in H$ である. $\tilde{\sigma}(\alpha) = \sigma(\alpha) \neq \alpha$ より $\alpha \notin \Psi(H) = F'$ となるが, これは $\alpha \in F'$ に矛盾する. 以上により $\Psi(H) = F' = F$ であることが示された.



(2) H を $G = \text{Gal}(L/K)$ の部分群, $F = \Psi(H)$ とするとき, $\Phi(F) = H$ であることを示す. $H' = \Phi(F) = \{\sigma \in G \mid \sigma(\alpha) = \alpha \ (\forall \alpha \in F)\} = \text{Gal}(L/F)$ とおくと, F の定義より $H \subset H'$ である. 定理 3.2 により, F 上代数的な元 $\alpha \in L$ があって $L = F(\alpha)$ が成立する. α の F 上の最小多項式を $f_\alpha(x)$ として, その根を $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ とする (これらは命題 3.1 により相異なる.) 定理 6.2 により

$$|H'| = |\text{Gal}(L/F)| = [L : F] = \deg f_\alpha = n$$

が成立する. 定理 6.1 により L は f の F 上の分解体であり, $\alpha_1, \dots, \alpha_n$ は L に属する. 従って命題 6.2 により, H' の任意の元 σ は集合 $A := \{\alpha_1, \dots, \alpha_n\}$ の置換を引き起こす. 定理 6.1 により, H' は A に推移的に作用している. すなわち, 任意の $j = 1, \dots, n$ に対して $\sigma_j(\alpha) = \alpha_j$ を満たすような $\sigma_j \in H'$ が存在する.

以下では H' の部分群 H も A に推移的に作用していることを示す. $\alpha_2, \dots, \alpha_n$ を並べ替えて

$$B := O(\alpha) = \{\sigma(\alpha) \mid \sigma \in H\} = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$$

とする ($1 \leq m \leq n$). (B は H の A における軌道と呼ばれる.) そして

$$g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) = x^m + c_1 x^{m-1} + \cdots + c_m \quad (c_1, \dots, c_m \in L)$$

とおく. $\sigma \in H$ は B の置換を引き起こすから,

$$\begin{aligned}\sigma(g)(x) &= x^m + \sigma(c_1)x^{m-1} + \cdots + \sigma(c_m) = (x - \sigma(\alpha_1)) \cdots (x - \sigma(\alpha_m)) \\ &= (x - \alpha_1) \cdots (x - \alpha_m) = x^m + c_1x^{m-1} + \cdots + c_m = g(x)\end{aligned}$$

が成立する. 従って $c_1, \dots, c_m$ は任意の $\sigma \in H$ で固定されるから $F = \Psi(H)$ に属する. よって $g(x) \in F[x]$ かつ $g(\alpha) = 0$ が成立する. $\deg g(x) = m \leq n = \deg f_\alpha(x)$ であるから, 最小多項式の定義によって $g(x) = f_\alpha(x)$, すなわち $m = n$ でなければならない. これは, $B = A$, すなわち任意の $j = 1, \dots, n$ に対して, $\sigma_j(\alpha) = \alpha_j$ を満たす $\sigma_j \in H$ が存在することを意味する. 従って H は少なくとも n 個の元を持ち, $|H| \geq n = |H'|$ が成立する. これと $H \subset H'$ より $H' = H$ が従う. $\square$

命題 7.2 体の有限次拡大 $L \supset K$ について次の 2 つの条件は同値である.

- (1) $L \supset K$ はガロア拡大である.
- (2) L から $\mathbb{C}$ への K 上の任意の体準同型 $\sigma: L \rightarrow \mathbb{C}$ に対して $\sigma(L) \subset L$ が成立する.

証明: (1) を仮定すれば $\sigma(L) = L$ であることは命題 6.1 で示した. (2) を仮定する. 定理 3.2 により $L = K(\alpha)$ となるような $\alpha \in L$ が存在する. α の K 上の最小多項式を $f_\alpha(x) \in K[x]$ とすると, $\mathbb{C}[x]$ において

$$f_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n) \quad (\alpha = \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C})$$

と既約分解され, $\alpha_1, \dots, \alpha_n$ は相異なる. 定理 4.1 により, 各 $j = 1, \dots, n$ に対して $\sigma_j(\alpha) = \alpha_j$ を満たす K 上の体準同型

$$\sigma_j: L = K(\alpha) \longrightarrow \mathbb{C}$$

が存在する. 仮定より $\sigma_j(L) \subset L$ であるから, $\alpha_j = \sigma_j(\alpha) \in L$ となる. 従って

$$L = K(\alpha) = K(\alpha)(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_n)$$

が成立するから L は $f(x)$ の K 上の分解体であり, 従って $L \supset K$ はガロア拡大である. $\square$

定理 7.2 $L \supset K$ をガロア拡大とする.

- (1) F_1 と F_2 を拡大 $L \supset K$ の 2 つの中間体とすると,

$$F_1 \subset F_2 \quad \Leftrightarrow \quad \Phi(F_1) \supset \Phi(F_2)$$

- (2) F を $L \supset K$ の中間体とすると, $[F:K] = \frac{|\text{Gal}(L/K)|}{|\text{Gal}(L/F)|}$

- (3) F を $L \supset K$ の中間体とするとき, $F \supset K$ がガロア拡大であるための必要十分条件は, $\text{Gal}(L/F)$ が $\text{Gal}(L/K)$ の正規部分群となることである. このとき, $\text{Gal}(F/K)$ と $\text{Gal}(L/K)/\text{Gal}(L/F)$ は群として同型である.

証明: (1) $F_1 \subset F_2$ なら定義より明らかに $\Phi(F_1) \supset \Phi(F_2)$ である. 逆に $\Phi(F_1) \supset \Phi(F_2)$ ならば, 定義と定理 7.1 より

$$F_1 = \Psi(\Phi(F_1)) \subset \Psi(\Phi(F_2)) = F_2$$

(2) 定理 6.2 と定理 1.2 により

$$\frac{|\text{Gal}(L/K)|}{|\text{Gal}(L/F)|} = \frac{[L:K]}{[L:F]} = \frac{[L:F][F:K]}{[L:F]} = [F:K]$$

(3) $F \supset K$ はガロア拡大であると仮定して $G = \text{Gal}(L/K)$, $H = \text{Gal}(L/F)$ とおく. $\sigma \in H$ と $\tau \in G$ を任意にとる. 命題 6.1 により, τ の F への制限 $\tau|_F$ は F の K 上の自己同型である. σ は F の元を固定するから,

$$(\tau^{-1} \circ \sigma \circ \tau)(\alpha) = \tau^{-1}(\sigma(\tau(\alpha))) = \tau^{-1}(\tau(\alpha)) = \alpha \quad (\forall \alpha \in F)$$

が成立する ($\tau(\alpha) \in F$ であることを用いた.) 従って $\tau^{-1} \circ \sigma \circ \tau \in H$ となるから, H は G の正規部分群である.

逆に, H が G の正規部分群であると仮定する. $\sigma: F \rightarrow \mathbb{C}$ を K 上の体準同型とする. 命題 7.1 によって, K 上の体準同型 $\tilde{\sigma}: L \rightarrow \mathbb{C}$ であって $\tilde{\sigma}|_F = \sigma$ を満たすものが存在する. $L \supset F$ はガロア拡大だから命題 7.2 より $\tilde{\sigma}$ は G の元とみなせる.

α を F の任意の元, τ を H の任意の元とする. H は正規部分群であるから $\tilde{\sigma}^{-1} \circ \tau \circ \tilde{\sigma}$ も H に属し $F = L^H$ より

$$(\tilde{\sigma}^{-1} \circ \tau \circ \tilde{\sigma})(\alpha) = \alpha$$

となる. また $\alpha \in F$ より $\tilde{\sigma}(\alpha) = \sigma(\alpha)$ である. 従って

$$\tau(\sigma(\alpha)) = \tau(\tilde{\sigma}(\alpha)) = (\tau \circ \tilde{\sigma})(\alpha) = (\tilde{\sigma} \circ (\tilde{\sigma}^{-1} \circ \tau \circ \tilde{\sigma}))(\alpha) = \tilde{\sigma}(\alpha) = \sigma(\alpha)$$

が成立する. $\tau \in H$ は任意だったから $\sigma(\alpha)$ は $F = L^H$ に属する. これで $\sigma(F) \subset F$ が示されたから, 命題 7.2 によって $F \supset K$ はガロア拡大である.

$F \supset K$ がガロア拡大であると仮定する. このとき群準同型

$$h: \text{Gal}(L/K) \ni \sigma \mapsto h(\sigma) = \sigma|_F \in \text{Gal}(F/K)$$

が定義される. 実際, $F \supset K$ がガロア拡大であるから, $\sigma(F) = F$ となり, $\sigma|_F \in \text{Gal}(F/K)$ である. 命題 7.1 と定理 6.1 より h は全射であることがわかる. h の核は

$$\text{Ker } h = \{\sigma \in \text{Gal}(L/K) \mid \sigma|_F = \text{id}_F\} = \text{Gal}(L/F) = H$$

であるから, 群準同型定理より h は群同型 $\bar{h}: \text{Gal}(L/K)/\text{Gal}(L/F) \rightarrow \text{Gal}(F/K)$ を引き起こす. $\square$

以上の定理 7.1 と定理 7.2 を合わせてガロア理論の基本定理という.

例 7.1 $f(x) = x^3 - 2$ の $\mathbb{Q}$ 上の分解体 L のガロア群 $G = \text{Gal}(L/\mathbb{Q})$ とガロア対応を考察しよう.

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2), \quad \omega = \frac{-1 + \sqrt{3}i}{2}$$

より, $f(x)$ の分解体は

$$L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

である. ガロア群 $G := \text{Gal}(L/\mathbb{Q})$ の元は

$$A = \{\alpha_1 = \sqrt[3]{2}, \alpha_2 = \sqrt[3]{2}\omega, \alpha_3 = \sqrt[3]{2}\omega^2\}$$

の置換を引き起こし G は S_3 の部分群とみなせるが, $|G| = [L : \mathbb{Q}] = 6$ より $G = S_3$ であった (例 3.2).

補題 6.2 により, G の元 σ は $f(x) = x^3 - 2$ の根の集合と $g(x) = x^2 + x + 1$ の根の集合をそれぞれ置換する. $g(x) = (x - \omega)(x - \omega^2)$ であることがわかるので, $\sigma(\sqrt[3]{2})$ は $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ のいずれかであり, $\sigma(\omega)$ は ω または ω^2 のいずれかでなければならない. σ の A への作用は $\sigma(\sqrt[3]{2})$ と $\sigma(\omega)$ から一意的に定まるから, σ の可能性は高々 $3 \times 2 = 6$ 通りであるが, $|G| = 6$ であるから, G はこの 6 通りの σ からなる. 従って G の元 σ と τ であって

$$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega, \quad \sigma(\omega) = \omega, \quad \tau(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\omega) = \omega^2$$

を満たすものが存在して,

$$G = \{\text{id}_L, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

となることがわかる (これらが上記の 6 通りの可能性に対応するから). これらは ω と A の元を下の表のようにうつす. ($\sqrt[3]{2}\omega$ と $\sqrt[3]{2}\omega^2$ への作用は $\sqrt[3]{2}$ と ω への作用から求まる.)

	id_L	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
ω	ω	ω	ω	ω^2	ω^2	ω^2
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$
$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$

この表から, G の元を A への作用によって S_3 の元と同一視すると,

$$\sigma = (1\ 2\ 3), \quad \sigma^2 = (3\ 2\ 1), \quad \tau = (2\ 3), \quad \sigma\tau = (1\ 2), \quad \sigma^2\tau = (1\ 3)$$

となることがわかる.

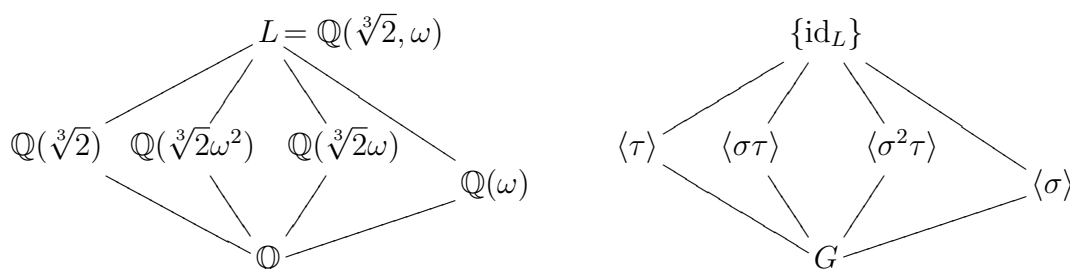
S_3 の部分群は S_3 と $\{\text{id}\}$ 以外は位数が 2 または 3 だから巡回群となり,

$$H_1 = \langle \tau \rangle = \{\text{id}_L, \tau\}, \quad H_2 = \langle \sigma\tau \rangle = \{\text{id}_L, \sigma\tau\}, \quad H_3 = \langle \sigma^2\tau \rangle = \{\text{id}_L, \sigma^2\tau\}, \\ A_3 = \langle \sigma \rangle = \{\text{id}_L, \sigma, \sigma^2\}$$

の4つである．このうち A_3 のみが正規部分群である (S_3 の3次の巡回置換は σ と σ^2 のみだから)．各々の部分群に対応する固定体は

$$L^{H_1} = \mathbb{Q}(\sqrt[3]{2}), \quad L^{H_2} = \mathbb{Q}(\sqrt[3]{2}\omega^2), \quad L^{H_3} = \mathbb{Q}(\sqrt[3]{2}\omega), \quad L^{A_3} = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$$

である．実際, H_1 については, $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ より $\mathbb{Q}(\sqrt[3]{2}) \subset L^{H_1}$ であり, $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $f(x)$ なので $[\mathbb{Q}(\sqrt[3]{2}\omega^2) : \mathbb{Q}] = 3$ であるが, 一方定理 7.2 より $[L^{H_1} : \mathbb{Q}] = |G|/|H_1| = 3$ であるから, $L^{H_1} = \mathbb{Q}(\sqrt[3]{2})$ が成立する．また, A_3 については, $\sigma(\omega) = \omega$ より $\mathbb{Q}(\omega) \subset L^{A_3}$ であるが, $[\mathbb{Q}[\omega] : \mathbb{Q}] = 2$ と $[L^{A_3}] = |G|/|A_3| = 2$ より $L^{A_3} = \mathbb{Q}(\omega)$ が成立する．なお, 以上のことは $1, \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2, \omega, \sqrt[3]{4}\omega, \sqrt[3]{4}\omega^2$ が $\mathbb{Q}(\sqrt[3]{2}, \omega)$ の $\mathbb{Q}$ 上の基底であることを用いて直接示すこともできる．中間体のうち $\mathbb{Q}$ 上のガロア拡大になるものは, $\mathbb{Q}, L$ と $\mathbb{Q}(\omega)$ である．



問題 7.1 $L = \mathbb{Q}(i\sqrt{2}, \sqrt{3})$ の $\mathbb{Q}$ 上のガロア群 $G = \text{Gal}(L/\mathbb{Q})$ のすべての部分群を求め, 対応する中間体を求めよ．また中間体の包含関係を図式で表せ．

問題 7.2 $x^3 - 3$ の $\mathbb{Q}$ 上の分解体 L のガロア群 $G = \text{Gal}(L/\mathbb{Q})$ のすべての部分群を求め, 対応する中間体を求めよ．中間体の包含関係を図式で表せ．また正規部分群をすべて求めよ．

問題 7.3 $x^4 + 1$ の $\mathbb{Q}$ 上の分解体 L のガロア群 $G = \text{Gal}(L/\mathbb{Q})$ のすべての部分群を求め, 対応する中間体を求めよ．また中間体の包含関係を図式で表せ．

問題 7.4 $x^4 - 2$ の $\mathbb{Q}$ 上の分解体 L のガロア群 $G = \text{Gal}(L/\mathbb{Q})$ とその部分群を次の方針で求めよ．

- (1) $L = \mathbb{Q}(\sqrt[4]{2}, i)$ となることを示せ (i は虚数単位)．
- (2) 拡大次数 $[L : \mathbb{Q}]$ を求めよ．
- (3) $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\sigma(i) = i$, $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$, $\tau(i) = -i$ を満たす $\sigma, \tau \in G$ が存在することを示せ．
- (4) $x^4 - 2$ の根の集合を A とする． G の元が引き起こす A の置換によって G を S_4 の部分群とみなしたとき, G に対応する置換を列挙せよ．また, それらを σ と τ を用いて表せ．
- (5) (難) G のすべての部分群を求めよ．それらのうち正規部分群になるのはどれか?
- (6) (難) G の各々の部分群に対応する $L \supset K$ の中間体を求め, それらの包含関係を図式で表せ．

8 1 の n 乗根

K を $\mathbb{C}$ の部分体, n を 2 以上の自然数として $x^n - 1$ の K 上の分解体 L のガロア群 $\text{Gal}(L/K)$ について考察しよう. $z = r(\cos \theta + i \sin \theta) \in \mathbb{C}$ ($r > 0, \theta \in \mathbb{R}$) とおくと, de Moivre の定理により

$$z^n = r^n(\cos n\theta + i \sin n\theta) = 1 \quad \Leftrightarrow \quad (r = 1, \quad n\theta = 2k\pi \quad (\exists k \in \mathbb{Z}))$$

であるから, $z^n = 1$ を満たす複素数は

$$\zeta_k := \exp\left(\frac{2k\pi i}{n}\right) = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \quad (k = 0, 1, \dots, n-1)$$

の n 個である. これらを 1 の n 乗根という. $\zeta = \zeta_1$ とおけば $\zeta_k = \zeta^k$ であるから, 1 の n 乗根は $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ である. 従って $\mathbb{C}[x]$ において

$$x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1})$$

と既約分解されるから, $x^n - 1$ の K 上の分解体は $L = K(\zeta)$ であり $K(\zeta) \supset K$ はガロア拡大である. 特に $K = \mathbb{Q}$ のとき $\mathbb{Q}(\zeta)$ を n 次の円分体 (cyclotomic field) と呼ぶ. 1 の n 乗根の全体 $U_n := \{\zeta^k \mid k = 0, 1, \dots, n-1\}$ は複素数の乗法に関して巡回群をなす.

命題 8.1 n を自然数とする. $\zeta = \exp\left(\frac{2\pi i}{n}\right)$ として $U_n := \{\zeta^k \mid k = 0, 1, \dots, n-1\}$ とおく. このとき, 整数 m に関する次の 3 つの条件は同値である.

- (1) ζ^m の位数は n である.
- (2) ζ^m は U_n を生成する.
- (3) m と n は互いに素である.

m がこの条件を満たすとき, ζ^m のことを 1 の原始 n 乗根という.

証明: (1) $\Leftrightarrow$ (2) の証明: ζ^m の位数を k とすると, ζ^m の生成する U_n の部分群

$$\langle \zeta^m \rangle = \{1, \zeta^{2m}, \dots, \zeta^{(k-1)m}\}$$

の位数は k である. 従って, $\langle \zeta^m \rangle$ が U_n と一致するための必要十分条件は $k = n$ である.

(2) $\Leftrightarrow$ (3) の証明: $\zeta^n = 1$ であり, $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ は互いに異なるから, U_n の定義より U_n は ζ で生成される巡回群である. 従って, ζ^m が U_n を生成するための必要十分条件は $(\zeta^m)^k = \zeta^{mk} = \zeta$ をみたす整数 k が存在することである.

$$\zeta^{mk} = \zeta \quad \Leftrightarrow \quad \zeta^{mk-1} = 1 \quad \Leftrightarrow \quad mk \equiv 1 \pmod{n}$$

が成立する. $mk \equiv 1 \pmod{n}$ とすると, $mk - 1 = ln$ をみたす整数 l が存在する. p が n と m の公約数であるとすると, $1 = mk - ln$ は p の倍数であるから, $p = \pm 1$ でなければならない. 従って m と n は互いに素である.

逆に m と n が互いに素であると仮定すると, $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}$ であるから, $1 = mk - ln$ を満たす整数 k, l が存在する. 従って $mk \equiv 1 \pmod{n}$ である. $\square$

ζ を 1 の原始 n 乗根とすれば $x^n - 1$ の体 K 上の分解体は $K(\zeta)$ である.

定義 8.1 自然数 n に対して $1, \dots, n-1$ のうち n と互いに素であるものの個数を $\phi(n)$ で表し, ϕ をオイラー (Euler) 関数という.

自然数 n に対して, 加法群 $\mathbb{Z}$ の剰余群 $\mathbb{Z}/\mathbb{Z}n = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$ の単元 (= 可逆元) の全体を $(\mathbb{Z}/\mathbb{Z}n)^\times$ (または $(\mathbb{Z}/\mathbb{Z}n)^*$) で表す. $(\mathbb{Z}/\mathbb{Z}n)^\times$ は乗法について群をなす.

補題 8.1 $(\mathbb{Z}/\mathbb{Z}n)^\times$ の位数 (元の個数) は $\phi(n)$ である.

証明: 命題 8.1 の証明より, 整数 m に対して整数 k が存在して $\mathbb{Z}/\mathbb{Z}n$ において $\overline{m}k = \overline{1}$ が成り立つための必要十分条件は, m と n が互いに素であることである. 従って $(\mathbb{Z}/\mathbb{Z}n)^\times$ の位数は $\phi(n)$ に等しい. $\square$

定理 8.1 K を $\mathbb{C}$ の部分体, L を $x^n - 1$ の K 上の分解体とすると, ガロア群 $G = \text{Gal}(L/K)$ は $(\mathbb{Z}/\mathbb{Z}n)^\times$ の部分群に同型である. 従って G はアーベル群であり, 位数は $\phi(n)$ の約数である.

証明: 命題 8.1 より $x^n - 1$ の K 上の最小分解体 L は 1 の任意の原始 n 乗根 ζ で生成される. すなわち, $L = K(\zeta)$ である. $\sigma \in G := \text{Gal}(L/K)$ とすると, $\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$ であり, 自然数 k に対して, $\sigma(\zeta)^k = \sigma(\zeta^k) = 1$ と $\zeta^k = 1$ は同値であるから, $\sigma(\zeta)$ も 1 の原始 n 乗根である. 従って n と互いに素な整数 $j(\sigma) \in \{1, \dots, n-1\}$ によって $\sigma(\zeta) = \zeta^{j(\sigma)}$ と表される. $\sigma, \tau \in G$ に対して

$$\zeta^{j(\tau\sigma)} = (\tau\sigma)(\zeta) = (\tau(\sigma(\zeta))) = \tau(\zeta^{j(\sigma)}) = (\tau(\zeta))^{j(\sigma)} = (\zeta^{j(\tau)})^{j(\sigma)} = \zeta^{j(\tau)j(\sigma)}$$

より $j(\tau\sigma) \equiv j(\tau)j(\sigma) \pmod{n}$ が成立するから, $G \ni \sigma \mapsto \overline{j(\sigma)} \in (\mathbb{Z}/\mathbb{Z}n)^\times$ は群準同型である. $\sigma(\zeta^k) = \sigma(\zeta)^k$ より σ の定める U_n の置換は $\sigma(\zeta)$ のみから定まる. さらに, 命題 6.2 により G の元は U_n の置換によって一意的に定まるから, この準同型 $G \ni \sigma \mapsto \overline{j(\sigma)} \in (\mathbb{Z}/\mathbb{Z}n)^\times$ は単射である. よって G は $(\mathbb{Z}/\mathbb{Z}n)^\times$ の部分群に同型である. $\square$

例 8.1 (3 次の円分体) $\omega := \frac{-1 + \sqrt{-3}}{2}$ とおくと, $x^3 - 1$ の $\mathbb{Q}$ 上の分解体は $L = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ であるから $|\text{Gal}(L/\mathbb{Q})| = 2$ である. 一方 $\phi(3) = 2$ だから定理 8.1 により $G \cong (\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ (加法群) となり, G は位数 2 の巡回群である.

例 8.2 (5 次の円分体) $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ と分解され, $g(x) = x^4 + x^3 + x^2 + x + 1$ は $\mathbb{Q}$ 上既約である ($g(x+1)$ に Eisenstein の判定法を適用). $\zeta = \exp\left(\frac{2\pi i}{5}\right)$ は $\zeta^5 - 1 = 0$ かつ $\zeta - 1 \neq 0$ より $g(\zeta) = 0$ を満たす. 従って $x^5 - 1$ の $\mathbb{Q}$ 上の分解体を L とすると $L = \mathbb{Q}(\zeta)$ であり $[L : \mathbb{Q}] = \deg g = 4$ となる. これと $\phi(5) = 4$ から $G = \text{Gal}(L/\mathbb{Q})$ は $(\mathbb{Z}/5\mathbb{Z})^\times$ に同型である. これは 4 次の巡回群であることが容易に確認できる.

問題 8.1 (1) 4 次の円分体 ($x^4 - 1$ の $\mathbb{Q}$ 上の分解体) のガロア群を求めよ.

(2) 6 次の円分体のガロア群を求めよ .

問題 8.2 (1) $x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ は $\mathbb{Q}$ 上の既約分解であることを示せ .

(2) 7 次の円分体のガロア群を求め , 巡回群になるかどうか判定せよ .

問題 8.3 8 次の円分体のガロア群を求め , 巡回群になるかどうか判定せよ .

9 2項方程式と巡回拡大

ここでは , 2 項方程式 $x^n - a = 0$ について考察する . この根は a の n 乗根である .

定理 9.1 K は $\mathbb{C}$ の部分体であり , 1 の原始 n 乗根を含む , すなわち $\mathbb{Q}$ 上の $x^n - 1$ の分解体を含むと仮定する . a を 0 でない K の元として , $x^n - a$ の K 上の分解体を L とする . このとき , $L \supset K$ のガロア群 $G = \text{Gal}(L/K)$ は巡回群であり , その位数は n の約数である . 特に $x^n - a$ が K 上既約であれば , G は n 次巡回群である .

証明: $\alpha^n = a$ を満たす複素数 α を 1 つとり固定する . ζ を 1 の原始 n 乗根の 1 つとすると , $k = 0, 1, \dots, n-1$ に対して $(\alpha\zeta^k)^n = a$ であり $\alpha\zeta^k$ は相異なるから , これらが $x^n - a$ の根のすべてである . $\zeta \in K$ より , $L = K(\alpha)$ となる . $\sigma \in G(L/K)$ とすると , ある $j(\sigma) \in \{0, 1, \dots, n-1\}$ があって , $\sigma(\alpha) = \alpha\zeta^{j(\sigma)}$ となる . σ は $\sigma(\alpha)$ で定まるから , $j(\sigma)$ を $\mathbb{Z}/n\mathbb{Z}$ の元とみなすと , 写像

$$\psi : \text{Gal}(L/K) \ni \sigma \longmapsto j(\sigma) \in \mathbb{Z}/n\mathbb{Z}$$

は単射である . $\sigma, \tau \in \text{Gal}(L/K)$ に対して $\zeta \in K$ より

$$\tau(\sigma(\alpha)) = \tau(\alpha\zeta^{j(\sigma)}) = \tau(\alpha)\zeta^{j(\sigma)} = \alpha\zeta^{j(\tau)}\zeta^{j(\sigma)} = \alpha\zeta^{j(\sigma)+j(\tau)}$$

が成立するから ψ は $G := \text{Gal}(L/K)$ から加法群 $\mathbb{Z}/n\mathbb{Z}$ への単射群準同型である . 従って G は巡回群 $\mathbb{Z}/n\mathbb{Z}$ の部分群とみなせる . 巡回群の部分群はまた巡回群であるから , G は巡回群であり , $|G|$ は n の約数である . $x^n - a$ が $\mathbb{Q}$ 上既約であれば , $x^n - a$ は α の K 上の最小多項式であるから , $|G| = [L : K] = [K(\alpha) : K] = n$ であり , G は $\mathbb{Z}/n\mathbb{Z}$ に同型である . $\square$

ガロア拡大のガロア群が巡回群であるとき巡回拡大 (cyclic extension) という . ガロア群がアーベル群のときアーベル拡大 (abelian extension) という .

例 9.1 3 次の円分体は $\mathbb{Q}(\sqrt{-3})$ であった . $x^3 - 2$ の $\mathbb{Q}(\sqrt{-3})$ 上の分解体を L とする . $L = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ であり , $[L : \mathbb{Q}] = 6$ であったから , $[L : \mathbb{Q}(\sqrt{-3})] = 3$ である . よって $x^3 - 2$ は $\sqrt[3]{2}$ の $\mathbb{Q}(\sqrt{-3})$ 上の最小多項式であり , $\mathbb{Q}(\sqrt{-3})$ 上既約である . 従って $\text{Gal}(L/\mathbb{Q}(\sqrt{-3}))$ は位数 3 だから 3 次の巡回群である . この群は例 7.1 では A_3 に対応する .

例 9.2 4 次の円分体は $\mathbb{Q}(i)$ である. $x^4 - 2$ の $\mathbb{Q}(i)$ 上の分解体は $L = \mathbb{Q}(i, \sqrt[4]{2})$ である.

$$[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2})(i) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \times 4 = 8$$

となることがわかる (なぜか?). よって $[L : \mathbb{Q}(i)] = [L : \mathbb{Q}] / [\mathbb{Q}(i) : \mathbb{Q}] = 4$ であるから, $x^4 - 2$ は $\sqrt[4]{2}$ の $\mathbb{Q}(i)$ 上の最小多項式であり既約である. 従って定理 9.1 により $\text{Gal}(L/\mathbb{Q}(i))$ は 4 次の巡回群である.

定理 9.2 K を $\mathbb{C}$ の部分体とする. $f(x) \in K[x]$ は 0 多項式ではなく, $\mathbb{C}[x]$ における既約分解が重複因子を持たないとすると, 次の (1) と (2) は同値である.

- (1) $f(x)$ は $K[x]$ の既約元である.
- (2) $f(x)$ の K 上の分解体を L とすると $\text{Gal}(L/K)$ は $f(x)$ の根の集合 A に推移的に作用する. すなわち, 任意の $\alpha, \beta \in A$ に対して $\sigma(\alpha) = \beta$ を満たす $\sigma \in \text{Gal}(L/K)$ が存在する.

証明: $f(x)$ の根の集合を $A = \{\alpha_1, \dots, \alpha_n\}$ とする. $G := \text{Gal}(L/K)$ の作用による A の軌道分解を

$$A = A_1 \cup \dots \cup A_m$$

とする. すなわち, $A_1, \dots, A_m$ のどの 2 つも共通元を持たず, G は各 A_j に推移的に作用しているとする. $A_j = \{\alpha_{j,1}, \dots, \alpha_{j,n_j}\}$ として,

$$f_j(x) = (x - \alpha_{j,1}) \cdots (x - \alpha_{j,n_j}) \quad (1 \leq j \leq m)$$

とおく. $\sigma \in G$ は A_j の元の置換を引き起こすから, $\sigma(f_j)(x) = f_j(x)$ である. 従って $f_j(x)$ の係数は G によって固定されるから, 定理 7.1 により K に属する. よって $K[x]$ において $f(x) = f_1(x) \cdots f_m(x)$ と分解される. このとき $f_1(x), \dots, f_m(x)$ は K 上で既約である. 実際たとえば $f_1(x)$ が既約でないとする. $K[x]$ において $f_1(x) = g(x)h(x)$ ($\deg g \geq 1, \deg h \geq 1$) と分解される. $\sigma \in G$ は $g(x)$ の根を $g(x)$ の根にうつし, $f(x)$ が重複因子を持たないことから, $g(x)$ と $h(x)$ は共通根を持たない. よって G は A_1 に推移的には作用しない. これは仮定に反するから $f_1(x)$ は既約である. 以上により $f(x)$ が既約であることと $m = 1$ とが同値であり, $m = 1$ と G の A への作用が推移的であることが同値であるから主張が示された. $\square$

命題 9.1 K を体, $\sigma_1, \dots, \sigma_n$ を K から $\mathbb{C}$ への相異なる体準同型として, $c_1, \dots, c_n \in K$ とすると,

$$c_1\sigma_1(a) + \cdots + c_n\sigma_n(a) = 0 \quad (\forall a \in K) \quad \Leftrightarrow \quad c_1 = \cdots = c_n = 0.$$

証明: n に関する帰納法で示す. $n = 1$ のときは明らかである. $n - 1$ のときは正しいと仮定する. 任意の $a \in K$ に対して $c_1\sigma_1(a) + \cdots + c_n\sigma_n(a) = 0$ が成立し, $c_1 = \cdots = c_n = 0$ ではないと仮定する. すると $c_1, \dots, c_n$ のうち少なくとも 2 つは 0 でないから, たとえば

$c_1 \neq 0$ かつ $c_2 \neq 0$ としてよい. $\sigma_1 \neq \sigma_2$ だから, ある $\gamma \in K$ が存在して $\sigma_1(\gamma) \neq \sigma_2(\gamma)$ となる. $\sigma_1(0) = \sigma_2(0) = 0$ より $\gamma \neq 0$ であることに注意する. このとき, 任意の $a \in K$ に対して

$$0 = c_1\sigma_1(\gamma a) + c_2\sigma_2(\gamma a) + \cdots + c_n\sigma_n(\gamma a) = c_1\sigma_1(\gamma)\sigma_1(a) + c_2\sigma_2(\gamma)\sigma_2(a) + \cdots + c_n\sigma_n(\gamma)\sigma_n(a)$$

$\gamma \neq 0$ より $\sigma_1(\gamma) \neq 0$ だから (体準同型は単射), $\sigma_1(\gamma)$ で割って

$$c_1\sigma_1(a) + c_2\sigma_2(\gamma)\sigma_1(\gamma)^{-1}\sigma_2(a) + \cdots + c_n\sigma_n(\gamma)\sigma_1(\gamma)^{-1}\sigma_n(a) = 0$$

これと $c_1\sigma_1(a) + c_2\sigma_2(a) + \cdots + c_n\sigma_n(a) = 0$ より,

$$c_2(\sigma_2(\gamma)\sigma_1(\gamma)^{-1} - 1)\sigma_2(a) + \cdots + c_n(\sigma_n(\gamma)\sigma_1(\gamma)^{-1} - 1)\sigma_n(a) = 0$$

となる. 帰納法の仮定により, $c_2(\sigma_2(\gamma)\sigma_1(\gamma)^{-1} - 1) = 0$. これと $\sigma_1(\gamma) \neq \sigma_2(\gamma)$ より $c_2 = 0$ となるが, これは仮定に反する. $\square$

定理 9.3 K は $\mathbb{C}$ の部分体であり, ガロア拡大 $L \supset K$ のガロア群 $G := \text{Gal}(L/K)$ が位数 n の巡回群であり, 1 の原始 n 乗根は K に含まれると仮定する. このとき, ある $a \in K$ が存在して, L は $x^n - a$ の分解体と一致する. さらに $x^n - a$ は K 上既約である.

証明: σ を G の生成元 (の 1 つ) とすると仮定より $G = \langle \sigma \rangle = \{\text{id}_L, \sigma, \dots, \sigma^{n-1}\}$ となる. 1 の原始 n 乗根 ζ を 1 つ固定して, 写像 $h: L \rightarrow L$ を

$$h(\alpha) = \alpha + \zeta\sigma(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha) \quad (\forall \alpha \in L)$$

で定義する (h は体準同型とは限らない). $h(\alpha)$ はラグランジュの分解式 (Lagrange resolvent) と呼ばれる. $\text{id}_L, \sigma, \dots, \sigma^{n-1}$ は相異なる L の自己同型だから, 命題 9.1 により h は 0 写像ではない. すなわち, ある $\gamma \in L$ が存在して $h(\gamma) \neq 0$ となる. $\zeta \in K, \zeta^n = 1, \sigma^n = \text{id}_L$ を用いて

$$\zeta\sigma(h(\gamma)) = \zeta\sigma(\gamma) + \zeta^2\sigma^2(\gamma) + \cdots + \zeta^n\sigma^n(\gamma) = \gamma + \zeta\sigma(\gamma) + \cdots + \zeta^{n-1}\sigma^{n-1}(\gamma) = h(\gamma)$$

すなわち $\sigma(h(\gamma)) = \zeta^{-1}h(\gamma)$ を得る. 従って, $\alpha = h(\gamma)^{-1} \in L$ とおけば,

$$\sigma(\alpha) = \sigma(h(\gamma)^{-1}) = \sigma(h(\gamma))^{-1} = (\zeta^{-1}h(\gamma))^{-1} = \zeta h(\gamma)^{-1} = \zeta\alpha$$

が成立する. 従って $a = \alpha^n \in L$ とおけば

$$\sigma(a) = \sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \zeta^n\alpha^n = a$$

を得る. よって $\sigma^j(a) = a$ も成立し $G = \{\text{id}_L, \sigma, \dots, \sigma^{n-1}\}$ であるから, a は G の任意の元で固定される. 定理 7.1 により $L \supset K$ の中間体と G の部分群とのガロア対応において K と G が対応する ($G = \text{Gal}(L/K) = \Phi(K)$ より) から, $K = L^G = \Psi(G)$ であり,

$a \in L^G = K$ 従って $x^n - a \in K[x]$ となる. $\sigma(\alpha) = \zeta\alpha$ と $\sigma(\zeta) = \zeta$ ($\zeta \in K$ だから) より $j = 0, 1, \dots, n-1$ に対して帰納的に

$$\sigma^j(\alpha) = \sigma^{j-1}(\sigma(\alpha)) = \sigma^{j-1}(\zeta\alpha) = \zeta\sigma^{j-1}(\alpha) = \zeta\zeta^{j-1}\alpha = \zeta^j\alpha$$

が成立することがわかるので, G は $x^n - a$ の根の集合 $A = \{\alpha, \zeta\alpha, \dots, \zeta^{n-1}\alpha\}$ に推移的に作用している. 従って定理 9.2 により $x^n - a$ は K 上既約である. よって $x^n - a$ の K 上の分解体 $F := K(\alpha)$ は $[F : K] = n$ を満たす. 一方, $[L : K] = n$ かつ $L \supset F$ だから, $L = F = K(\alpha)$ である. $\square$

問題 9.1 $x^4 + 1$ の $\mathbb{Q}(i)$ 上のガロア群を求めよ.

10 3 次方程式のガロア群と根の公式

K を $\mathbb{C}$ の部分体として, $K[x]$ に属する 3 次多項式 $f(x) = x^3 + a_2x^2 + a_1x + a_0$ ($a_0, a_1, a_2 \in K$) を考察する. $y = x + \frac{1}{3}a_2$ とすれば

$$f(x) = f\left(y - \frac{1}{3}a_2\right) = y^3 + b_1y + b_0 \quad (\exists b_0, b_1 \in K)$$

となるから, 最初から $f(x) = x^3 + ax + b$ ($a, b \in K$) としてよい. $f(x)$ の根を α, β, γ とすると,

$$x^3 + ax + b = (x - \alpha)(x - \beta)(x - \gamma) = x^3 - (\alpha + \beta + \gamma)x^2 + (\beta\gamma + \gamma\alpha + \alpha\beta)x - \alpha\beta\gamma$$

より,

$$\alpha + \beta + \gamma = 0, \quad \beta\gamma + \gamma\alpha + \alpha\beta = a, \quad \alpha\beta\gamma = -b$$

を得る (根と係数の関係). このとき,

$$\Delta := (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma), \quad D(f) := \Delta^2$$

とおき, Δ を α, β, γ の差積, $D(f)$ を $f(x)$ の判別式 (discriminant) という. $\alpha + \beta + \gamma = 0$ より,

$$\begin{aligned} D(f) &= (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = \{(\alpha + \beta)^2 - 4\alpha\beta\}\{(\beta + \gamma)^2 - 4\beta\gamma\}\{(\alpha + \gamma)^2 - 4\alpha\gamma\} \\ &= (\gamma^2 - 4\alpha\beta)(\alpha^2 - 4\beta\gamma)(\beta^2 - 4\alpha\gamma) \\ &= -63\alpha^2\beta^2\gamma^2 + 16\alpha\beta\gamma(\alpha^3 + \beta^3 + \gamma^3) - 4(\alpha^3\beta^3 + \beta^3\gamma^3 + \alpha^3\gamma^3) \end{aligned}$$

ここで恒等式

$$x^3 + y^3 + z^3 = (x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx) + 3xyz$$

を用いて $\alpha + \beta + \gamma = 0$ に注意すると

$$\begin{aligned}
 \alpha^3 + \beta^3 + \gamma^3 &= 3\alpha\beta\gamma = -3b, \\
 \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 &= (\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) = a^2, \\
 \alpha^3\beta^3 + \beta^3\gamma^3 + \gamma^3\alpha^3 &= (\alpha\beta + \beta\gamma + \gamma\alpha)(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 - \alpha^2\beta\gamma - \alpha\beta^2\gamma - \alpha\beta\gamma^2) \\
 &\quad + 3\alpha^2\beta^2\gamma^2 \\
 &= (\alpha\beta + \beta\gamma + \gamma\alpha)(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2) + 3\alpha^2\beta^2\gamma^2 \\
 &= a^3 + 3b^2
 \end{aligned}$$

以上をまとめて, 判別式の公式

$$D(f) = \Delta^2 = -63(-b)^2 + 16(-b)(-3b) - 4(a^3 + 3b^2) = -4a^3 - 27b^2$$

を得る. 以下では, $f(x) = x^3 + ax + b$ は K 上既約であると仮定する. $f(x)$ の K 上の分解体は $L = K(\alpha, \beta, \gamma)$ である. ガロア群 $G = \text{Gal}(L/K)$ の元は $\{\alpha, \beta, \gamma\}$ の置換を引き起こすから, G は 3 次対称群 S_3 の部分群と見なすことができる.

定理 10.1 K を $\mathbb{C}$ の部分体として, $f(x) = x^3 + ax + b \in K[x]$ は K 上既約と仮定する. $f(x)$ の K 上の分解体を L とし, $G = \text{Gal}(L/K)$, $K^2 = \{a^2 \mid a \in K\}$ とおく.

(1) $\Delta \notin K$ すなわち $D(f) = -4a^3 - 27b^2 \notin K^2$ ならば $G = S_3$

(2) $\Delta \in K$ すなわち $D(f) \in K^2$ ならば $G = A_3 \cong \mathbb{Z}/3\mathbb{Z}$

さらに, いずれの場合でも L における A_3 の固定体 L^{A_3} は $K(\Delta)$ である.

証明: $f(x)$ は K 上既約であるから, 根 α, β, γ は相異なり, $f(x)$ の K 上の分解体は $L = K(\alpha, \beta, \gamma)$ である. 定義により $\Delta \in L$ であるから $K \subset K(\Delta) \subset L$ となり $K(\Delta)$ は $L \supset K$ の中間体である. 3 次交代群 A_3 は偶置換の全体からなる S_3 の (正規) 部分群である. $\sigma \in S_3$ が奇置換ならば $\sigma(\Delta) = -\Delta$, 偶置換ならば $\sigma(\Delta) = \Delta$ が成立するので, $K(\Delta)$ に対応する G の部分群 $\text{Gal}(L/K(\Delta))$ は A_3 である. 従って $[L : K(\Delta)] = |A_3| = 3$ であり, また, 定理 7.1 により $K(\Delta) = L^{A_3}$ も成立する.

一方, $\Delta^2 = D(f) = -4a^3 - 27b^2 \in K$ より, $\Delta \notin K$ ならば $[K(\Delta) : K] = 2$ であり, $[L : K] = [L : K(\Delta)][K(\Delta) : K] = 3 \cdot 2 = 6$ であるから $G = S_3$ となる. また, $\Delta \in K$ ならば $K(\Delta) = K$ であるから $G = \text{Gal}(L/K(\Delta)) = A_3$ となる. $\square$

例 10.1 $f(x) = x^3 + 3x + 1$ は $f(\pm 1) \neq 0$ より $\mathbb{Q}$ 上既約であり, 判別式は $D(f) = -4 \cdot 3^3 - 27 = -135 \notin \mathbb{Q}^2$ であるから, $f(x)$ の $\mathbb{Q}$ 上の分解体 L のガロア群は S_3 である.

例 10.2 $f(x) = x^3 - 3x + 1$ は $f(\pm 1) \neq 0$ より $\mathbb{Q}$ 上既約であり, 判別式は $D(f) = -4 \cdot (-3)^3 - 27 = 81 = 9^2 \in \mathbb{Q}^2$ であるから, $f(x)$ の $\mathbb{Q}$ 上の分解体 L のガロア群は A_3 である.

以下では、体 K は 1 の原始 3 乗根 $\omega := \frac{-1 + \sqrt{-3}}{2}$ を含む、すなわち $K \supset \mathbb{Q}(\sqrt{-3})$ であり、 $f(x) = x^3 + ax + b$ ($a, b \in K$) は K 上既約であると仮定して、3 次方程式 $f(x) = 0$ の根の公式を導こう。

L を $f(x)$ の K 上の分解体として体の拡大 $L \supset K(\Delta) \supset K$ を中間体 $K(\Delta)$ を経由して考察する。定理 10.1 より $\text{Gal}(L/K(\Delta)) = A_3$ は 3 次巡回群であるから、定理 9.3 によりある $c \in K(\Delta)$ があって L は $x^3 - c$ の $K(\Delta)$ 上の分解体になる。従って L の元は $c \in K(\Delta)$ の 3 乗根で表される。次に $K(\Delta)$ は K 上高々 2 次拡大なので、 c は K に属するか、または K の元を係数とする 2 次方程式の根となる。これで $f(x) = 0$ の根の公式が得られることになる。以上の方針を具体的に実行しよう。

$$\begin{array}{c} L = K(\alpha, \beta, \gamma) \ni \delta_1, \delta_2 \\ \left| \quad \text{Gal}(L/K(\Delta)) \cong \mathbb{Z}/3\mathbb{Z} \right. \\ K(\Delta) \ni d_1, d_2 \\ \left| \quad \text{Gal}(K(\Delta)/K) \cong \mathbb{Z}/2\mathbb{Z} \right. \\ K \ni d_1 + d_2, d_1 d_2 \end{array}$$

3 次の巡回置換は A_3 に属するから、 $\text{Gal}(L/K(\Delta)) \cong A_3$ の元 σ であって

$$\sigma(\alpha) = \beta, \quad \sigma(\beta) = \gamma, \quad \sigma(\gamma) = \alpha$$

を満たすものが存在する。 σ は偶置換であるから $K(\Delta)$ の元（従って ω も）を固定する。そこで Lagrange の分解式に従って、

$$\delta_1 = \alpha + \omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) = \alpha + \omega\beta + \omega^2\gamma, \quad \delta_2 = \alpha + \omega\sigma^2(\alpha) + \omega^2\sigma^4(\alpha) = \alpha + \omega^2\beta + \omega\gamma$$

とおく。

$$\begin{aligned} \omega\sigma(\delta_1) &= \omega\sigma(\alpha) + \omega^2\sigma(\beta) + \omega^3\sigma(\gamma) = \alpha + \omega\beta + \omega^2\gamma = \delta_1, \\ \omega^2\sigma(\delta_2) &= \omega^2\sigma(\alpha) + \omega^4\sigma(\beta) + \omega^3\sigma(\gamma) = \alpha + \omega^2\beta + \omega\gamma = \delta_2 \end{aligned}$$

より

$$\sigma(\delta_1) = \omega^{-1}\delta_1 = \omega^2\delta_1, \quad \sigma(\delta_2) = \omega^{-2}\delta_2 = \omega\delta_2 \quad (2)$$

が成立する。よって $k = 1, 2$ について $d_k = \delta_k^3$ とおけば $\sigma(d_k) = \sigma(\delta_k)^3 = \delta_k^3 = d_k$ が成立し、 $\text{Gal}(L/K(\Delta)) = \langle \sigma \rangle = \{\text{id}_L, \sigma, \sigma^2\}$ であるから、 d_k は $K(\Delta)$ に属する。

また、(2) より $\sigma(\delta_1\delta_2) = \delta_1\delta_2$ が成り立つことがわかるので、 $\delta_1\delta_2$ は $L^{\langle \sigma \rangle} = K(\Delta)$ に属する。実際に計算すると

$$\begin{aligned} \delta_1\delta_2 &= (\alpha + \omega\beta + \omega^2\gamma)(\alpha + \omega^2\beta + \omega\gamma) = \alpha^2 + \beta^2 + \gamma^2 + (\omega + \omega^2)(\alpha\beta + \beta\gamma + \gamma\alpha) \\ &= \alpha^2 + \beta^2 + \gamma^2 - (\alpha\beta + \beta\gamma + \gamma\alpha) = (\alpha + \beta + \gamma)^2 - 3(\alpha\beta + \beta\gamma + \gamma\alpha) = -3a \in K \end{aligned}$$

を得る．これから $d_1 d_2 = -27a^3$ が従う．次に d_1 を具体的に計算すると

$$\begin{aligned} d_1 &= \delta_1^3 = (\alpha + \omega\beta + \omega^2\gamma)^3 \\ &= \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega^2(\alpha^2\beta^2 + \beta\gamma^2 + \gamma\alpha^2) \\ &= -9b + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega^2(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) \end{aligned}$$

を得る． δ_1 の定義において ω に ω^2 を代入したものが δ_2 であるから，

$$d_2 = \delta_2^3 = -9b + 3\omega^2(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2)$$

となることもわかる．従って

$$\begin{aligned} d_1 + d_2 &= -18b + 3(\omega + \omega^2)(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3(\omega^2 + \omega)(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) \\ &= -18b - 3(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) - 3(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) \\ &= -18b - 3\alpha\beta(\alpha + \beta) - 3\beta\gamma(\beta + \gamma) - 3\gamma\alpha(\gamma + \alpha) \\ &= -18b + 9\alpha\beta\gamma = -18b - 9b = -27b \end{aligned}$$

を得る．これと $d_1 d_2 = -27a^3$ から， d_1, d_2 は共に t についての2次方程式

$$t^2 + 27bt - 27a^3 = 0$$

の根であることがわかる．従って

$$d_1, d_2 = -\frac{27}{2}b \pm \frac{1}{2}\sqrt{27(4a^3 + 27b^2)} = -\frac{27}{2}b \pm \frac{3\sqrt{3}}{2}\sqrt{-D(f)}$$

を得る．ここで， $f(x)$ の既約性から α, β, γ は相異なるので $D(f) \neq 0$ であり，従って $d_1 \neq d_2$ であることを用いた．さて，

$$\alpha + \beta + \gamma = 0, \quad \delta_1 = \alpha + \omega\beta + \omega^2\gamma, \quad \delta_2 = \alpha + \omega^2\beta + \omega\gamma$$

より

$$P \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ \delta_1 \\ \delta_2 \end{pmatrix}, \quad P := \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

が成立する． P は (3 次の) 離散 Fourier 変換と呼ばれる． $Q = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix}$ とおくと

$PQ = 3I_3$ となることが容易に確かめられるので，

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = P^{-1} \begin{pmatrix} 0 \\ \delta_1 \\ \delta_2 \end{pmatrix} = \frac{1}{3}Q \begin{pmatrix} 0 \\ \delta_1 \\ \delta_2 \end{pmatrix}$$

より

$$\alpha = \frac{1}{3}(\delta_1 + \delta_2), \quad \beta = \frac{1}{3}(\omega^2\delta_1 + \omega\delta_2), \quad \gamma = \frac{1}{3}(\omega\delta_1 + \omega^2\delta_2), \quad \delta_1^3 = d_1, \quad \delta_2^3 = d_2 \quad (3)$$

を得る. d_1 と d_2 は a, b と平方根を用いて表され, δ_1, δ_2 は d_1, d_2 の 3 乗根であるから, これで 3 次方程式 $x^3 + ax + b = 0$ の根が平方根と 3 乗根および四則演算を用いて表されたことになる. (3) を Cardano の公式という. ここで d_1 と d_2 が決まったとき, δ_1 と δ_2 の選び方は $3 \times 3 = 9$ 通りあるが, $\delta_1\delta_2 = -3a$ を満たすように選ぶ必要がある. これを満たすような δ_1 と δ_2 の選び方は 3 通りあるが, これは α, β, γ の巡回置換に対応することがわかるので, $\delta_1\delta_2 = -3a$ を満たせば 3 通りのいずれでもよい. さらに d_1 と d_2 の決め方は 2 通りあるので, 根の公式 (3) は 6 通りの値を取り得るが, それらは α, β, γ の置換に対応するので, 結局 $\delta_1\delta_2 = -3a$ を満たしさえすれば, d_1, d_2 と δ_1, δ_2 は任意の一組を取ればよい.

例 10.3 $x^3 + 3x + 1 = 0$ の根を求めよう. $D(f) = -135$ であるから,

$$d_1 = -\frac{27}{2} + \frac{3\sqrt{3}}{2}\sqrt{135} = \frac{-27 + 3\sqrt{405}}{2}, \quad d_2 = \frac{-27 - 3\sqrt{405}}{2}$$

としてよい. ここで $-27 + 3\sqrt{405} > 0$ に注意して

$$\delta_1 = \sqrt[3]{\frac{-27 + 3\sqrt{405}}{2}}, \quad \delta_2 = -\sqrt[3]{\frac{27 + 3\sqrt{405}}{2}}$$

とおくと $\delta_1^3 = d_1, \delta_2^3 = d_2$ かつ δ_1 は正の実数, δ_2 は負の実数であるから, $\delta_1\delta_2 = -3a = -9$ を満たす (符号のみチェックすればよい). 従って $x^3 + 3x + 1 = 0$ の 3 根は

$$\alpha = \frac{1}{3} \left(\sqrt[3]{\frac{-27 + 3\sqrt{405}}{2}} - \sqrt[3]{\frac{27 + 3\sqrt{405}}{2}} \right), \quad \beta = \frac{1}{3} \left(\omega^2 \sqrt[3]{\frac{-27 + 3\sqrt{405}}{2}} - \omega \sqrt[3]{\frac{27 + 3\sqrt{405}}{2}} \right),$$

$$\gamma = \frac{1}{3} \left(\omega \sqrt[3]{\frac{-27 + 3\sqrt{405}}{2}} - \omega^2 \sqrt[3]{\frac{27 + 3\sqrt{405}}{2}} \right)$$

ここで α は負の実数であり, β, γ は互いに共役な複素数である.

問題 10.1 次の多項式の $\mathbb{Q}$ 上の分解体 L のガロア群 $\text{Gal}(L/\mathbb{Q})$ を求めよ.

$$(1) \quad x^3 - x - 1 \qquad (2) \quad x^3 - 3x^2 + 1$$

11 可解群

定義 11.1 群 G が可解群 (solvable group) であるとは, G の部分群の列

$$\{\text{id}\} = H_0 \subset H_1 \subset \cdots \subset H_{m-1} \subset H_m = G$$

が存在して, すべての $i = 1, \dots, m$ について H_{i-1} は H_i の正規部分群であり, 剰余群 H_i/H_{i-1} はアーベル群となることである. ここで id は G の単位元を表す.

特に G がアーベル群ならば $\{\text{id}\} \subset G$ は定義の条件を満たすから G は可解群である。

例 11.1 3次対称群 S_3 は可解群である。実際、部分群の列 $\{\text{id}\} \subset A_3 \subset S_3$ において、 A_3 は S_3 の正規部分群であり $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ はアーベル群である。また、 $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ もアーベル群である。

例 11.2 4次対称群 S_4 は可解群である。実際、

$$N := \{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

とおくと、 $N \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$ であり、 N は単位元とサイクル分解が2つの互換の積になるようなすべての S_4 の元からなるから、 S_4 の正規部分群、よって A_4 の正規部分群でもある。従って S_4 の部分群の列

$$\{\text{id}\} \subset N \subset A_4 \subset S_4$$

は可解群の条件を満たす。実際、 $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$ であり、 A_4/N は位数3だから $\mathbb{Z}/3\mathbb{Z}$ に同型である。

補題 11.1 $n \geq 3$ のとき3交代群 A_n は3次巡回置換で生成される。すなわち、 A_n の任意の元はいくつかの3次巡回置換の積で表される。

証明: A_n の元は偶数個の互換の積(合成)で表されるから、2つの互換の積がいくつかの3次巡回置換の積で表されることを示せばよい。2つの相異なる互換が共通成分を持つとき、数字を入れ替えれば $(1\ 2)$ と $(2\ 3)$ とできるが、 $(1\ 2)(2\ 3) = (1\ 2\ 3)$ が成立する。一方、2つの相異なる互換が共通成分を持たないときは、数字を入れ替えれば $(1\ 2)(3\ 4)$ とできるが、 $(1\ 2)(3\ 4) = (1\ 4\ 3)(1\ 2\ 3)$ が成立する。従って2つの互換の積は1つまたは2つの3次巡回置換の積で表される。□

定理 11.1 $n \geq 5$ のとき n 交代群 A_n は $\{\text{id}\}$ と A_n 以外に正規部分群を持たない。

証明: $H \neq \{\text{id}\}$ を A_n の正規部分群とする。 H が長さ3の巡回置換 σ を少なくとも1つ含むことを示せばよい。実際このとき、長さ3の任意の巡回置換はある $\tau \in S_n$ によって $\tau\sigma\tau^{-1}$ と表される。もし τ が偶置換であれば、 $\tau \in A_n$ より $\tau\sigma\tau^{-1}$ は H に属する。もし τ が奇置換であれば、 $n \geq 5$ より $\sigma(j_1) = j_1$ かつ $\sigma(j_2) = j_2$ をみたす相異なる $j_1, j_2 \in \{1, \dots, n\}$ がとれるので $\tau' = \tau \circ (j_1\ j_2)$ とおけば τ' は偶置換であり、

$$\tau\sigma\tau^{-1} = \tau \circ (j_1\ j_2) \circ \sigma \circ (j_1\ j_2) \circ \tau^{-1} = \tau'\sigma\tau'^{-1}$$

は H に属する。従って補題 11.1 により、いずれにせよ $H = A_n$ であることがわかる。

さて、 H が長さ3の巡回置換を含まないと仮定しよう。 H の単位元以外の元 σ の中で、 $\sigma(j) = j$ となる $j \in \{1, \dots, n\}$ の個数が最大となるものを取り、それを σ とする。 $1, \dots, n$ を適当に入れ替えて、

$$\{j \in \{1, 2, \dots, n\} \mid \sigma(j) = j\} = \{m+1, \dots, n\}$$

としてよい。もし $m \leq 3$ ならば σ は(偶置換であるから)長さ3の巡回置換となり仮定に反する。よって $4 \leq m \leq n$ である。以下で σ のサイクル分解の形に応じて場合分けして矛盾を導く。

(1) σ のサイクル分解が互換の積であるとき：このとき σ は偶数個の互換の積になる．

(i) σ のサイクル分解が2つの互換の積であるとき： $1, \dots, m$ を入れ替えて $\sigma = (1\ 2)(3\ 4)$ としてよい． $n \geq 5$ であることを用いて $\tau = (3\ 4\ 5) \in A_n$ とおくと $\sigma' := \tau\sigma\tau^{-1} = (1\ 2)(4\ 5)$ は H に属する．このとき

$$\sigma^{-1}\sigma' = (3\ 4)(1\ 2)(1\ 2)(4\ 5) = (3\ 4)(4\ 5) = (3\ 4\ 5)$$

も H に属するが，これは H が3次の巡回置換を含まないという仮定に反する．

(ii) σ のサイクル分解が4つ以上の互換の積であるとき： $1, \dots, m$ を入れ替えて $\sigma = (1\ 2)(3\ 4)(5\ 6)(7\ 8)\cdots$ としてよい（従って $m \geq 8$ である．） $\tau = (3\ 4\ 5) \in A_n$ とおくと $\sigma' := \tau\sigma\tau^{-1} = (1\ 2)(4\ 5)(3\ 6)(7\ 8)\cdots$ は H に属し， σ と σ' のサイクル分解は異なるから $\sigma' \neq \sigma$ である．よって $\rho := \sigma^{-1}\sigma'$ は単位元 id ではなく，

$$\rho(1) = \sigma^{-1}(\sigma'(1)) = \sigma^{-1}(2) = 1$$

と $m \geq 5$ より ρ は1と $m+1, \dots, n$ を固定する．これは m の定義に反する．

(2) σ のサイクル分解が3次以上の巡回置換を含むとき： $3 \leq k \leq m$ を満たす k があって $\sigma = (1\ 2 \cdots k)\cdots$ であるとしてよい． σ は仮定により3次の巡回置換ではなく，また4次の巡回置換（奇置換）でもない．従って σ は少なくとも5個以上の元を動かすから $m \geq 5$ である．

$\tau = (3\ 4\ 5) \in A_n$ とおくと $\sigma' := \tau\sigma\tau^{-1}$ は H に属する．従って $\rho := \sigma^{-1}\sigma'$ も H に属し，

$$\rho(1) = \sigma^{-1}(\sigma'(1)) = \sigma^{-1}(2) = 1$$

が成立する．これと $m \geq 5$ より， ρ は1, $m+1, \dots, n$ を固定する．これは m の定義に反する．

以上により，いずれの場合にも仮定に矛盾するから， H は3次の巡回置換を含み，従って A_n に等しい．よって A_n は A_n と $\{\text{id}\}$ 以外に正規部分群を持たない．□

A_n のようにそれ自身と $\{\text{id}\}$ 以外に正規部分群を持たないような群は単純群 (simple group) と呼ばれる．位数が素数の群は巡回群であるが単純群でもある．

系 11.1 $n \geq 5$ のとき n 次交代群 A_n と n 次対称群 S_n は可解群ではない．

証明: $n \geq 4$ のとき A_n は，たとえば

$$(1\ 2\ 3)(2\ 3\ 4) = (1\ 2)(3\ 4), \quad (2\ 3\ 4)(1\ 2\ 3) = (1\ 3)(2\ 4)$$

よりアーベル群ではない．上の定理により $n \geq 5$ ならば A_n は A_n と $\{\text{id}\}$ 以外に正規部分群を持たず， A_n はアーベル群ではないから A_n は可解群ではない．

$n \geq 5$ のとき S_n は可解群ではないことを示そう． S_n の正規部分群は $\{\text{id}\}$, A_n , S_n のみであることを示せば， A_n は可解でないことから主張が従う． H を S_n の A_n に含ま

れない正規部分群とすると, $H \cap A_n$ は A_n の正規部分群であるから, 上の定理によって $H \cap A_n$ は $\{\text{id}\}$ または A_n に等しい. $H \cap A_n = A_n$ であれば $H \supset A_n$ と仮定より $H = S_n$ となる. よって $H \cap A_n = \{\text{id}\}$ としてよい. 仮定より H はある奇置換 σ を含む. 正規部分群であることから, H は σ と同じ型のサイクル分解を持つようなすべての置換を含み $n \geq 5$ であるから特に σ^{-1} と異なる奇置換 τ を含む. このとき $\sigma\tau$ は偶置換だから $H \cap A_n = \{\text{id}\}$ に属するが, $\sigma\tau \neq \text{id}$ であるからこれは矛盾である. $\square$

命題 11.1 G が可解群ならば G の任意の正規部分群 H と剰余群 G/H も可解群である.

証明: H を G の正規部分群とする.

$$\{\text{id}\} = H_0 \subset H_1 \subset \cdots \subset H_{m-1} \subset H_m = G$$

を可解群の定義を満たす G の部分群の列とする. このとき H の部分群の列

$$\{\text{id}\} = H_0 \subset H_1 \cap H \subset \cdots \subset H_{m-1} \cap H \subset H_m \cap H = H$$

は可解群の条件を満たすことを示せばよい. $1 \leq i \leq m$ とする. H_{i-1} は H_i の正規部分群であるから, 任意の $\sigma \in H_{i-1} \cap H$ と任意の $\tau \in H_i \cap H$ に対して $\tau\sigma\tau^{-1}$ は H_{i-1} に属するが, H は G の正規部分群であるから, $\tau\sigma\tau^{-1}$ は H にも属する. 従って $H_{i-1} \cap H$ は $H_i \cap H$ の正規部分群である. 自然な群準同型

$$\varphi: H_i \cap H \ni \sigma \mapsto H_{i-1}\sigma \in H_i/H_{i-1}$$

の核は

$$\text{Ker } \varphi = \{\sigma \in H_i \cap H \mid \varphi(\sigma) = H_{i-1}\sigma = H_{i-1}\} = H_i \cap H \cap H_{i-1} = H_{i-1} \cap H$$

であるから群準同型定理より剰余群 $(H_i \cap H)/(H_{i-1} \cap H) = (H_i \cap H)/\text{Ker } \varphi$ は $\text{Im } \varphi$ に同型である. 仮定より H_i/H_{i-1} はアーベル群であるから, $(H_i \cap H)/(H_{i-1} \cap H) \cong \text{Im } \varphi$ もアーベル群である. 以上により H は可解群であることが示された.

次に剰余群 G/H が可解群であることを示そう. $\pi: G \rightarrow G/H$ を自然な群準同型とする. $\sigma \in G$ に対して $\pi(\sigma) = \sigma H$ である. $G/H = \pi(G)$ の部分群の列

$$\{\text{id}\} = \pi(H_0) \subset \pi(H_1) \subset \cdots \subset \pi(H_{m-1}) \subset \pi(H_m) = \pi(G)$$

が可解群の条件を満たすことを示せばよい. 任意の $\sigma \in H_{i-1}$ と $\tau \in H_i$ に対して $\tau\sigma\tau^{-1} \in H_{i-1}$ であるから,

$$\pi(\tau)\pi(\sigma)\pi(\tau)^{-1} = \pi(\tau\sigma\tau^{-1}) \in \pi(H_{i-1})$$

より $\pi(H_{i-1})$ は $\pi(H_i)$ の正規部分群である. π は全射群準同型

$$\bar{\pi}: H_i/H_{i-1} \longrightarrow \pi(H_i)/\pi(H_{i-1})$$

を引き起こす. H_i/H_{i-1} はアーベル群であるから, その $\bar{\pi}$ による像 $\pi(H_i)/\pi(H_{i-1})$ もアーベル群である. よって G/H は可解群である. $\square$

12 方程式のべき根による可解性

3 次方程式の根の公式では，方程式の係数から四則演算，平方根，3 乗根という演算を組み合わせることで根が表示された．これを一般化して，方程式が「べき根によって解ける」または「可解」であるということを次のように定義する．

定義 12.1 K を $\mathbb{C}$ の部分体とする． $f(x) \in K[x]$ に対して方程式 $f(x) = 0$ が K 上でべき根によって解けるまたは K 上可解であるとは， $f(x) = 0$ のすべての根が K の元から出発して，べき乗根（2 項方程式の根）と 1 のべき乗根および四則演算を組み合わせることで表示できることと定義する．ただし表示とは理論的な意味であり，具体的な表示を求めることができるかどうかは問わない．

定理 12.1 K をすべての 1 のべき乗根を含むような $\mathbb{C}$ の部分体， $f(x) \in K[x]$ を 2 次以上の多項式とする．このとき，方程式 $f(x) = 0$ が K 上べき根によって解けるための必要十分条件は $f(x)$ の K 上の分解体 L のガロア群 $\text{Gal}(L/K)$ が可解群となることである．

証明: (1) 必要性： $f(x) = 0$ が K 上可解であると仮定する． n 乗根による表示は，ある a に対して 2 項方程式 $x^n - a$ の根を表すから， $F_m \supset L$ となるような拡大体の列

$$F_m \supset F_{m-1} \supset \cdots \supset F_1 \supset F_0 = K$$

であって，各々の $i = 1, \dots, m$ に対してある $n_i \in \mathbb{N}$ とある $a_i \in F_{i-1}$ があり， F_i は $x^{n_i} - a_i$ の F_{i-1} 上の分解体となっているとしてよい．このとき $F_i = K(\sqrt[n_i]{a_1}, \dots, \sqrt[n_i]{a_i})$ であるから， F_i は K 上のガロア拡大である．ただし $\sqrt[n_i]{a_i}$ は $x^{n_i} - a_i$ の根の 1 つを表すものとする（仮定より 1 の n_i 乗根は K に含まれるので，どれを選んでも以下の議論に影響はない．）体の拡大 $F_m \supset K$ の中間体のガロア対応により，

$$H_i := \Phi(F_i) = \text{Gal}(F_m/F_i) \quad (i = 1, 2, \dots, m)$$

とおく．このとき定理 7.2 より $\text{Gal}(L/K)$ の部分群の列

$$\{\text{id}\} = H_m \subset H_{m-1} \subset \cdots \subset H_1 \subset H_0 = \text{Gal}(F_m/K)$$

ができ， $H_i = \text{Gal}(F_m/F_i) \subset \text{Gal}(F_m/F_{i-1}) = H_{i-1}$ とみなせる． $F_i \supset F_{i-1}$ はガロア拡大であるから， F_i をガロア拡大 $F_m \supset F_{i-1}$ の中間体とみなせば， F_i に対応する $\text{Gal}(F_m/F_{i-1})$ の部分群が H_i であり，定理 7.2 により H_i は H_{i-1} の正規部分群であり， $H_i/H_{i-1} \cong \text{Gal}(F_i/F_{i-1})$ が成立する．さらに定理 9.1 により H_i/H_{i-1} は巡回群である．以上により $\text{Gal}(F_m/K)$ は可解群であることがわかった． $F_m \supset L \supset K$ と L が K のガロア拡大であることと命題 11.1 により $\text{Gal}(L/K) \cong \text{Gal}(F_m/K)/\text{Gal}(F_m/L)$ も可解群である．

(2) 十分性： $\text{Gal}(L/K)$ は可解群であると仮定する．部分群の列

$$\{\text{id}\} = H_m \subset H_{m-1} \subset \cdots \subset H_1 \subset H_0 = \text{Gal}(L/K)$$

であって, すべての $i = 1, \dots, m$ について, H_i は H_{i-1} の正規部分群であり H_{i-1}/H_i はアーベル群であるようなものが存在する. アーベル群の基本定理によって, H_{i-1}/H_i はいくつかの (有限) 巡回群の直和になる. 従って H_{i-1} の部分群の列

$$H_i = G_l \subset G_{l-1} \subset \dots \subset G_1 \subset G_0 = H_{i-1}$$

が存在して, すべての $j = 1, \dots, l$ について G_j は G_{j-1} の正規部分群であって G_{j-1}/G_j は巡回群であるようにできる. 従って, 最初から各 H_{i-1}/H_i は巡回群であると仮定しても一般性を失わない.

$$F_i := L^{H_i} = \{\alpha \in L \mid \sigma(\alpha) = \alpha \quad (\forall \sigma \in H_i)\}$$

とおけば, 定理 7.1 と定理 7.2 により

$$L = F_m \supset F_{m-1} \supset \dots \supset F_2 \supset F_1 \supset F_0 = K$$

が成立する. 前半の証明で示したように, $H_i = \text{Gal}(L/F_i) \subset \text{Gal}(L/F_{i-1}) = H_{i-1}$ とみなせて H_i は H_{i-1} の正規部分群であるから, $F_i \supset F_{i-1}$ はガロア拡大である. $\text{Gal}(F_i/F_{i-1}) = \text{Gal}(L/F_{i-1})/\text{Gal}(L/F_i) = H_{i-1}/H_i$ は位数 $n_i := [F_i : F_{i-1}]$ の巡回群である. 定理 7.2 により, ある $a_i \in F_{i-1}$ が存在して F_i は $x^{n_i} - a_i$ の F_{i-1} 上の分解体となる. 以上により, $f(x) = 0$ はべき根によって解けることが示された. $\square$

13 5 次方程式のガロア群の例と根の公式の不可能性

$\mathbb{Q}$ 上のガロア群が S_5 になるような 5 次多項式の例を構成しよう. S_5 は可解群ではないので, 定理 12.1 により, べき根によって解けない 5 次方程式が存在することになる. これから特に, べき根を用いた 5 次方程式の根の公式は存在しないことがわかる. もし公式が存在すれば, 任意の有理数係数の 5 次方程式がべき根で解けることになるからである.

命題 13.1 p を素数とする. p 次対称群 S_p の部分群 G が集合 $X := \{1, \dots, p\}$ に推移的に作用していて, かつ互換を 1 つでも含めば, $G = S_n$ である.

証明: $(1\ 2) \in G$ としてよい. 集合 X に関係 $\sim$ を

$$i \sim j \iff ((i\ j) \in G \text{ または } i = j)$$

で定義すると $\sim$ は同値関係になる. 実際, i, j, k を X の相異なる 3 つの元で $i \sim j$ かつ $j \sim k$ とすると, $(i\ k) = (i\ j)(j\ k)(i\ j) \in G$ であるから $i \sim k$ となる. この同値関係による X の類別を

$$X = X_1 \cup \dots \cup X_r$$

とする. $\sigma \in G$ を任意にとる. もし $i \sim j$ ならば $\sigma(i) \sim \sigma(j)$ である. 実際 $i \neq j$ かつ $(i\ j) \in G$ ならば $(\sigma(i)\ \sigma(j)) = \sigma \circ (i\ j) \circ \sigma^{-1} \in G$ である. これと σ が全単射であることから, σ は各々の X_i をある X_j に写す ($\sigma(X_i) = X_j$) ことがわかる. 仮定により G は

X に推移的に作用しているから, 任意の $i, j \in \{1, \dots, r\}$ に対して, ある $\sigma \in G$ が存在して $\sigma(X_i) = X_j$ が成立する. 特に

$$|X_1| = \dots = |X_r| \quad \text{従って} \quad p = r|X_1|$$

が成立する. $(1\ 2) \in G$ より $|X_1| \geq 2$ であり, p は素数だから $r = 1$, すわち $X = X_1$ でなければならない. これは G が任意の互換を含むことを意味するから, $G = S_p$ である. $\square$

定理 13.1 p を素数として, $\mathbb{Q}$ 上既約な p 次多項式 $f(x) \in \mathbb{Q}[x]$ の実根の個数がちょうど $p-2$ 個であると仮定する. このとき $f(x)$ の $\mathbb{Q}$ 上の分解体を L とすると $\text{Gal}(L/\mathbb{Q}) = S_p$ である.

証明: $f(x)$ の $\mathbb{C}$ における根を $\alpha_1, \alpha_2, \dots, \alpha_p$ とする. このうち α_1 と α_2 のみが虚数であるとしてよい.

$$L := \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_p), \quad F := \mathbb{Q}(\alpha_3, \dots, \alpha_p)$$

とおくと L は $\mathbb{Q}$ 上のガロア拡大であり, $L \not\subset \mathbb{R}$ かつ $F \subset \mathbb{R}$ より $F \subsetneq L$ であるから, $\text{Gal}(L/F)$ は位数 2 以上であり, ある $\sigma \neq \text{id}$ を含む. このとき

$$\sigma(\alpha_1) = \alpha_2, \quad \sigma(\alpha_2) = \alpha_1, \quad \sigma(\alpha_j) = \alpha_j \quad (3 \leq j \leq p)$$

であるから, $G = \text{Gal}(L/\mathbb{Q})$ を $\alpha_1, \dots, \alpha_p$ への作用によって S_p の部分群とみなせば, G は互換 $(1\ 2)$ を含む. 定理 9.2 より G は $\{\alpha_1, \dots, \alpha_p\}$ に推移的に作用するから, 命題 13.1 によって $G = S_p$ となる. $\square$

例 13.1 $f(x) = x^5 - 4x + 2$ の $\mathbb{Q}$ 上の分解体 L のガロア群 $G := \text{Gal}(L/\mathbb{Q})$ は S_5 である. 従って $f(x) = 0$ は $\mathbb{Q}$ 上べき根によって解けない. まず, Eisenstein の判定法を $p = 2$ として適用すれば, $f(x)$ は $\mathbb{Q}$ 上既約であることがわかる. $f'(x) = 5x^4 - 4$ はちょうど 2 つの実根 $\pm\alpha$, $\alpha := \left(\frac{4}{5}\right)^{\frac{1}{4}}$ を持つ.

$$f(\pm\alpha) = \pm \left(\frac{4}{5}\alpha - 4\alpha \right) + 2 = \mp \frac{16}{5}\alpha + 2, \quad \alpha > \frac{4}{5}$$

より, $f(x)$ の極小値は $f(\alpha) < 0$ であり極大値は $f(-\alpha) > 0$ であることがわかる. 従って $f(x) = 0$ はちょうど 3 個の実根を持つから, 定理 13.1 により $G = S_5$ である.

14 円分体

n を自然数とすると, $x^n - 1$ の $\mathbb{Q}$ 上の最小分解体のことを円分体 (cyclotomic field) という. ここでは n が素数の場合を詳しく調べよう.

定理 14.1 p を素数とすると, $x^p - 1$ の $\mathbb{Q}$ 上のガロア群 $G := \text{Gal}_{\mathbb{Q}}(x^p - 1)$ は $(\mathbb{Z}/\mathbb{Z}p)^{\times}$ と同型であり, 位数 $p-1$ の巡回群である.

証明: ζ を 1 の原始 p 乗根とすると, $x^p - 1$ の $\mathbb{Q}$ 上の最小分解体は $L = \mathbb{Q}(\zeta)$ である (命題 8.1). ζ の $\mathbb{Q}$ 上の最小多項式は

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

であることを示そう. $x^p - 1 = (x - 1)f(x)$ と $\zeta^p = 1, \zeta \neq 1$ より $f(\zeta) = 0$ である. $f(x)$ が $\mathbb{Q}$ 上既約であることを示そう.

$$xf(x+1) = (x+1)^p - 1 = x^p + px^{p-1} + {}_pC_2x^{p-2} + \cdots + px$$

よって

$$f(x+1) = x^{p-1} + px^{p-2} + {}_pC_2x^{p-3} + \cdots + p$$

であり, $1 \leq j \leq p-1$ のとき ${}_pC_j = p(p-1)\cdots 2/j!$ は p の倍数だから, Eisenstein の判定法により $f(x+1)$ は $\mathbb{Q}$ 上既約である. 従って $f(x)$ も $\mathbb{Q}$ 上既約である. 以上により $[L : \mathbb{Q}] = p-1 = \phi(p)$ であり G は $(\mathbb{Z}/\mathbb{Z}p)^\times$ の部分群であったから, $G = (\mathbb{Z}/\mathbb{Z}p)^\times$ である.

最後に, G が巡回群であることを示そう. $\mathbb{F}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ は体であり, $(\mathbb{Z}/\mathbb{Z}p)^\times = \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\bar{0}\}$ である. $\mathbb{F}_p^\times$ は乗法に関して位数 $p-1$ のアーベル群だから, 単因子論によるアーベル群の基本定理の証明 (「環と加群」を参照) から, 自然数の列 $d_1 | d_2 | \cdots | d_r$ があって, アーベル群としての直和分解

$$\mathbb{F}_p^\times \cong (\mathbb{Z}/\mathbb{Z}d_1) \oplus \cdots \oplus (\mathbb{Z}/\mathbb{Z}d_r)$$

が存在する. ここで $d_1 \geq 2$ と仮定してよい. この同型から, $d = d_r$ とおけば任意の $\bar{j} \in \mathbb{F}_p^\times$ について $\bar{j}^d = \bar{1}$ が成立する. $d_1 \cdots d_r = p-1$ であるから, $r \geq 2$ と仮定すると, $d < p-1$ である. 一方, 多項式 $x^d - 1$ の体 $\mathbb{F}_p$ における根は高々 d 個だから, これは矛盾である. 従って $r = 1$ かつ $d = p-1$ でなければならないから, $\mathbb{F}_p^\times$ は巡回群 $\mathbb{Z}/\mathbb{Z}(p-1)$ に同型である. $\square$

索引

アーベル拡大, 34

アーベル群, 18

位数, 18

1 の n 乗根, 32

円分体, 32

オイラー関数, 33

Gauss の補題, 10

可解 (方程式), 45

可解群, 41

可換環, 3

可換群, 18

拡大次数, 5

拡大体, 3

拡張 (体準同型の), 26

Cardano の公式, 41

ガロア拡大, 20

ガロア群, 21

環, 2

奇置換, 19

軌道, 19

既約, 9

偶置換, 19

群, 17

群準同型, 18

群同型, 18

原始 n 乗根, 32

原始多項式, 10

交代群, 19

互換, 19

固定体, 25

最小多項式, 5

差積, 37

作用, 19

自己同型, 3

巡回拡大, 34

巡回置換, 19

剰余群, 18

推移的 (作用), 19

正規部分群, 18

体準同型, 3

対称群, 18

代数的, 5

代数閉体, 13

体同型, 3

単純拡大, 4

単純群, 43

置換, 18

中間体, 24

超越的, 5

内容, 10

判別式, 37

部分群, 18

部分体, 3

分解体, 13

べき根によって解ける, 45

有限群, 18

有限次拡大, 5