最低限の Galois 理論

高瀬 幸一

ver.2021.11.5

1　体の拡大

体 K の部分体 $F \subset K$ があるとき，これを K/F と書いて，**体の拡大**と呼ぶ．このとき K を F 上のベクトル空間とみなすことができる．即ち，$u, v \in K$ のベクトル和を K における加法による和 $u+v \in K$ と定義し，$v \in K$ の定数 $\lambda \in F$ 倍を K における乗法による積 $\lambda u \in K$ により定義するのである．このようにして K を F-ベクトル空間とみなしたとき，その F 上の次元 $\dim_F K$ を体の拡大 K/F の**拡大次数** と呼び，$(K:F)$ と書く．$(K:F) < \infty$ のとき，体の拡大 K/F は有限次拡大であるという．体の拡大 K/F に対して $F \subset L \subset K$ なる K の部分体 L を，体の拡大 K/F の**中間体** と呼ぶ.

体の拡大次数に関して，次のことが基本的である：

命題 1.1 体の有限次拡大 K/F の中間体 L に対して

$$(K:F) = (K:L)(L:F)$$

である.

[**証明**] K/L 及び L/F が体の有限次拡大となることは明らかである．そこで $(K:L) = m, (L:F) = n$ として，L-ベクトル空間 K の L 上の基底を $\{\alpha_i\}_{i=1,2\cdots,m}$ とし，F-ベクトル空間 L の F 上の基底を $\{\beta_j\}_{j=1,2,\cdots,n}$ とする．任意の $x \in K$ は $x = \sum_{i=1}^{m} a_i\alpha_i$ $(a_i \in L)$ と書け，$a_i \in L$ は $a_i = \sum_{j=1}^{n} a_{ij}\beta_j$ $(a_{ij} \in F)$ と書けるから，$x = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\alpha_i\beta_j$ となり，F-ベクトル空間 K は F 上 $\{\alpha_i\beta_j\}_{i=1,\cdots,m,j=1,\cdots,n}$ により生成される．一方，$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\alpha_i\beta_j = 0$ $(a_{ij} \in F)$ とすると，$a_i = \sum_{j=1}^{n} a_{ij}\beta_j \in L$ に対して $\sum_{i=1}^{m} a_i\alpha_i = 0$ となり，基底の一次独立性から $a_i = 0$，よって再び基底の一次独立性から $a_{ij} =$

0 となる．よって $\{\alpha_i\beta_j\}_{i=1,\cdots,m,j=1,\cdots,n}$ は F 上一次独立である．よって $\{\alpha_i\beta_j\}_{i=1,\cdots,m,j=1,\cdots,n}$ が F-ベクトル空間 K の F 上の基底となるから，$(K:F)=mn$ である．■

体の拡大 K/F があったとき，部分集合 $S\subset K$ に対して $F\cup S$ を含む K の最小の部分体を $F(S)$ と書き，F に S を**添加した体**と呼ぶ．特に $S=\{\alpha\}$ のとき $F(S)=F(\alpha)$ と書く．具体的には

$$F(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}\;\middle|\; f(X),g(X)\in F[X],g(\alpha)\neq 0\right\}$$

である．ここで多項式環 $F[X]$ から K への環の準同型写像

$$\varphi:F[X]\to K\qquad (f(X)\mapsto f(\alpha))$$

を考えると，その核

$$\mathrm{Ker}(\varphi)=\{f(X)\in F[X]\mid f(\alpha)=0\}$$

は $F[X]$ のイデアルとなる．二つの場合が考えられる；

I) $\mathrm{Ker}(\varphi)=\{0\}$ の場合．即ち，$f(\alpha)=0$ となる F-係数多項式 $f(X)\in F[X]$ は 0-多項式に限るとき，$\alpha\in K$ は F 上**超越的**であるという．この場合 φ の像 $\mathrm{Im}(\varphi)$ は多項式環 $F[X]$ と同型な K の部分環となる．

II) $\mathrm{Ker}(\varphi)\supsetneqq\{0\}$ の場合．即ち，$f(\alpha)=0$ となる F-係数多項式 $f(X)\in F[X]$ で $f(X)\neq 0$ なるものが存在するとき，$\alpha\in K$ は F 上**代数的**であるという．体 F 上の一変数多項式環 $F[X]$ は単項イデアル整域だから

$$\mathrm{Ker}(\varphi)=(p(X))=\{p(X)\cdot h(X)\mid h(X)\in F[X]\}$$

なる $p(X)\in F[X]$ が存在する．具体的には $\mathrm{Ker}(\varphi)$ に含まれる 0 でない F-係数多項式で次数が最小のものをとればよい．言い換えれば $p(X)\in F[X]$ は $p(\alpha)=0$ となる次数最小の多項式である．更に最高次の係数で割れば，$p(X)$ の最高次の係数は 1（このような多項式を monic な多項式と呼ぶ）としてよい．このとき $p(X)$ を α の**最小多項式** と呼ぶ．さて，環の準同型定理から，環の同型

$$\overline{\varphi}:F[X]/(p(X))\xrightarrow{\sim}\mathrm{Im}(\varphi)\qquad (\overline{f(X)}\mapsto f(\alpha))$$

が成り立つが，$\mathrm{Im}(\varphi)$ は体 K の部分環だから整域となり，従って同型な $F[X]/(p(X))$ も整域となり，$F[X]$ が単項イデアル整域であることに注意すると，$F[X]/(p(X))$ は体となり，従って $\mathrm{Im}(\varphi)$ も体となる．ところで $F\cup\{\alpha\}\subset\mathrm{Im}(\varphi)$ だから，$\mathrm{Im}(\varphi)=F(\alpha)$ である．即ち $\alpha\in K$ が F 上代数的ならば

$$F(\alpha)=\{f(\alpha)\mid f(X)\in F[X]\}$$

となる．更に $F[X]/(p(X))$ が整域（従って体）だから $p(X)$ は F 上既約な多項式となる．以上をまとめて，次の命題を得る：

命題 1.2 体の拡大 K/F において，F 上代数的な $\alpha \in K$ の F 上の最小多項式を $p(X) \in F[X]$ とおくと

1) $p(X)$ は F 上既約である，

2) 任意の $f(X) \in F[X]$ に対して，$f(\alpha) = 0 \Leftrightarrow p(X)|f(X)$,

3) 体の同型

$$\overline{\varphi} : F[X]/(p(X)) \tilde{\to} F(\alpha) \quad (\overline{f(X)} \mapsto f(\alpha))$$

が成り立つ．

代数的数の最小多項式と体の拡大次数とは密接な関係にある；

命題 1.3 体の拡大 K/F において，F 上代数的な $\alpha \in K$ の F 上の最小多項式を $p(X) \in F[X]$ として $\deg p(X) = n$ とすると

$$\left\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\right\}$$

が $F(\alpha)$ の F 上の基底となる．特に $(F(\alpha) : F) = \deg p(X)$ である．

[**証明**] $\deg p(X) = n$ とする．$f(X) \in F[X]$ を $p(X)$ で割った商を $q(X)$ 余りを $r(X)$ とすると，$f(X) = q(X)p(X) + r(X)$ かつ $\deg r(X) < n$ である．このとき $f(\alpha) = r(\alpha)$ だから

$$F(\alpha) = \mathrm{Im}(\varphi) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F\}$$

となり，$\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ が F-ベクトル空間 $F(\alpha)$ を生成することがわかる．一方，

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0$$

とすると，$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} \in F[X]$ に対して $f(\alpha) = 0$ となり，$f(X) \in \mathrm{Ker}(\varphi) = (p(X))$ より $f(X)$ は $p(X)$ で割り切れるが，$f(X)$ は高々 $n-1$ 次式だから $f(X) = 0$，即ち $a_0 = a_1 = a_2 = \cdots = a_{n-1} = 0$ となり，$\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ は F 上一次独立である．よって $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ が $F(\alpha)$ の F 上の基底となり，$(F(\alpha) : F) = n$ となる．■

体の拡大 K/F に対して，K の元が全て F 上代数的のとき，K/F を**代数的拡大** と呼ぶ．

命題 1.4 体の有限次拡大は代数的拡大である．

[**証明**] 体の有限次拡大 K/F をとり $(K:F)=n<\infty$ とする．任意の $\alpha\in K$ に対して，$\{1,\alpha,\alpha^2,\cdots,\alpha^n\}\subset K$ は F 上一次従属となるから

$$a_0\cdot 1+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n=0$$

なる $a_i\in F$ で $(a_1,a_1,a_2,\cdots,a_n)\neq(0,0,0,\cdots,0)$ なるものがとれる．$f(X)=a_0+a_1+a_2X^2+\cdots+a_nX^n\in F[X]$ とおくと，$f(X)\neq 0$ かつ $f(\alpha)=0$ となる．■

系 1.5 体の拡大 K/F に対して，部分集合 $S\subset K$ の元が全て F 上代数的ならば $F(S)/F$ は代数的拡大である．

[**証明**] 任意の $\alpha\in F(S)$ に対して，有限個の $\{\beta_1,\cdots,\beta_r\}\subset S$ があって $\alpha\in F(\beta_1,\cdots,\beta_r)$ となる．

$$F_0=F,\quad F_i=F_{i-1}(\beta_i)\quad(i=1,\cdots,r)$$

とおくと $(F_i:F_{i-1})<\infty$ だから F_r/F は有限次拡大となり，従って代数的拡大である．■

課題 1.1 1) $K=\{x+\sqrt{2}y\mid x,y\in\mathbb{Q}\}$ は体であり，$\mathbb{Q}\subset K$ であることを示せ．

2) 拡大次数 $(K:\mathbb{Q})$ を求めよ．

課題 1.2 体の拡大 K/F において，$\alpha\in K$ は F 上代数的であるとする．このとき，F 上既約かつ monic な多項式 $p(X)\in F[X]$ に対して $p(\alpha)=0$ ならば，$p(X)$ は α の F 上の最小多項式であることを示せ．

2 1 の冪乗根

$z\in\mathbb{C}$ を 1 の n 乗根，即ち $z^n=1$ とする．ここで $n=1$ ならば $z=1$ であり，$n=2$ ならば $z=\pm1$ となって，この場合には簡単であるから，$n\geq 3$ とする．

$$|z|^n=|z^n|=|1|=1,\qquad\therefore|z|=1$$

だから，複素数の曲表示により $z=\cos\theta+i\sin\theta$ とする．

$$1=z^n=(\cos\theta+i\sin\theta)^n=\cos(n\theta)+i\sin(n\theta)$$

だから

$$\begin{cases}\cos(n\theta)=1,\\ \sin(n\theta)=0\end{cases}\qquad\therefore n\theta=2\pi m\quad(m=0,\pm1,\pm2,\cdots)$$

となる．$m = qn + k$ $(q, k \in \mathbb{Z}, 0 \leq k < n)$ とおくと

$$\theta = 2\pi q + \frac{2\pi}{n} \cdot k \qquad (q \in \mathbb{Z}, k = 0, 1, 2, \cdots, n-1),$$

従って

$$\begin{aligned} z &= \cos\left(\frac{2\pi}{n} \cdot k\right) + i \sin\left(\frac{2\pi}{n} \cdot k\right) \\ &= \left(\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\right)^k \quad (k = 0, 1, 2, \cdots, n-1) \end{aligned}$$

となる．以下では特に $n = p$ が素数の場合を詳しく調べてみよう．

$$\omega = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$$

は 1 の p 乗根で，1 の p 乗根は ω^k $(k = 0, 1, 2, \cdots, p-1)$ で尽くされる．

有理数体 $\mathbb{Q}$ 上の ω の最小多項式を求めるために，一つ準備となる命題を，証明なしに述べておく：

定理 2.1 (Eisenstein の判定法) 整数係数多項式

$$p(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in \mathbb{Z}[X]$$

に対して，

$$p \not| a_0, \quad p | a_k \ \ (k = 1, 2, \cdots, n), \quad p^2 \not| a_n$$

なる素数 p が存在するならば，$p(X)$ は $\mathbb{Q}$ 上既約である．

この定理を用いて次の定理を示す：

定理 2.2 素数 p に対して

$$\omega = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}$$

の $\mathbb{Q}$ 上の最小多項式は

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

である．

[**証明**] $p = 2$ のときには $\omega = -1$, $p(X) = X + 1$ となり，明らかに主張は成り立つから，$p \geq 3$ とする．$(X-1)p(X) = X^p - 1$ だから

$$Xp(X+1) = (X+1)^p - 1 = \sum_{k=0}^{p-1} \left(\frac{p}{k}\right) \cdot X^{p-k}$$

である．ここで

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad (\text{但し } 0! = 1 \text{ とする})$$

は二項係数である．よって

$$q(X) = p(X+1) = X^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} X^{p-k-1}$$

となる．$k = 1, 2, \cdots, p-1$ に対して，$\mathrm{GCD}\{p, k!\} = 1$ だから

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!} = p \cdot \frac{(p-1)(p-2)\cdots(p-k+1)}{k!},$$

よって $p \Big| \binom{p}{k}$ である．更に

$$\binom{p}{p-1} = p \qquad \therefore p^2 \not\Big| \binom{p}{p-1}$$

である．よって Eisenstein の判定法（定理 2.1）より $q(X)$ は $\mathbb{Q}$ 上既約である．よって $p(X) = q(X-1)$ は $\mathbb{Q}$ 上既約である．$\omega^p = 1$ で $(X-1)p(X) = X^p - 1$ かつ $\omega \neq 1$ だから，$p(\omega) = 0$ である．よって課題 1.2 より，$p(X)$ は ω の $\mathbb{Q}$ 上の最小多項式である．■

課題 2.1 p を素数として $\omega = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p} \in \mathbb{C}$ とおく．このとき

1) $\{1, \omega, \omega^2, \cdots, \omega^{p-2}\}$ は $\mathbb{Q}(\omega)$ の $\mathbb{Q}$ 上の基底であることを示せ．

2) $\{\omega, \omega^2, \cdots, \omega^{p-1}\}$ は $\mathbb{Q}(\omega)$ の $\mathbb{Q}$ 上の基底であることを示せ．

3　体の自己同型群

体 K に対して，K から K への環の同型写像全体 $\mathrm{Aut}(K)$ は写像の合成に関して群となる．これを体 K の**自己同型群** と呼ぶ．体の拡大 K/F に対して，

$$\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(x) = x \text{ for } \forall x \in F\}$$

は $\mathrm{Aut}(K)$ の部分群となるから，これを体 K の F 上の（或いは簡単に体の拡大 K/F の）**自己同型群** または **Galois 群** と呼ぶ．

$\mathrm{Aut}(K/F)$ の様子を調べることが大きな目標となるが，そのための一歩として，次のことを注意しておこう：

命題 3.1 体 K から体 L への環の準同型写像 $\sigma : K \to L$ は単射である．

[**証明**] $\mathrm{Ker}(\sigma) = \{0\}$ を示せば良い．$\mathrm{Ker}(\sigma) \lneqq \{0\}$ と仮定すると，$0 \neq x \in \mathrm{Ker}(\sigma)$ が取れる．$0 \neq x \in K$ で RK は体だから，$x^{-1} \in K$ である．$\mathrm{Ker}(\sigma) \subset K$ はイデアルだから $1 = x^{-1} \cdot x \in \mathrm{Ker}(\sigma)$ となる．よって $\sigma(1) = 0$ となるが，σ は環の準同型写像だから，定義により $\sigma(1) = 1$ である．よって $1 = 0$ となるが，これは矛盾である．■

上の命題 3.1 を踏まえて，一般に体の拡大 K/F と L/F に対して，K から L への環の準同型写像 $\sigma : K \to L$ であって任意の $x \in F$ に対しては $\sigma(x) = x$ となるもの全体を $\mathrm{Hom}_F(K, L)$ と書く．$\mathrm{Hom}_F(K, L)$ は空集合である可能性もあるが，次の命題が示すように，体の拡大の自己同型群と深い関係がある：

命題 3.2 体の有限次拡大 K/F に対して $\mathrm{Aut}(K/F) = \mathrm{Hom}_F(K, K)$ である．

[**証明**] 定義から $\mathrm{Aut}(K/F) \subset \mathrm{Hom}_F(K, K)$ は明らかである．任意の $\sigma \in \mathrm{Hom}_F(K.K)$ が K から K への環の同型写像であることを示せば良い．命題 3.1 より σ は単射だから，σ が全射であることを示せば良い．ここで

$$\sigma(x + y) = \sigma(x) + \sigma(y), \quad \sigma(ax) = \sigma(a)\sigma(x) = a\sigma(x) \quad (x, y \in K, a \in F)$$

であるが，これは K を F-ベクトル空間と見たときに，$\sigma : K \to K$ が F-線形写像であることを示している．σ は単射だから，F-ベクトル空間の同型

$$K \xrightarrow{\sim} \mathrm{Im}(\sigma)$$

が成り立つ．ここで $\mathrm{Im}(\sigma) \subset K$ は F-ベクトル部分空間で

$$\dim_F K = \dim_F \mathrm{Im}(\sigma) \leq \dim_F K$$

である．一方 K/F は有限次拡大だから $\dim_F K = (K : F) < \infty$ である．よって $\dim_F \mathrm{Im}(\sigma) = \dim_F K$ となり，$\mathrm{Im}(\sigma) = K$ となる．即ち $\sigma : K \to K$ は全射である．■

一般の体の拡大 $K/F, L/F$ に対する $\mathrm{Hom}_F(K, L)$ の様子を調べる前に，特殊な拡大 K/F に関して調べておこう．

定理 3.3 体の拡大 $K/F, L/F$ をとる．F 上代数的な $\alpha \in K$ の F 上の最小多項式を $p(X) \in F[X]$ とする．このとき全単射

$$\mathrm{Hom}_F(F(\alpha), L) \to \{\gamma \in L \mid p(\gamma) = 0\} \quad (\sigma \mapsto \sigma(\alpha))$$

が成り立つ．$\deg p(X) = n$ とすると，$p(\gamma) = 0$ なる $\gamma \in L$ に対応する $\sigma \in \mathrm{Hom}_F(F(\alpha), L)$ は

$$\sigma\left(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}\right) = a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{n-1}\gamma^{n-1}$$
$$(a_i \in F, i = 0, 1, 2, \cdots, n-1)$$

である．

[**証明**] $\alpha \in K$ は F 上代数的だから

$$F(\alpha) = \{f(\alpha) \mid f(X) \in F[X]\}$$

である．$\sigma \in \mathrm{Hom}_F(F(\alpha), L)$ とする．$f(X) = \sum_{k=0}^{n} a_k X^k \in F[X]$ に対して

$$\sigma\left(f(\alpha)\right) = \sum_{k=0}^{n} \sigma(a_k)\sigma(\alpha)^k = \sum_{k=0}^{n} a_k \sigma(\alpha)^k = f(\sigma(\alpha))$$

だから，$\sigma \in \mathrm{Hom}_F(F(\alpha) < L)$ は $\sigma(\alpha) \in L$ の値により決定される．更に

$$p(\sigma(\alpha)) = \sigma\left(p(\alpha)\right) = \sigma(0) = 0$$

だから，写像

$$\mathrm{Hom}_F(F(\alpha), L) \to \{\gamma \in L \mid p(\gamma) = 0\} \quad (\sigma \mapsto \sigma(\alpha))$$

は単射である．逆に $p(\gamma) = 0$ なる $\gamma \in L$ をとる．このとき

$$s : F[X]/(p(X)) \to L \quad \left(\overline{f(X)} \mapsto F(\gamma)\right)$$

は well-defined な環の準同型写像だえる．実際，$f(X), g(Xi) \in F[X]$ に対して

$$\begin{aligned}
&\overline{f(X)} = \overline{g(X)} \in F[X]/(p(X)) \\
\Rightarrow\ & f(X) - g(X) \in (p(X)) \\
\Rightarrow\ & f(X) - g(X) = p(X) \cdot h(X) \ \ (h(X) \in F[X]) \\
\Rightarrow\ & f(\gamma) - g(\gamma) = p(\gamma) \cdot h(\gamma) = 0 \quad \therefore f(\gamma) = g(\gamma)
\end{aligned}$$

だから，写像 s は well-defined である．これが環の準同型写像であることは，すぐに判る．一方，命題 1.2 の 3) から，環の同型

$$\overline{\varphi} : F[X]/(p(X)) \tilde{\to} F(\alpha) \quad \left(\overline{f(X)} \mapsto f(\alpha)\right)$$

が成り立つ．よって合成写像

$$\sigma = s \circ \overline{\varphi}^{-1} : F(\alpha) \to L \quad (f(\alpha) \mapsto f(\gamma))$$

は環の準同型写像となり，$\sigma \in \mathrm{Hom}_F(F(\alpha), L)$ かつ $\sigma(\alpha) = \gamma$ となる．■

系 3.4 体の拡大 K/F をとり，F 上代数的な $\alpha \in K$ の F 上の最小多項式を $p(X) \in F[X]$ とする．このとき全単射

$$\mathrm{Aut}(F(\alpha)/F) \to \{\gamma \in F(\alpha) \mid p(\gamma) = 0\} \quad (\sigma \mapsto \sigma(\alpha))$$

が成り立つ．

例 3.5 体の拡大 $\mathbb{C}/\mathbb{R}$ を考えると，虚数単位 $i \in \mathbb{C}$ は $\mathbb{R}$ 上代数的で，$\mathbb{R}$ 上の最小多項式は $p(X) = X^2 + 1 \in \mathbb{R}[X]$ である．更に $\mathbb{C} = \mathbb{R}(i)$ である．

$$\{\gamma \in \mathbb{C} \mid p(\gamma) = 0\} = \{\pm i\}$$

だから，$\sigma\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ が i に対応すれば

$$\sigma(x + iy) = x + iy \qquad (x, y \in \mathbb{R})$$

となり，σ は $\mathbb{C}$ 上の恒等写像である．一方，$\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$ が $-i$ に対応すれば

$$\sigma(x + iy) = x - iy \qquad (x, y \in \mathbb{R})$$

となり，σ は共役複素数を対応させる自己同型写像となる．よって

$$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \tau\}, \quad \begin{cases} \mathrm{id}_{\mathbb{C}} = \mathbb{C} \text{ 上の恒等写像}, \\ \tau = \text{共役複素数を対応させる自己同型写像} \end{cases}$$

となる．

さて，一般の体の拡大 $K/F, L/F$ に対する $\mathrm{Hom}_F(K, L)$ の様子を調べよう．議論の出発点は次の **Dedekind の定理**である；

定理 3.6 体 K から体 L への相異なる環の準同型写像 $\tau_i : K \to L$ $(i = 1, 2, \cdots, n)$ と $a_i \in L$ $(i = 1, 2, \cdots, n)$ に対して $\sum_{i=1}^{n} a_i \tau_i(x) = 0$ for $\forall x \in K$ ならば $a_i = 0$ $(i = 1, 2, \cdots, n)$ である．

[**証明**] n に関する帰納法により示す．$n = 1$ のときは $\tau_1(1) = 1$ だから明らか．$n-1$ まで成り立つと仮定して，$n > 1$ のとき，$\tau_1 \neq \tau_n$ だから $\tau_1(x_0) \neq \tau_n(x_0)$ なる $x_0 \in K$ がとれる．このとき任意の $x \in K$ に対して

$$\sum_{i=1}^{n} a_i \tau_i(x)\tau_n(x_0) = 0, \qquad \sum_{i=1}^{n} a_i \tau_i(x)\tau_i(x_0) = \sum_{i=1}^{n} a_i \tau_i(xx_0) = 0$$

だから，辺々を引いて $\sum_{i=1}^{n-1} a_i(\tau_i(x_0) - \tau_n(x_0))\tau_i(x) = 0$ を得る．よって帰納法の仮定から $a_i(\tau_i(x_0) - \tau_n(x_0)) = 0$ $(i = 1, 2, \cdots, n-1)$ となるが，$\tau_1(x_0) - \tau_n(x_0) \neq 0$ だから $a_1 = 0$ である．よって任意の $x \in K$ に対して $\sum_{i=2}^{n} a_i \tau_i(x) = 0$ となり，再び帰納法の仮定から $a_i = 0$ $(i = 2, \cdots, n)$ となる．
■

Dedekind の定理から次の評価を得る；

命題 3.7 体の拡大 K/F と体 L 及び環の準同型写像 $\sigma : F \to L$ に対して

$$\sharp\{\tau : K \to L : \text{環の準同型写像} \mid \tau|_F = \sigma\} \leq (K : F).$$

[**証明**] $(K : F) = m < \infty$ の場合が問題である．$\{\alpha_1, \cdots, \alpha_m\} \subset K$ を F-ベクトル空間 K の F 上の基底とする．相異なる環の準同型写像 $\tau_i : K \to L$ $(1 = 1, 2, \cdots, n)$ をとって $\tau_i|_F = \sigma$ と仮定する．

$$v_i = \begin{bmatrix} \tau_i(\alpha_1) \\ \tau_i(\alpha_2) \\ \vdots \\ \tau_i(\alpha_m) \end{bmatrix} \in L^m \qquad (i = 1, 2, \cdots, n)$$

とおくと $\{v_1, v_2, \cdots, v_n\}$ は L 上一次独立である．実際，$\sum_{i=1}^{n} \lambda_i v_i = 0$ $(\lambda_i \in L)$ とすると，ベクトルの各成分をみて

$$\sum_{i=1}^{n} \lambda_i \tau_i(\alpha_j) = 0 \qquad (j = 1, 2, \cdots, m)$$

となり，任意の $x = \sum_{j=1}^{m} t_j \alpha_j \in K$ $(t_i \in F)$ に対して

$$\sum_{i=1}^{n} \lambda_i \tau_i(x) = \sum_{j=1}^{m} \sigma(t_j) \left(\sum_{i=1}^{n} \lambda_i \tau_i(\alpha_j) \right) = 0$$

となるから，Dedekind の定理（定理 3.6）より $\lambda_i = 0$ $(i = 1, 2, \cdots, n)$ となる．従って $n \leq m$ となる．■

体の拡大 K/F に対して，上の命題から直ちに次の系を得る；

系 3.8 体の拡大 K/F に対して $|\mathrm{Aut}(K/F)| \leq (K : F)$ である．

課題 3.1 体 K から環 L への環準同型写像 $\sigma : K \to L$ の像 $\mathrm{Im}(\sigma)$ は L の部分体となることを示せ．

課題 3.2 $m \in \mathbb{Z}$ を平方数でない整数として，次の問いに答えよ：

1) $\sqrt{m} \in \mathbb{C}$ の $\mathbb{Q}$ 上の最小多項式を求めよ．

2) 拡大次数 $(\mathbb{Q}(\sqrt{m}) : \mathbb{Q})$ を求めよ．

3) 自己同型群 $\mathrm{Aut}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ を決定せよ．

課題 3.3 p を素数として $\omega = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p} \in \mathbb{C}$ とおく．このとき $l = 1, 2, \cdots, p-1$ に対して，写像 $\sigma_l : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ を

$$\sigma_l\left(\sum_{k=1}^{p-1} a_k \cdot \omega^k\right) = \sum_{k=1}^{p-1} a_k \cdot \omega^{lk} \qquad (a_k \in \mathbb{Q})$$

により定義すると，

$$\mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\sigma_l \mid l = 1, 2, \cdots, p-1\}$$

であることを示せ．

4 Galois 対応

体 K と部分集合 $S \subset \mathrm{Aut}(K)$ に対して

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

とおくと，K^S は K の部分体となる．体の拡大 K/F と部分集合 $S \subset \mathrm{Aut}(K/F)$ に対して K^S は拡大 K/F の中間体となる．

次の命題が基本的である；

命題 4.1 体 K と有限部分群 $G \subset \mathrm{Aut}(K)$ に対して $\mathrm{Aut}(K/K^G) = G$ かつ $(K : K^G) = |G|$ である．

[**証明**] $G \subset \mathrm{Aut}(K/K^G)$ だから，系 3.8 より $|G| \leq |\mathrm{Aut}(K/K^G)| \leq (K : K^G)$ である．従って $(K : K^G) \leq |G|$ が示されれば，$(K : K^G) = |G|$ が得られ，又 $G = \mathrm{Aut}(K/K^G)$ となる．以下，$|G| = m$ として $(K : K^G) \leq m$ を示そう．そのためには，任意の $\{\alpha_1, \cdots, \alpha_n\} \subset K$ $(n > m)$ をとって，これが K^G 上一次従属であることを示せばよい．

$$G = \{\sigma_1, \cdots, \sigma_m\} \qquad (\sigma_1 = 1)$$

として

$$v_j = \begin{bmatrix} \sigma_1(\alpha_j) \\ \sigma_2(\alpha_j) \\ \vdots \\ \sigma_m(\alpha_j) \end{bmatrix} \in K^m \qquad (j = 1, 2, \cdots, n)$$

とおく．K-ベクトル部分空間 $\langle v_1, v_2, \cdots, v_n\rangle_K \subset K^m$ の K 上の基底を $\{v_1, v_2, \cdots, v_r\}$ とすると $r \leq m < n$ だから

$$v_n = a_1 v_1 + a_2 v_2 + \cdots + a_r v_r \qquad (a_j \in K) \tag{4.1}$$

と書ける．即ち

$$\sigma_i(\alpha_n) = \sum_{j=1}^{r} a_j \sigma_i(\alpha_j) \qquad (i = 1, 2, \cdots, m) \tag{4.2}$$

である．この両辺に任意の $\sigma \in G$ を作用させると，$G \subset \mathrm{Aut}(K/F)$ が部分群であることから

$$\sigma_i(\alpha_n) = \sum_{j=1}^{r} \sigma(a_j) \sigma_i(\alpha_j) \qquad (i = 1, 2, \cdots, m)$$

となるから

$$v_n = \sigma(a_1)v_1 + \sigma(a_2)v_2 + \cdots + \sigma(a_r)v_r \qquad (\sigma(a_j) \in K) \tag{4.3}$$

となる．(4.1) と (4.3) を比べて $\sigma(a_j) = a_j$ $(j = 1, 2, \cdots, r)$ となる．$\sigma \in G$ は任意だから $a_j \in K^G$ $(j = 1, 2, \cdots, r)$ となる．よって (4.2) で $\sigma_1 = 1$ の部分をみれば

$$\alpha_n = \sum_{i=1}^{r} a_j \alpha_j \qquad (a_j \in K^G)$$

となり，$\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ は K^G 上一次従属となる．■

更に次の命題が成り立つ；

命題 4.2 体 K と有限部分群 $G \subset \mathrm{Aut}(K)$ 及び中間体 $K^G \subset L \subset K$ に対して

1) $H = \mathrm{Aut}(K/L) \subset G$ で $L = K^H$,

2) 全単射 $G/H \to \mathrm{Hom}_{K^G}(L, K)$ が $\sigma H \mapsto \sigma|_L$ により与えられる．特に $\sharp \mathrm{Hom}_{K^G}(L, K) = (L : K^G)$.

[**証明**] $K^G \subset L \subset K$ だから，命題 4.1 より

$$\mathrm{Aut}(K/L) \subset \mathrm{Aut}(K/K^G) = G.$$

G は $\mathrm{Hom}_{K^G}(L, K)$ に $(\sigma, \tau) \mapsto \sigma \circ \tau$ により作用して，$id_L \in \mathrm{Hom}_{K^G}(L, K)$ の G-軌道は

$$\{\sigma \circ id_L \mid \sigma \in G\} = \{\sigma|_L \mid \sigma \in G\}$$

であり，$id_L \in \mathrm{Hom}_{K^G}(L, K)$ の固定部分群は

$$\begin{aligned} \{\sigma \in G \mid \sigma \circ id_L = id_L\} &= \{\sigma \in \mathrm{Aut}(K/K^G) \mid \sigma|_L = id_L\} \\ &= \mathrm{Aut}(K/L) = H \end{aligned}$$

である．よって $K^G \subset L \subset K^H$ と命題 3.7 より

$$|G/H| = \sharp\{\sigma|_L \mid \sigma \in G\} \leq \sharp \mathrm{Hom}_{K^G}(L, K) \leq (L : K^G) \leq (K^H : K^G).$$

一方，命題 4.1 より

$$|G/H| = |G|/|H| = (K : K^G)/(K : K^H) = (K^H : K^G).$$

よって $(L : K^G) = (K^H : K^G)$ より $L = K^H$ となり

$$\sharp\{\sigma|_L \mid \sigma \in G\} = \sharp \mathrm{Hom}_{K^G}(L, K)$$

より 2) を得る．■

以上をまとめると次の定理が示される；

定理 4.3 (Galois 理論の基本定理) 体 K と有限部分群 $G \subset \mathrm{Aut}(K)$ に対して，G の部分群全体の集合を $\mathcal{G}$ とし，K/K^G の中間体全体の集合を $\mathcal{F}$ とすると，$H \mapsto K^H$ は $\mathcal{G}$ から $\mathcal{F}$ への全単射である．その逆写像は $L \mapsto \mathrm{Aut}(K/L)$ である．

[**証明**] $H \in \mathcal{G}$ に対して，命題 4.1 より $\mathrm{Aut}(K/K^H) = H$ となる．$L \subset \mathcal{F}$ に対して，命題 4.2 から $H = \mathrm{Aut}(K/L) \in \mathcal{G}$ で $K^H = L$ となる．■

課題 4.1 素数 p に対して $\omega = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p} \in \mathbb{C}$ とおく．

$$\mathbb{Q}(\omega)^{\mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})} = \mathbb{Q}$$

であることを示せ．

5 Galois 拡大

定理 4.3 を踏まえて，次のように定義する；

定義 5.1 体の拡大 K/F に対して $K^{\mathrm{Aut}(K/F)} = F$ となるとき，K/F は体の **Galois 拡大**であるという．

例 5.2 素数 p に対して $\omega = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p} \in \mathbb{C}$ とおくと，課題 4.1 より，$\mathbb{Q}(\omega)/\mathbb{Q}$ は Galois 拡大である．

定理 4.3 から直ちに

系 5.3 有限次 Galois 拡大 K/F に対して，$\mathrm{Aut}(K/F)$ の部分群全体を $\mathcal{G}$ とし，K/F の中間体全体を $\mathcal{F}$ とすると，$H \mapsto K^H$ は $\mathcal{G}$ から $\mathcal{F}$ への全単射となり，逆写像は $L \mapsto \mathrm{Aut}(K/L)$ である．

定理 5.4 体の有限次拡大 K/F に対して，K/F が Galois 拡大となる必要十分条件は $|\mathrm{Aut}(K/F)| = (K:F)$ なることである．

[**証明**] $G = \mathrm{Aut}(K/F)$ とおくと，命題 4.1 から $|G| = (K : K^G)$ だから，$K^G = F$ と $|G| = (K:F)$ は同値である．■

有限次 Galois 拡大 K/F の中間体に関しては，次の定理が基本的である；

定理 5.5 有限次 Galois 拡大 K/F の中間体 $F \subset L \subset K$ に対して K/L は Galois 拡大である．

[**証明**] 定理 4.3 から　$H = \mathrm{Aut}(K/L)$ に対して $K^H = L$ だから K/L は Galois 拡大である．■

有限次 Galois 拡大 K/F の中間体 $F \subset L \subset K$ に対して，定理 5.5 より K/L は常に Galois 拡大となるが，L/F が Galois 拡大となる条件を求めよう．その準備として，命題 4.2 を言い換えて

命題 5.6 有限次 Galois 拡大 K/F の中間体 $F \subset L \subset K$ に対して

$$\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L) \to \mathrm{Hom}_F(L,K) \qquad (\sigma\mathrm{Aut}(K/L) \mapsto \sigma|_L)$$

は全単射である．特に $\sharp\mathrm{Hom}_F(L,K) = (L:F)$ である．

命題 5.7 有限次 Galois 拡大 K/F の中間体 $F \subset L \subset K$ と $\sigma \in \mathrm{Aut}(K/F)$ に対して，$\sigma(L)$ は K/F の中間体で $\mathrm{Aut}(K/\sigma(L)) = \sigma\mathrm{Aut}(K/L)\sigma^{-1}$ である．

[**証明**] $\tau \in \mathrm{Aut}(K/F)$ に対して，$\tau \in \mathrm{Aut}(K/\sigma(L))$ は $\tau \circ \sigma(x) = \sigma(x)$ $(\forall x \in L)$ と同値であり，これは $\sigma^{-1} \circ \tau \circ \sigma(x) = x$ $(\forall x \in L)$ 即ち $\sigma^{-1} \circ \tau\sigma \in \mathrm{Aut}(K/L)$ と同値である．■

定理 5.8 有限次 Galois 拡大 K/F の中間体 $F \subset L \subset K$ に対して，次は同値である；

1) L/F は Galois 拡大である，

2) $\mathrm{Aut}(K/L)$ は $\mathrm{Aut}(K/F)$ の正規部分群である，

3) 任意の $\sigma \in \mathrm{Aut}(K/F)$ に対して $\sigma(L) = L$ である，

4) $\mathrm{Aut}(L/F) = \mathrm{Hom}_F(L,K)$ である．

このとき $\sigma\mathrm{Aut}(K/L) \mapsto \sigma|_L$ は群の同型

$$\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L) \tilde{\to} \mathrm{Aut}(L/F)$$

を与える．

[**証明**] $\mathrm{Aut}(L/F) \subset \mathrm{Hom}_F(L,K)$ で，命題 5.6 より $\sharp\mathrm{Hom}_F(L,K) = (L:F)$ だから，1) と 4) が同値であることは定理 5.4 から従う．一方，命題 5.7 より 2) と 3) が同値であることがわかる．更に命題 5.6 より

$$\mathrm{Hom}_F(L,K) = \{\sigma|_L \mid \sigma \in \mathrm{Aut}(K/F)\}$$

だから 3) と 4) が同値であることが示される．さて同値な 1),2),3),4) が成り立つとき，命題 5.6 より $\sigma \mapsto \sigma|_L$ は $\mathrm{Aut}(K/F)$ から $\mathrm{Aut}(L/F)$ への全射群準同型写像で，その核が $\mathrm{Aut}(K/L)$ となる．よって群の準同型定理から求める群の同型を得る．■

課題 5.1 素数 $p > 2$ に対して

$$\omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p} \in \mathbb{C}$$

とおくと，課題 4.1 より $\mathbb{Q}(\omega)/\mathbb{Q}$ は Galois 拡大である．

1) p で割り切れない整数 $n \in \mathbb{Z}$ に対して $\sigma_n(\omega) = \omega^n$ なる $\sigma \in \mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})$ が定まることを示せ．

2) 体 $\mathbb{Z}/p\mathbb{Z}$ の乗法群は

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{n} \in \mathbb{Z}/p\mathbb{Z} \mid p \not| n\} = \left\{\overline{1}, \overline{2}, \cdots, \overline{p-1}\right\}$$

であることを示せ．

3) $\overline{n} \mapsto \sigma_n$ は群の同型

$$(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})$$

を与えることを示せ．

注意 5.9 一般に体 K の乗法群 $K^\times$ の有限部分群は常に巡回群であることが証明できる．特に，素数 p に対して，体 $\mathbb{Z}/p\mathbb{Z}$ の乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である．例えば $p = 5$ の場合

$$2^2 = 4 \equiv -1 \pmod 5, \quad 2^3 = 8 \equiv 3 \pmod 5, \quad 2^4 \equiv (-1)^2 = 1 \pmod 5$$

だから

$$(\mathbb{Z}/5\mathbb{Z})^\times = \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\right\} = \langle\overline{2}\rangle$$

となる．

6　多項式の分解体

以下，体 F を固定しておく．

命題 6.1 任意の多項式 $f(X) \in F[X]$ に対して，体の拡大 K/F で

$$f(X) = a(X - \alpha_1) \cdots (X - \alpha_n) \qquad (a \in F, \alpha_i \in K)$$

なるものが存在する．そのような K で最小のもの，即ち $F(\alpha_1, \cdots, \alpha_n)$ を $f(X)$ の F 上の**分解体** と呼ぶ．

[**証明**] $n = \deg f(X)$ に関する数学的帰納法により証明する．

i) $n = 1$ のとき，$f(X) = aX + b$ $(a, b \in F, a \neq 0)$ だから，$K = F$ で十分である．

ii) $n - 1$ のとき成り立つと仮定して $n > 1$ のとき．$f(X)$ を割り切る既約多項式 $p(X) \in F[X]$ が存在する．$E = F[X]/(p(X))$ は体で，環の単射準同型写像

$$F \to E = F[X]/(p(X)) \qquad (a \mapsto \overline{a})$$

が成り立つから，これにより F を $E = F[X]/(p(X))$ の部分体と同一視する．即ち E は F の拡大体で $\alpha = \overline{X} \in E$ とおくと

$$p(\alpha) = \overline{p(X)} = 0 \in E = F[X]/(p(X))$$

となる．即ち $f(\alpha) = 0$ となるから $f(X) = (X - \alpha)g(X)$ $(g(X) \in E[X])$ とおく．$\deg g(X) = n - 1$ だから，帰納法の仮定から E の拡大体 K があって

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_{n-1}) \qquad (\alpha_1, \cdots, \alpha_{n-1} \in K)$$

とできる．このとき K は F の拡大体で

$$f(X) = (X - \alpha)(X - \alpha_1)(\cdots (X = \alpha_{n-1}) \quad (\alpha, \alpha_1, \cdots, \alpha_{n-1} \in K)$$

となる．■

以前に示した定理 3.3 を簡単化した次の命題を思い出しておく：

命題 6.2 体の拡大 L/F に対して，$\alpha \in L$ は既約多項式 $p(X) \in F[X]$ の根とする．L に含まれる $p(X)$ の相異なる根の全体を $\{\alpha_1, \cdots, \alpha_r\} \subset L$ とすると

$$\mathrm{Hom}_F(F(\alpha), L) \ni \sigma \mapsto \sigma(\alpha) \in \{\alpha_1, \cdots, \alpha_r\}$$

は全単射である．

基本的なことは

命題 6.3 $f(X) \in F[X]$ の F の分解体を K として，中間体 $F \subset L \subset K$ をとる．このとき

1) $\mathrm{Aut}(K/F) \to \mathrm{Hom}_F(L, K)$ $(\sigma \mapsto \sigma|_L)$ は全射である．

2) L がある多項式 $g(X) \in F[X]$ の F 上の分解体ならば

$$\mathrm{Hom}_F(L, K) = \mathrm{Aut}(L/F)$$

である．

[**証明**] 1) $\tau \in \mathrm{Hom}_F(L, K)$ とする．$L \lneqq K$ ならば $f(\alpha) = 0$ なる $\alpha \in K$ で L に含まれないものがある．$\alpha \in K$ の L 上の最小多項式を $p(X) \in L[X]$ とすると，$p^\tau(X) \in \tau(L)[X]$ で $p^\tau(X)|f(X)$ だから，$p^\tau(\beta) = 0$ なる $\beta \in K \subset K$ がある．このとき

$$\begin{aligned} L[X]/(p(X)) &\tilde{\to} L(\alpha) \qquad (\overline{\varphi(X)} \mapsto \varphi(\alpha)), \\ \tau(L)[X]/(p^\tau(X)) &\tilde{\to} \tau(L)(\beta) \qquad (\overline{\psi(X)} \mapsto \psi(\beta)) \end{aligned}$$

だから，$\varphi(\alpha) \mapsto \varphi^\tau(\beta)$ $(\varphi \in L[X])$ が $\rho \in \mathrm{Hom}_F(L(\alpha), K)$ を定義し $\rho|_{L(\alpha)} = \tau$ となる．以下同様に続ければ，$\sigma|_L = \tau$ なる $\sigma \in \mathrm{Aut}(K/F)$ を得る．

2) 任意の $\sigma \in \mathrm{Hom}_F(L, K)$ に対して $\sigma(L)$ は $g^\sigma(X)$ の F 上の分解体となるが，$g(X) \in F[X]$ だから $g^\sigma(X) = g(X)$，従って $\sigma(L) = L$ である．よって $\sigma \in \mathrm{Aut}(L/F)$ となる．∎

以上の準備の下に，有限次 Galois 拡大は次のように特徴付けられる；

定理 6.4 体の有限次拡大 K/F に対して次は同値である；

1) K/F は Galois 拡大である，

2) 既約多項式 $p(X) \in F[X]$ が K に根を持てば，$p(X)$ は重根をもたず K で一次式の積に分解する，

3) K は或る $f(X) \in F[X]$ の F 上の分解体で，K の任意の元の F 上の最小多項式は重根を持たない．

[**証明**] 1) $\Rightarrow$ 2) K における $p(X)$ の相異なる根の全体を $S = \{\alpha_1, \cdots, \alpha_r\}$ とすると $\sigma \in G = \mathrm{Aut}(K/F)$ は S 上の置換を生ずるから

$$q(X) = \prod_{i=1}^{r} (X - \alpha_i) \in K^G[X] = F[X]$$

であり，$q(X)|p(X)$ である．$p(X) \in F[X]$ は既約だから $p(X) = c \cdot q(X)$ $(c \in F)$ となり，$p(X)$ は重根を持たず K で一次式の積に分解する．

2) $\Rightarrow$ 3) $K = F(\alpha_1, \cdots, \alpha_r)$ として $\alpha_i \in K$ の F 上の最小多項式を $p_i(X) \in F[X]$ とする．$p_i(X)$ は重根を持たず K で一次式の積に分解するから，K は $f(X) = \prod_{i=1}^{r} p_i(X) \in F[X]$ の F 上の分解体となる．

3) $\Rightarrow$ 1) $G = \mathrm{Aut}(K/F)$ として $\alpha \in K^G$ をとる．α の F 上の最小多項式を $p(X) \in F[X]$ として，$f(X)p(X) \in F[X]$ の F 上の分解体を L $(K \subset L)$ とする．命題 6.3 より

$$\mathrm{Aut}(L/F) \to \mathrm{Hom}_F(F(\alpha), L) \qquad (\sigma \mapsto \sigma|_{F(\alpha)})$$

と

$$\mathrm{Aut}(L/F) \to \mathrm{Aut}(K/F) \qquad (\sigma \mapsto \sigma|_K)$$

は共に全射だから

$$\mathrm{Aut}(K/F) \to \mathrm{Hom}_F(F(\alpha), L) \qquad (\sigma \mapsto \sigma|_{F(\alpha)})$$

は全射である．一方 $\alpha \in K^G$ $(G = \mathrm{Aut}(K/F))$ だから，任意の $\sigma \in \mathrm{Aut}(K/F)$ に対して $\sigma|_{F(\alpha)} = \mathrm{id}_{F(\alpha)}$ である．よって

$$\mathrm{Hom}_F(F(\alpha), L) = \{id_{F(\alpha)}\}$$

となり，命題 6.2 より $p(X)$ の L における根は 1 個である．$p(X)$ は重根を持たないから，$p(X) = X - \alpha$ である．即ち $\alpha \in F$ となる．よって $E^G = F$ である．■

$n(> 1)$ 次既約多項式 $p(X) \in F[X]$ を一つ固定して考えよう．$p(X)$ の F 上の分解体を E として $\alpha \in E$ を $p(X)$ の根の一つとする．$\mathrm{Aut}(F(\alpha)/F) \subset \mathrm{Hom}_F(F(\alpha), E)$ で，命題 6.2 から

$$|\mathrm{Aut}(F(\alpha)/F)| \leq \sharp\mathrm{Hom}_F(F(\alpha), E) \leq \deg p(X) = (F(\alpha) : F)$$

である．ここで定理 5.4 に注意すると，$F(\alpha)/F$ が Galois 拡大となる必要十分条件は

1) $p(X)$ の根は全て $F(\alpha)$ に含まれ，かつ

2) $p(X)$ は重根を持たない

ことである．$p(X)$ の根全体を $\mathbb{X} = \{\alpha_1, \cdots, \alpha_n\}$ として

$$\sigma_i : F(\alpha) \ni \sum_{j=0}^{n-1} a_j \alpha^j \mapsto \sum_{j=0}^{n-1} a_j \alpha_i^j \in F(\alpha) \qquad (i = 1, \cdots, n)$$

とおくと $\mathrm{Aut}(F(\alpha)/F) = \{\sigma_1, \cdots, \sigma_n\}$ である．また $\sigma \in \mathrm{Aut}(F(\alpha)/F)$ とすると，$\gamma \in \mathbb{X}$ ならば $\sigma(\gamma) \in \mathbb{X}$ となって，$\sigma|_{\mathbb{X}}$ は $\mathbb{X}$ 上の全単射となる．即

ち，$\sigma \mapsto \sigma|_{\mathbb{X}}$ は $\mathrm{Aut}(F(\alpha)/F)$ から n 次対称群 $S(\mathbb{X}) = S_n$ への単射群準同型写像となる．従って $\mathrm{Aut}(F(\alpha)/F)$ は $p(X)$ の根の置換群の部分群（と同型）である．

例 6.5 p を素数とすると

$$p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$$

は既約多項式である．その根は 1 の p-乗根で

$$\omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p} \in \mathbb{C}$$

とおくと

$$p(X) = (X-\omega)(X-\omega^2)\cdots(X-\omega^{p-1})$$

である．よって $\mathbb{Q}(\omega)/\mathbb{Q}$ は Galois 拡大となり $(\mathbb{Q}(\omega):\mathbb{Q}) = p-1$ である．$m, n \in \mathbb{Z}$ にたいして

$$\omega^m = \omega^n \ \Leftrightarrow\ m \equiv n \pmod{p}$$

に注意すれば，群の同型

$$(\mathbb{Z}/(p))^\times \ni \overline{n} \tilde{\to} \sigma_n \in \mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})$$

が成り立つことがわかる．ここで $\sigma_n \in \mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})$ は $\sigma_n(\omega) = \omega^n$ により定義される．

7　方程式の代数的可解性

以下，考える体は全て複素数体 $\mathbb{C}$ の部分体であると仮定する．自然数 n に対して

$$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid k = 0, 1, 2, \cdots, n-1\right\}$$

とおく．

7.1　可解群

定義 7.1.1 群 G に対して，G の部分群の列

$$G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_{r-1} \supset N_r = \{1\}$$

があって，$i = 0, 1, 2, \cdots, r-1$ に対して N_{i+1} は N_i の正規部分群であり N_i/N_{i+1} が可換群となるとき，G は**可解群**であるという．

命題 7.1.2　1) 可解群の部分群は可解群である.

2) 群 G の正規部分群 $N \subset G$ に対して

$$G \text{ は可解群} \quad \Leftrightarrow \quad N \text{ と } G/N \text{ が可解群.}$$

3) 可解群 G に対して，G の部分群の列

$$G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_{r-1} \supset N_r = \{1\}$$

があって，$i = 0, 1, 2, \cdots, r-1$ に対して N_{i+1} は N_i の正規部分群であり N_i/N_{i+1} が素数次巡回群となるものが存在する.

7.2　体の冪根拡大と可解拡大

定義 7.2.1 $X^n - a \in F[X]$ の F 上の分解体を F の**冪根拡大**と呼ぶ.

定義 7.2.2 体の有限次 Galois 拡大 K/F に対して，$\mathrm{Aut}(K/F)$ が可解群のとき，K/F を**可解拡大**と呼ぶ.

命題 7.2.3 冪根拡大 E/F は可解拡大である.

[**証明**] E は $X^n - a \in F[X]$ の F 上の分解体とする．$\alpha^n = a$ なる $\alpha \in E$ をとり $\mu_n = \{\zeta \in E \mid \zeta^n = 1\}$ とおく．$\mu_n \subset E^\times$ は有限部分群だから巡回群となり，$\mu_n = \langle \omega \rangle$ とおく．$F(\omega)$ は $X^n - 1$ の F 上の分解体だから $F(\omega)/F$ は Galois 拡大で $\sigma \in \mathrm{Aut}(F(\omega)/F)$ に対して $\sigma(\omega) = \omega^t$ ($t \in \mathbb{Z}$ s.t. $\mathrm{GCD}\{t, n\} = 1$) となる．このとき群準同型写像

$$\mathrm{Aut}(F(\omega)/F) \to (\mathbb{Z}/(n))^\times \qquad (\sigma \mapsto \bar{t})$$

は単射となる．よって $\mathrm{Aut}(F(\omega)/F)$ は可換群である．$\tau \in \mathrm{Aut}(E/F(\omega))$ に対して $\tau(\alpha)/\alpha \in \mu_n$ で，$\sigma, \tau \in \mathrm{Aut}(E/F(\omega))$ に対して

$$\sigma \circ \tau(\alpha)/\alpha = \frac{\sigma \circ \tau(\alpha)}{\sigma(\alpha)} \frac{\sigma(\alpha)}{\alpha} = \frac{\tau(\alpha)}{\alpha} \frac{\sigma(\alpha)}{\alpha}$$

だから

$$\mathrm{Aut}(E/F(\alpha)) \to \mu_n \qquad (\tau \mapsto \tau(\alpha)/\alpha)$$

は単射群準同型写像となる．よって $\mathrm{Aut}(E/F(\omega))$ は可換群である．$\mathrm{Aut}(E/F(\omega)) \triangleleft \mathrm{Aut}(E/F)$ で

$$\mathrm{Aut}(E/F)/\mathrm{Aut}(E/F(\omega)) \xrightarrow{\sim} \mathrm{Aut}(F(\omega)/F)$$

だから $\mathrm{Aut}(E/F)$ は可解群となる．■

命題 7.2.4 n 次 Galois 拡大 E/F に対して，$\mathrm{Aut}(E/F)$ が巡回群であるとする．$\mu_n \subset F$ ならば E/F は冪根拡大である．

[**証明**] $\mathrm{Aut}(E/F) = \langle\sigma\rangle$ とすると，F 上の線形写像 $\sigma \in \mathrm{End}_F(E)$ の最小多項式は $X^n - 1$ である（定理 3.6）．一方，$\mu_n = \langle\omega\rangle$ とすると ω は $X^n - 1$ の根，従って $\sigma \in \mathrm{End}_F(E)$ の固有値である．よって $\sigma(\alpha) = \omega\alpha$ なる $0 \neq \alpha \in E$ がある（固有ベクトル）．よって

$$\sigma^i(\alpha) = \omega^i\alpha \neq \alpha \quad (i = 1, 2, \cdots, n-1)$$

より $\mathrm{Aut}(E/F(\alpha)) = \{1\}$．よって $E = F(\alpha)$ となる．一方，$\sigma(\alpha^n) = \sigma(\alpha)^n = \omega^n\alpha^n = \alpha^n$ だから $\alpha^n = a \in F$ である．即ち E は $X^n - a \in F[X]$ の F 上の分解体である．■

命題 7.2.5 体の有限次 Galois 拡大 K/F と L/K が共に可解拡大ならば，可解拡大 M/F で $L \subset M$ なるものが存在する．

[**証明**] K は $f(X) \in F[X]$ の F 上の分解体とし，L は $g(X) \in K[X]$ の K 上の分解体であるとする．$\sigma \in \mathrm{Aut}(K/F)$ に対して $g^\sigma(X) \in K[X]$ の K 上の分解体を L_σ とする．

$$h(X) = f(X) \cdot \prod_{\sigma \in \mathrm{Aut}(K/F)} g^\sigma(X) \in F[X]$$

の F 上の分解体を M とすると，M は K 及び $L\sigma$ ($\sigma \in \mathrm{Aut}(K/F)$) 全てを含む最小の体である．ここで $\mathrm{Aut}(L_\sigma/K)$ ($\sigma \in \mathrm{Aut}(K/F)$) は $\mathrm{Aut}(L/K)$ と同型だから可解群である．更に

$$\mathrm{Aut}(M/K) \to \prod_{\sigma \in \mathrm{Aut}(K/F)} \mathrm{Aut}(L_\sigma/K) \qquad \left(\tau \mapsto (\tau|_{L_\sigma})_{\sigma \in \mathrm{Aut}(K/F)}\right)$$

は単射群準同型写像だから，$\mathrm{Aut}(M/K)$ は可解群である．一方

$$\mathrm{Aut}(M/F)/\mathrm{Aut}(M/K) \xrightarrow{\sim} \mathrm{Aut}(K/F) \quad (\sigma\mathrm{Aut}(M/K) \mapsto \sigma|_K)$$

だから $\mathrm{Aut}(M/F)/\mathrm{Aut}(M/K)$ は可解群である．よって命題 7.1.2 の 2) より $\mathrm{Aut}(M/F)$ は可解群である．■

7.3 方程式の可解性

定義 7.3.1 1) 多項式 $f(X) \in F[X]$ の F 上の分解体を K としたとき $\mathrm{Aut}(K/F)$ を $f(X)$ の F 上の **Galois 群** と呼び $\mathrm{Aut}(f(X)/F)$ と書く．

2) 多項式 $f(X) \in F$ の F 上の分解体を K としたとき，拡大体の列

$$F = F_0 \subset F_1 \subset \cdots \subset F_m$$

があって $K \subset F_m$ かつ F_{i+1}/F_i $(1 = 0, 1, \cdots, m-1)$ が冪根拡大であるとき，$f(X)$ は F **上代数的に可解** であるという．

定理 7.3.2 多項式 $f(X) \in F[X]$ が F 上代数的に可解である必要十分条件は $\mathrm{Aut}(f(X)/F)$ が可解群なることである．

[**証明**] $f(X)$ の F 上の分解体を K とする．$f(X)$ が F 上代数的に可解であるとして，拡大体の列

$$F = F_0 \subset F_1 \subset \cdots \subset F_m$$

があって $K \subset F_m$ かつ F_{i+1} は $X^{m_i} - \alpha_i \in F_i[X]$ の F_i 上の分解体であるとする．命題 7.2.3 から F_l/F_{m-1}, F_{m-1}/F_{m-2} は共に可解拡大だから，命題 7.2.5 より，可解拡大 L_1/F_{l-2} であって $F_l \subset L_1$ なるものが存在する．F_{m-2}/F_{m-3} は可解拡大だから，同じく命題 7.2.5 より，可解拡大 L_2/F_{m-3} で $F_m \subset L_1 \subset L_2$ なるものが存在する．以下同様にして，可解拡大 L_{m-1}/F_0 で $F_m \subset L_{m-1}$ なるものが存在する．よって $\mathrm{Aut}(L_{m-1}/F)$ は可解群で，全射群準同型写像

$$\mathrm{Aut}(L_{m-1}/F) \to \mathrm{Aut}(K/F) \qquad (\sigma \mapsto \sigma|_K)$$

があるから，命題 7.1.2 の 2) より $\mathrm{Aut}(K/F)$ は可解群となる．

逆に $\mathrm{Aut}(f(X)/F) = \mathrm{Aut}(K/F)$ が可解であるとして，中間体の列

$$F = F_0 \subset F_1 \subset \cdots \subset F_l = K$$

があって $\mathrm{Aut}(K/F_{i+1}) \triangleleft \mathrm{Aut}(K/F_i)$（従って F_{i+1}/F_i は Galois 拡大）かつ

$$\mathrm{Aut}(K/F_i)/\mathrm{Aut}(K/F_{i+1}) \tilde{\to} \mathrm{Aut}(F_{i+1}/F_i)$$

が巡回群であるとする．$n = (K : F) = |\mathrm{Aut}(K/F)|$ として $L_i = F_i(\mu_n)$ とおくと

$$\mathrm{Aut}(L_{i+1}/L_i) \to \mathrm{Aut}(F_{i+1}/F_i) \qquad (\sigma \mapsto \sigma|_{F_{i+1}})$$

は単射群準同型写像だから $\mathrm{Aut}(L_{i+1}/L_i)$ は巡回群となり

$$|\mathrm{Aut}(L_{i+1}/L_i)| \big| |\mathrm{Aut}(F_{i+1}/F_i)|, \qquad |\mathrm{Aut}(F_{i+1}/F_i)| \big| |\mathrm{Aut}(K/F)|$$

である．よって命題 7.2.4 より L_{i+1}/L_i は冪根拡大となる．$L_0 = F(\mu_n)$ だから L_0/F も冪根拡大で $K \subset L_l$ だから $f(X)$ は F 上代数的に可解である．
■

7.4 一般の n 次方程式

$\alpha_1, \cdots, \alpha_n$ を有理数体 $\mathbb{Q}$ 上の変数として $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ とおく．n 次対称群の元 $\sigma \in S_n$ を $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ により $\sigma \in \mathrm{Aut}(K/\mathbb{Q}) \subset \mathrm{Aut}(K)$ と同一視すると，$S_n \subset \mathrm{Aut}(K)$ は有限部分群である．$\alpha_1, \alpha_2, \cdots, \alpha_n$ の対称式は基本対称式

$$a_k = (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} \alpha_{i_1} \cdots \alpha_{i_k} \qquad (k = 1, 2, \cdots, n)$$

の有理式として書けるから（対称式論の基本定理）

$$F = K^{S_n} = \mathbb{Q}(a_1, \cdots, a_n)$$

となり，命題 4.1 と 定理 5.4 から K/F は Galois 拡大で $\mathrm{Aut}(K/F) = S_n$ である．ここで K は

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in F[X]$$

の F 上の分解体となるから，$\mathrm{Aut}(f(X)/F) = S_n$ である．

$n \ge 5$ のとき A_n は非自明な正規部分群を持たない非可換群だから，A_n は可解群でない．よって $\mathrm{Aut}(f(X)/F) = S_n$ は可解でない．

7.5 一般の 3 次方程式

7.4 節の記号で，$n = 3$ のとき $a = a_1, b = a_2, c = a_3$ として

$$f(X) = X^3 + aX^2 + bX + c = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

の $F = \mathbb{Q}(a, b, c)$ 上の分解体が $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ で $\mathrm{Aut}(f(X)/F) = S_3$ である．

3 次交代群 A_3 は S_3 の正規部分群で，S_3/A_3 は 2 次巡回群，A_3 は 3 次次巡回群となるから，3 次対称群 S_3 は可解群である．よって一般の 3 次方程式 $f(X) = 0$ は冪根による解の公式をもつ．

$\mu_3 = \langle \omega \rangle$ として $\omega^2 + \omega + 1 = 0$ である．

$$\begin{cases} u = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \\ v = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 \end{cases}$$

とおくと，$-a = \alpha_1 + \alpha_2 + \alpha_3$ だから

$$\begin{cases} \alpha_1 = \dfrac{1}{3}(u + v - a), \\ \alpha_2 = \dfrac{1}{3}(\omega^2 u + \omega v - a), \\ \alpha_3 = \dfrac{1}{3}(\omega u + \omega^2 v - a) \end{cases}$$

である．

	$(1,2)$	$(1,3)$	$(2,3)$
u	ωv	$\omega^2 v$	v
v	$\omega^2 u$	ωu	u
u^3	v^3	v^3	v^3
v^3	u^3	u^3	u^3
uv	uv	uv	uv.

だから

$$u^3+v^3=B\in F,\qquad uv=C\in F$$

である．$\delta=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)$ とおくと，$\delta^2=D(f)\in F$ は $f(X)$ の判別式で

$$u^3-v^3=3(\omega-\omega^2)\delta,\qquad \left(u^3-v^3\right)^2=-27\cdot D(f)$$

である．

1) $X^2+27\cdot D(f)\in F[X]$ の F 上の分解体を F_1 とおくと，$\{u^3,v^3\}\subset F_1$,

2) $X^3-u^3\in F_1[X]$ の F_1 上の分解体を F_2 とおくと，$\{\omega,u,v\}\subset F_2$.

即ち拡大体の列

$$F=F_0\subset F_1\subset F_2$$

があって，F_{i+1}/F_i $(i=0,1)$ が冪根拡大であり $K\subset L_2$ となる．

具体的には u^3,v^3 は二次方程式

$$T^2-BT+C^3=0$$

の二根となるが

$$\begin{aligned}B^2-4C^3&=\left(u^3+v^3\right)^2-4u^3v^3=\left(u^3-v^3\right)^2\\&=-27\cdot D(f)\end{aligned}$$

だから

$$u^3,v^3=\frac{B\pm\sqrt{B^2-4C^3}}{2}=\frac{B\pm\sqrt{-27\cdot D(f)}}{2}$$

である．

7.6 一般の 4 次方程式

7.4 節の記号で $n=4$ のとき，$a_1=a,a_2=b,a_3=c,a_4=d$ とおくと

$$\begin{aligned}f(X)&=X^4+aX^3+bX^2+cX+d\\&=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)\end{aligned}$$

の $F=\mathbb{Q}(a,b,c,d)$ 上の分解体が $K=\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ で

$$\mathrm{Aut}(f(X)/F)=S_4$$

である．

$$\begin{cases} u=\alpha_1+\alpha_2-(\alpha_3+\alpha_4), \\ v=\alpha_1+\alpha_3-(\alpha_2+\alpha_4), \\ w=\alpha_1+\alpha_4-(\alpha_2+\alpha_3) \end{cases}$$

とおくと，$-a=\alpha_1+\alpha_2+\alpha_3+\alpha_4$ だから

$$\begin{cases} \alpha_1=\dfrac{1}{4}(u+v+w-a), \\ \alpha_2=\dfrac{1}{4}(u-v-w+a), \\ \alpha_3=\dfrac{1}{4}(-u+v-w-a), \\ \alpha_4=\dfrac{1}{4}(-u-v+w-a) \end{cases}$$

となる．ここで

	$(1,2)$	$(1,3)$	$(1,4)$	$(2,3)$	$(2,4)$	$(3,4)$
u	u	$-w$	$-v$	v	w	u
v	$-w$	v	$-u$	u	v	w
w	$-v$	$-u$	w	w	u	v
u^2	u^2	w^2	v^2	v^2	w^2	u^2
v^2	w^2	v^2	u^2	u^2	v^2	w^2
w^2	v^2	u^2	w^2	w^2	u^2	v^2.

よって S_4 は $X=\{u^2,v^2,w^2\}$ に作用して，付随する群準同型写像

$$(*):S_4\to S(X)=S_3$$

は全射となる．

$$\begin{aligned} V&=\mathrm{Ker}[(*):S_4\to S_3] \\ &=\{\mathbf{1},(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} \end{aligned}$$

とおくと（V を Klein の四元群と呼ぶ），S_4 の正規部分群の列

$$S_4\supset A_4\supset V\supset\{1\}$$

が出来て

1) $S_4/A_4\simeq\{\pm1\}$ は 2 次巡回群,

2) $|A_4/V|=12/4=3$ だから，A_4/V は 3 次巡回群,

3) $|V|=2^2$ だから，V は可換群

となり，$\mathrm{Aut}(f(X)/F) = S_4$ は可解群である．よって一般の 4 次方程式 $f(X) = 0$ は冪根による解の公式をもつ．

具体的には

$$A = u^2 + v^2 + w^2, \quad B = v^2v^2 + v^2w^2 + w^2u^2, \quad C = uvw$$

は全て S_4 の作用で不変だから，対称式論の基本定理により，$F = \mathbb{Q}(a, b, c, d)$ の元である．よって 3 次方程式の解の公式により

$$g(X) = T^3 - AT^2 + Bt - C^2 = 0$$

を解いて，u^2, v^2, w^2 が求まり，それらの平方根を $uvw = C$ となるように選んで，$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ が求められる．

具体的な冪根拡大を次の通りである：

$$\begin{aligned}\delta = &\prod_{1\le i<j\le 4}(\alpha_i - \alpha_j)\\ =&(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)\\ &(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)\\ &(\alpha_3 - \alpha_4)\end{aligned}$$

とおくと，$D(f) = \delta^2 \in F$ が $f(X)$ の判別式である．ここで

$$u^2 - v^2 = (u + v)(u - v) = 2^2(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$$

等々から $(u^2 - v^2)(u^2 - w^2)(v^2 - w^2) = 2^6\delta$，よって $D(g) = 2^{12}D(f)$ となる．そこで

$$\begin{cases} s = u^2 + \omega v^2 + \omega^2 w^2, \\ t = u^2 + \omega^2 v^2 + \omega w^2 \end{cases}$$

とおいて，7.5 節の 3 次方程式の分解体の列を参考にすると，

1) $X^2 + 27D(g) = X^2 + 2^{12}3^3D(f)$ の F 上の分解体を F_1 とおくと，$\{s^3, t^3\} \subset F_1$,

2) $X^3 - s^3 \in F_1[X]$ の F_1 上の分解体を F_2 とおくと $\{\omega, s, t\} \subset F_2$, よって $\{u^2, v^2, w^2\} \subset F_2$,

3) $X^2 - u^2 \in F_2[X]$ の F_2 上の分解体を F_3 とし，$X^2 - v^2 \in F_3[X]$ の F_3 上の分解体を F_4 とおくと，$\{u, v, w\} \subset F_4$

となる．即ち拡大体の列

$$F = F_0 \subset F_1 \subset F_2 \subset F_3 \subset F_4$$

があって，F_{i+1}/F_i $(i = 0, 1, 2, 3)$ が冪根拡大であり $K \subset F_4$ となる．