数理解析研究所講究録
1154巻 2000年 125-136

二面体群に対するガロアの逆問題

早稲田大学理工学部: 橋本喜一朗
(Ki-ichiro HASHIMOTO)

§0 序文

一般に有限群の群拡大

$$\varepsilon(G/N): \qquad 1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} G/N \longrightarrow 1 \qquad (\text{exact})$$

と体のガロア拡大 K/k で $\mathrm{Gal}(K/k) \cong G/N$ なるものが与えられたとき, K を含む k のガロア拡大 L/k で図式

$$\begin{array}{ccc} \mathrm{Gal}(L/k) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(K/k) \\ \cong\downarrow & & \downarrow\cong \\ G & \xrightarrow{\pi} & G/N \end{array}$$

を可換にするものの集合を $\mathrm{Emb}(G/N, K/k)$ とかく. ガロア理論における「埋蔵問題」とは,

•(問題 1) どのような条件下で $\mathrm{Emb}(G/N, K/k) \neq \emptyset$ となるか?

を問うものである. いわゆる「ガロアの逆問題」は, 与えられた有限群 G と体 k に対して 自明な拡大 $\varepsilon(G/G)$ に対応する (問題 1) のことをさす. すなわち集合

$$\mathrm{Emb}(G,k) := \mathrm{Emb}(G/G, k/k) = \{L/k \mid \mathrm{Gal}(L/k) \cong G\}$$

が空か否かを問題にするが, 最も重要な $k = \mathbf{Q}$ の場合において近年目覚しい進展があり, 多くの有限群 G が $\mathbf{Q}$ 上のガロア群となることが示されたことは周知の処である. 他方, さらに一歩進んで

•(問題 2) 集合 $\mathrm{Emb}(G/N, K/k)$ を記述せよ: それは如何なる "構造" をもつか?

•(問題 3) $\mathrm{Emb}(G/N, K/k)$ の各元 L/k を具体的に構成せよ.

という問題が考えられる. ここでいう "構造" とは, 集合 $\mathrm{Emb}(G/N, K/k)$ の適当な座標 (パラメータ) 付け, 又は代数多様体などから $\mathrm{Emb}(G/N, K/k)$ への射を与える, 等々を意味する. このような問題が「ガロアの逆問題」の次の段階として重要であることは明白であるが, これらは G が簡単な群の場合でも容易な問題ではない. 一例として, $\mathbf{Q}$ 上のアーベル拡大は Kronecker-Weber の定理によって「(全て) 決定されている」という主張は一面では正しいが, $G \cong \mathbf{Z}/2\mathbf{Z}$

の場合を除き, $\mathrm{Emb}(G, \mathbf{Q})$ をきちんと座標 (パラメータ) 付ける問題には「素数分布」の問題が含まれ, 巡回群 $G \cong C_n := \mathbf{Z}/n\mathbf{Z}$ $(n = 3, 4, 5, \ldots)$ の場合でも簡単ではないことを注意する. 例として $G \cong C_3$, S_3 のとき, $\mathrm{Emb}(G, \mathbf{Q})$ は $\mathbf{A}^1(\mathbf{Q})$ によって cover されることが知られている (Serre [Se2]) が [Se2] に略述されている証明は易しくはない. 本文はこれらの初等的な証明を含むものである.

(問題 2),(問題 3) に対する我々の方法は, 「ガロアの逆問題」に対する古典的方法である E.Noether のアプローチの変形である. その概略は以下の通り:

•(A-1) G を有理関数体 $k(x)$ の自己同型群 $\mathrm{Aut}_k(k(t)) \cong \mathrm{PGL}_2(k)$ に埋め込み, 不変体 $k(x)^G$ を考察する. これと Lüroth の定理とを組み合わせると G をガロア群にもつ有理関数体 $k(s)$ 上の k 上正則なガロア拡大 $k(x)/k(s)$ が得られる:

•(A-2) $L \in \mathrm{Emb}(G, k)$ に対して, 正規底定理によって, G 加群 L の既約分解を行い, その 2 次元既約成分への G の作用を考察する.

•(A-3) (A-1) と (A-2) の比較により, 適当な条件下で (A-1) から得られる G-拡大のパラメータ族が生成的 (generic), すなわち specialization map $\mathbf{A}^1(\mathbf{k}) \longrightarrow \mathrm{Emb}(G, k)$ が全射を与えることが結論される.

以上のアプローチがうまく行くためには, G が $\mathrm{PGL}_2(k)$ の部分群と同型, 従って $G \cong C_n$, D_n (n 次 二面体群), S_4, A_4, A_5 のいずれかでなければならない. ここでは, 最も簡単な非アーベル群である 二面体群 D_n を考察するが, アイデアを明確にするために, 巡回群 C_n の場合から始めることにする.

以下では簡単のため, $\mathrm{char}(k) = 0$ とする. また, この場合 基礎体 k は $\omega_n := \zeta_n + {\zeta_n}^{-1}$ ($\zeta_n = e^{2\pi\sqrt{-1}/n}$ は 1 の原始 n 乗根) としなければならない.

§1 巡回群の場合

$G =< \alpha > \cong C_n$ とする. この時, 上記の仮定を充たす体 k に対して, G の k 上の群環を $k[G]$ と書くとき,

$$k[G] \cong k[X]/(X^n - 1) \cong \bigoplus_{d|n} k[X]/(\Phi_d(X)).$$

但し, $\Phi_d(X)$ は円分多項式 ($\varphi(d)$ 次). いま, $\zeta_n \in k$ と仮定すると, $X^n - 1$ は $k[X]$ 内で完全分解するから, $k[G] = \oplus_{i=1}^n k^{(i)}$, $k^{(i)} \cong k$ と分解し, $G =< \alpha >$ の第 i 成分 k への作用は $\alpha(z) = {\zeta_n}^i z$ $(\forall z \in k^{(i)})$ で与えられる. 従って, L/k が n 次巡回拡大なら 正規底定理によって $\mathrm{Gal}(L/k)$ 加群として $L \cong k[G]$ であるから $i = 1$ に対応する成分 ($\cong k$) の元 $z \in L^\times$ について $\alpha(z) = \zeta_n z$, $a := z^n \in k^\times$. こうして, Kummer 拡大の基本定理

$$\mathrm{Emb}(C_n, k) \approx k^\times/(k^\times)^n, \qquad L = k(\sqrt[n]{a}) \longleftrightarrow a(k^\times)^n$$

を得る. 次に k の仮定 $\zeta_n \in k$ を $\omega_n \in k$ と緩める. 簡単のため, 特に $\zeta_n \notin k$ としよう. このとき, $\Phi_n(X)$ は k 上では $\frac{1}{2}\varphi(n)$ 個の既約 2 次式 $\Psi^{(i)}(X) := X^2 - {\omega_n}^{(i)}X + 1$ $({\omega_n}^{(i)} := {\zeta_n}^i + {\zeta_n}^{-i}, i \in (\mathbf{Z}/n\mathbf{Z})^\times)$ の積に分解し, これらに対応して n 次巡回拡大 L/k は 2 次元既約 G-部分加群 $W^{(i)}$ を持ち, $\alpha|_{W^{(i)}}$ の特性多項式が $\Psi^{(i)}(X)$ である. 明らかに, $W^{(i)} \otimes_k k(\zeta_n) \cong k^{(i)} \oplus k^{(-i)}$ であるから, $i = 1$ に対して

$$W := W^{(1)} = ku + kv, \qquad \alpha \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & \omega_n \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} \tag{1}$$

を充たす基底 u, v が存在する. 更にこのような (u, v) は $k[G] = k[\alpha]$ の作用 (それは 直和成分 $k[\alpha|_{W^{(i)}}] \cong k[X]/(\Psi^{(i)}(X))$ を経由する) を除いて一意的に定まる.

定理 1-1 ([Mi]) n が奇数で k は $\omega_n \in k$ を充たす標数 0 の体とする. L/k を n 次巡回拡大, $\mathrm{Gal}(L/k) =< \alpha >$ とするとき,

$$\alpha(z) \;=\; 1/(\omega_n - z), \qquad L = k(z) \tag{2}$$

をみたす $z \in L$ が存在する.

実際, $z = u/v$ とおけば $\alpha(z) = \dfrac{\alpha(u)}{\alpha(v)} = \dfrac{v}{-u + \omega_n v} = \dfrac{1}{\omega_n - z}$. あとは $L = k(z)$ を示せばよいが, それには z の $< \alpha >$-orbit (共役) が n 個あることを示せばよい. そうならない場合, z は $\alpha^j(z) = z, 0 < \exists\, j < n$ の形の関係式を充たす. 従ってそのような z は有限個しかないが, 上記の注意により k 上一次独立な (u, v) が無限に存在する. □

定理 1-1 の n 次巡回拡大 L/k と (1) をみたす u, v に対して

$$\gamma(u, v) \;:=\; u^2 - \omega_n uv + v^2 \tag{3}$$

とおく. このとき容易に次の性質が示される:

補題 1-1 (i) $\alpha(\gamma(u, v)) = \gamma(u, v)$ よって $\gamma(u, v) \in k$.

(ii) 別の (u', v') を取るとき $\gamma(u', v')/\gamma(u, v) \in \mathrm{N}_{k(\zeta_n)/k}(k(\zeta_n)^\times)$.

以上の議論から, 定理 1-1 の n 次巡回拡大 L/k に対して一つの不変量 $\gamma(L/k) \in k^\times/\mathrm{N}_{k(\zeta_n)/k}(k(\zeta_n)^\times)$ を $\gamma(L/k) = \gamma(u, v) \bmod \mathrm{N}_{k(\zeta_n)/k}(k(\zeta_n)^\times)$ で定義することができる. $\gamma(L/k)$ は 相対判別式を精密化したものである.

他方, 行列 $T := \begin{pmatrix} 0 & 1 \\ -1 & \omega_n \end{pmatrix}$ で定まる分数一次変換 $x \mapsto T(x) := 1/(\omega_n - x)$ は, 有理関数体 $k(x)$ の自己同型を与え, その位数は n の偶奇に従ってそれぞ

れ $n/2$, n となる. 簡単のため, ここでは n は 奇数としよう. 不変体 $k(x)^{<T>}$ は Lüroth の定理よって再び有理関数体 $k(u)$ となる ($\exists u = u(x) \in k(x)$). こうして k 上正則な C_n 拡大 $k(x)/k(u)$ が得られる. これと定理 1-1 を比較してただちに次を得る:

定理 1-2 ([Mi]) k は定理 1-1 と同じ仮定をみたすものとする. このとき, n が奇数なら正則 C_n 拡大 $k(x)/k(u)$ は k 上生成的 (generic) である.

次の結果は §2 で $u = u(x)$ の具体形を求めた結果の副産物である.

定理 1-3 ([HM], [Ri]) 拡大 $k(x)/k(u)$ を分解体とする C_n-方程式が以下で与えられる:

$$L(X;u) := \frac{\zeta_n{}^{-1}(X-\zeta_n)^n - \zeta_n(X-\zeta_n{}^{-1})^n}{\zeta_n{}^{-1}-\zeta_n} - \frac{u\{(X-\zeta_n)^n-(X-\zeta_n{}^{-1})^n\}}{n(\zeta_n{}^{-1}-\zeta_n)}. \tag{4}$$

§2 A family of D_n-polynomials

以下では正整数 N に対して $G = D_N$ は N 次二面体群:

$$D_N := < \alpha, \beta | \alpha^N = \beta^2 = 1, \alpha\beta = \beta\alpha^{-1} >$$

とし基礎体 k は $\omega_N \in k$ を充たすとする. このとき, §1 と同様に $T, J \in \mathrm{GL}_2(k)$ を $T := \begin{pmatrix} 0 & 1 \\ -1 & \omega_N \end{pmatrix}$, $J := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ で定めると $T^N = J^2 = I_2$, $TJ = JT^{-1}$ から $< T, J > \cong D_N$ となる. また, $N = 2n$ が偶数のとき $T^n = -I_2$ となるから, $\mathrm{PGL}_2(k)$ に射影すると $< \overline{T}, \overline{J} > \cong D_n \subset \mathrm{PGL}_2(k)$ となる. そこで, $n := N$ (N: odd), $n := N/2$ (N: even), $\varepsilon := (-1)^N$ とおく. まず 有理関数体 $k(x)$ の自己同型群 $< \overline{T}, \overline{J} >$ による不変体を考察する.

$$u = u(x) := \sum_{j=0}^{n-1} T^j(x) = x + T(x) + \cdots + T^{n-1}(x). \tag{5}$$

とおくと, 明らかに $u \in k(x)^{<T>}$ であるが, 実は

命題 2-1

$$k(x)^{<T>} = k(u). \tag{6}$$

これは以下のように示される. 各 $j \in \mathbf{Z}$ に対して $\xi_j := \dfrac{\zeta_N^j - \zeta_N^{-j}}{\zeta_N - \zeta_N^{-1}}$ とおく

と $\xi_0=0, \xi_1=1, \xi_2=\omega_N, \xi_{j+n}=-\varepsilon\xi_j=\varepsilon\xi_{-j}$, かつ $j>0$ に対して

$$\xi_j=\omega_N^{(j-1)}+\omega_N^{(j-3)}+\ldots+\begin{cases}1 & \cdots \quad j=\text{odd}\\ 0 & \cdots \quad j=\text{even}\end{cases} \qquad (\omega_N^{(j)}=\zeta_N+\zeta_N^{-1}).$$

これより $\xi_j \in k$.

命題 2-2 任意の整数 $j \in \mathbf{Z}$ に対して

$$T^j = \begin{pmatrix} -\xi_{j-1} & \xi_j \\ -\xi_j & \xi_{j+1}\end{pmatrix}. \tag{7}$$

これより $T^j(x)$ 達の分母は互いに素であることがわかり, $u(x)=P(x)/Q(x)$,

$$Q(x) := \prod_{j=0}^{n-1}(-\xi_j x+\xi_{j+1}) = -\varepsilon x\prod_{j=1}^{n-2}(-\xi_j x+\xi_{j+1}), \tag{8}$$

$$P(x)=Q(x)u(x) = \sum_{j=0}^{n-1}(-\xi_{j-1}x+\xi_j)\prod_{k\neq j}(-\xi_k x+\xi_{k+1}). \tag{9}$$

と表され, $P(x)$ の主項 x^{n-1} の係数 a_0 は

$$a_0=\sum_{j=0}^{n-1}(-\xi_{j-1})\prod_{k\neq j}(-\xi_k) = (-1)^{n-1}\prod_{k=1}^{n-1}\xi_k \neq 0. \tag{10}$$

また

$$P(0)=\sum_{j=0}^{n-1}\xi_j\prod_{k\neq j}\xi_{k+1}=\xi_{n-1}\prod_{k\neq n-1}\xi_{k+1}=\varepsilon\prod_{k=1}^{n-1}\xi_k=(-1)^{n-1}\varepsilon a_0.$$

これより $\deg(Q)=n, \deg(P)=n-1$ がわかり 命題 2-1 が出る. 次に, $J(x)=1/x$ から $a'(x):=u(x)u(1/x)$ が $<T,J>$-不変であることがわかるが, 次数の比較から容易に $k(x)^{<T,J>}=k(a'(x))$ が示される. すなわち, $s'(x):=x+1/x$ とおくとき $[k(s'):k(a')]=n$. そこで, s' の $k(a')$ 上の既約方程式を求めれば, これが D_n をガロア群にもつ n 次方程式のパラメータ族を与える. 小さな n $(n=3,4,5)$ に対する実際の計算から, s', a' を

$$s=s(x):=x+\frac{1}{x}-\omega_N, \qquad a=a(x):=u(x)u(\frac{1}{x})-n^2 \tag{11}$$

で置き換えると, 以下に見る如く驚くほど簡明な方程式を得る.

命題 2-3 a を不定元とするとき, 以下の多項式 $F(X;a)\in k[a,X]$ は $k(a)$ 上

既約であり, $F(s(x);a(x))=0$. さらに, $F(X;a)$ の $k(a)$ 上のガロア群は D_n となる.

$$F(X;a) := {a_0}^2X^n+(-1)^{n-1}\varepsilon a\prod_{j=1}^{n-2}(\xi_j\xi_{j+1}X-1). \tag{12}$$

これを示すには, まず関係式

$$x^nQ(1/x)=-\varepsilon Q(x), \qquad x^nP(1/x)=-\varepsilon\{n\omega_NQ(x)-P(x)\} \tag{13}$$

に注意して $a(x)$ の分子を観察する:

$$a(x)=u(x)u(\frac{1}{x})-n^2 = \frac{P(x)\{n\omega_NQ(x)-P(x)\}-n^2Q(x)^2}{Q(x)^2},$$

$$\begin{aligned}&P(X)^2-n\omega_NP(X)Q(X)+n^2Q(X)^2\\ &= \{P(X)-\frac{1}{2}n\omega_NQ(X)\}^2-\frac{1}{4}n^2(\omega_N^2-4)Q(X)^2\\ &= \{P(X)-n\zeta_NQ(X)\}\{P(X)-n\zeta_N^{-1}Q(X)\}.\end{aligned}$$

ここで, 次の驚くべき (!?) 関係式が成立する:

$$\begin{aligned}P(X)-n\zeta_NQ(X) &= a_0(X-\zeta_N)^n,\\ P(X)-n\zeta_N^{-1}Q(X) &= a_0(X-\zeta_N^{-1})^n.\end{aligned} \tag{14}$$

実際, $0\le j\le n-1$ に対して

$$\tau^j(X)-\zeta_N=\zeta_N\cdot\left(\frac{(\zeta_N^{2j-1}-\zeta_N)X+(1-\zeta_N^{2j})}{(\zeta_N^{2j+1}-\zeta_N)X+(1-\zeta_N^{2j+2})}-1\right)=\frac{\zeta_N^{2j}(X-\zeta_N)}{1-\frac{\zeta_N(1-\zeta_N^{2j})}{1-\zeta_N^2}(X-\zeta_N)}.$$

この右辺をベキ級数に展開すると

$$\begin{aligned}u(X)-n\zeta_N &= \sum_{j=0}^{n-1}\{\tau^j(X)-\zeta_N\}\\ &= (X-\zeta_N)\sum_{j=0}^{n-1}\sum_{k=0}^{\infty}\zeta_N^{k+2j}\left(\frac{1-\zeta_N^{2j}}{1-\zeta_N^2}\right)^k(X-\zeta_N)^k\\ &= \sum_{k=0}^{\infty}\left(\frac{\zeta_N}{1-\zeta_N^2}\right)^k(X-\zeta_N)^{k+1}\sum_{j=0}^{n-1}\zeta_N^{2j}(1-\zeta_N^{2j})^k.\end{aligned}$$

ここで,

$$\sum_{j=0}^{n-1}\zeta_N^{2j}(1-\zeta_N^{2j})^k=\sum_{i=0}^{k}(-1)^i\begin{pmatrix}k\\ i\end{pmatrix}\sum_{j=0}^{n-1}\zeta_N^{2j(1+i)}=0\qquad(0\le k\le n-2).$$

に注意すると $u(X)-n\zeta_N$ が, $k(\zeta_N)[[X]]$ において, $(X-\zeta_N)^n$ で割り切れる. 従って $k(\zeta_N)[X]$ でも同様で, 次数の関係から, $P(X)-n\zeta_N Q(X)$ は $(X-\zeta_N)^n$ の定数倍でなければならない. □

$a(x)$ の定義式 (11) から

$$P(x)^2-n\omega_N P(x)Q(x)+n^2Q(x)^2+a(x)Q(x)^2=0,$$

$$a_0{}^2\{(x-\zeta_N)(x-\zeta_N^{-1})\}^n+a(x)Q(x)^2=0.$$

これを x^n で割って (13) を用いると

$$a_0{}^2(x+\frac{1}{x}-\omega_N)^n-\varepsilon a(x)Q(x)Q(\frac{1}{x})\ =\ 0. \tag{15}$$

一方, (8) と (11) から

$$\begin{aligned}Q(x)Q(\frac{1}{x})\ &=\ \prod_{j=1}^{n-2}(-\xi_j x+\xi_{j+1})(-\xi_j\frac{1}{x}+\xi_{j+1})\\ &=\ \prod_{j=1}^{n-2}\{(\xi_j{}^2+\xi_{j+1}{}^2)-\xi_j\xi_{j+1}(x+\frac{1}{x})\}\\ &=\ (-1)^{n-2}\prod_{j=1}^{n-2}\{\xi_j\xi_{j+1}(s+\omega_N)-(\xi_j{}^2+\xi_{j+1}{}^2)\}\\ &=\ (-1)^{n-2}\prod_{j=1}^{n-2}(\xi_j\xi_{j+1}s-1).\end{aligned}$$

これで命題 2-3 が示された. □

ここで, $c:=-\varepsilon a_0{}^2/a$ と置き, $X\to 1/X$ と変換すると次のような簡明な n 次多項式 $G_N(X;c)$ を得る:

$$G_N(X;c):=\prod_{j=0}^{n-1}(X-\xi_j\xi_{j+1})+\ c\ =\ X^2\prod_{j=1}^{n-2}(X-\xi_j\xi_{j+1})+\ c. \tag{16}$$

以上の結果をまとめると

定理 2-1 c を不定元とするとき, 多項式 $G_N(X;c)\in\mathbf{Q}(\omega_N)[c,X]$ は $k(c)$ 上既約でそのガロア群は D_n となる.

§3 主結果 (奇数次の場合: $N = n$)

定理 3-1 ([HM]) $N(=n)$ が奇数のとき $G_N(X;c)$ は $\mathbf{Q}(\omega_n)$ 上 generic な D_n-多項式である.

証明. §2 に於ける 関数体での議論, 特に $k(x)$ への $D_n =< \alpha, \beta >$ の作用と次の定理を比較することからただちに示される:

定理 3-2 K/k を 奇数 n 次の D_n 拡大とする. このとき n の各約数 m $(m < n)$ に対して $\mathrm{Gal}(K_m/k) \cong D_{n/m}$ かつ

$$\alpha(x_m) = T(x_m) := \frac{1}{-x_m + \omega_n}, \qquad \beta(x_m) = J(x_m) := \frac{1}{x_m}.$$

をみたす $x_m \in K$ が存在する.

奇数 $n > 1$ に対して D_n は $(n-1)/2$ 個の 2 次 (絶対) 既約表現をもつ. そのモデルとして 次の ρ_m $(1 \leq m \leq (n-1)/2)$ が取れる:

$$\rho_m(\alpha) = T_m = \begin{pmatrix} 0 & 1 \\ -1 & \omega_n^{(m)} \end{pmatrix}, \qquad \rho_m(\beta) = J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{17}$$

ここで k の仮定から $\mathrm{Tr}(\rho_m(\alpha^j\beta)) = 0, \mathrm{Tr}(\rho_m(\alpha^j)) = \omega_n^{(jm)} \in k, (0 \leq j < n)$. これから

$$k[D_n] \;\cong\; k \oplus k \oplus \mathrm{M}_2(k)^{\oplus(n-1)/2}. \tag{18}$$

この分解の 2 次行列環からなる単純因子に対応する中心巾等元は

$$\varepsilon_m \;=\; \frac{1}{n}\sum_{j=0}^{n-1} \omega_n^{(jm)}\, \alpha^j \qquad (1 \leq m \leq \frac{n-1}{2}) \tag{19}$$

で与えられ, ρ_m は projection

$$\psi_m :\; k[D_n] \to A_m := k[D_n]\varepsilon_m \cong \mathrm{M}_2(k), \qquad \alpha\varepsilon_m \mapsto T_m, \quad \beta\varepsilon_m \mapsto J. \tag{20}$$

を factors through する. このとき特に

$$\psi_m((\alpha+\beta)\varepsilon_m) = \begin{pmatrix} 0 & 2 \\ 0 & \omega_n^{(m)} \end{pmatrix}, \qquad \psi_m(\beta(\alpha+\beta)\varepsilon_m) = \begin{pmatrix} 0 & \omega_n^{(m)} \\ 0 & 2 \end{pmatrix}. \tag{21}$$

補題 3-1 各 m $(1 \leq m \leq (n-1)/2)$ に対して A_m の左 left ideal

$$\wp_m \;:=\; k[D_n](\alpha+\beta)\varepsilon_m + k[D_n]\beta(\alpha+\beta)\varepsilon_m \tag{22}$$

は ρ_m と同値な D_n の表現を定める.

以下 $m=1$ とし, 定理 3-2 の証明をする. K/k が D_n-拡大のとき, 正規底定理によって D_n-加群として $K \cong k[D_n]$ であるから, $K = k[G]\cdot z$ をみたす $z \in K$ が存在する. 上記の議論から

$$u_m := \beta(\alpha+\beta)\varepsilon_m \cdot z, \quad v_m := (\alpha+\beta)\varepsilon_m \cdot z$$

とおくと, $\alpha^2\varepsilon_m = (-1+\omega_n^{(m)}\alpha)\varepsilon_m, \quad \alpha^{-1}\varepsilon_m = (\omega_n^{(m)}-\alpha)\varepsilon_m.$

$$\begin{aligned} \alpha\cdot u_m &= v_m, \qquad \alpha\cdot v_m = -u_m + \omega_n^{(m)} v_m, \\ \beta\cdot u_m &= v_m, \qquad \beta\cdot v_m = u_m. \end{aligned} \tag{23}$$

(21) と同様に, $\mathrm{M}_2(k)$ の第 1 列からなるもう一つの左イデアル $\wp_m\beta$ が $(\alpha^{-1}+\beta)\varepsilon_m$ and $\beta(\alpha^{-1}+\beta)\varepsilon_m$ で生成される. そして

$$u_m' := (\alpha^{-1}+\beta)\varepsilon_m \cdot z, \quad v_m' := \beta(\alpha^{-1}+\beta)\varepsilon_m \cdot z$$

は, (23) と同じ関係式をみたす. よって $t \in k$ に対して

$$u_m(t) := u_m + tu_m', \quad v_m(t) := v_m + tv_m'.$$

も同様で, u_m, u_m', v_m, v_m' は k 上一次独立であるから (23) をみたす無限個の対 $u_m(t)$, $v_m(t)$ が得られる. そこで

$$x_m(t) := u_m(t)/v_m(t).$$

とおくと

$$\alpha(x_m(t)) = \frac{\alpha(u_m(t))}{\alpha(v_m(t))} = \frac{v_m(t)}{-u_m(t)+\omega_n^{(m)}v_m(t)} = \frac{1}{-x_m(t)+\omega_n^{(m)}} = T_m(x_m(t)),$$

$$\beta(x_m(t)) = \frac{\beta(u_m(t))}{\beta(v_m(t))} = \frac{1}{x_m}(t) = J(x_m(t)).$$

これらの $x_m(t)$ の族のうち, 有限個を除いてその D_n-orbit の位数は $2n/m$ となり, $k(x_m)/k$ が $D_{n/m}$-拡大であることがわかる. □

§4 主結果 (偶数次の場合: $N=2n$)

$N(=2n)$ が偶数のとき $D_N = <\tilde{\alpha}, \tilde{\beta}>$ の中心は $Z(D_N) = \{1, \tilde{\alpha}^n\} \cong C_2$ となり, $D_N \longrightarrow D_N/Z(D_N) \cong D_n$ は中心拡大である. L を k の D_N-拡大とするとき, $Z(D_N)$, $<\tilde{\alpha}>$ に対応する中間体を K, k_1 とする. L/k_1 は N 次巡回拡大であるから §1 と類似の不変量 $\gamma_*(L/k_1)$ が以下の (27) で定まる. §2,3 と同様に基礎体 k は $\mathrm{char}(k)=0$, $\omega_N \in k$ をみたすとする. また $\omega = \omega_n = \omega_N^2 - 2$

(n :奇数), $\omega=\omega_N$ (n :偶数) とする.

定理 4-1 $N=2n$ が偶数のとき $G_N^*(X;c):=G_N(\dfrac{X^2-1}{\omega+2};c)$ とおくと,

(i) $G_N^*(X;c)\in\mathbf{Q}(\omega_N)[c,X]$ は $k(c)$ 上既約でそのガロア群は D_N となる.

(ii) $\mathrm{Emb}(D_N/Z(D_N),K/k)\cap\{\gamma_*(L/k_1)=1\}\subseteq\{\mathrm{Spl}(G_N^*(X;c))|c\in k^\times\}$.

証明の概略. まず関数体モデルで埋蔵問題 $\mathrm{Emb}(D_N/<\tilde{\alpha}^n>,k(x)/k(c))$ を解く. $k(x)/k(c(x))$ は定理 2-1 における D_n-拡大. また計算の都合により $T:=-\begin{pmatrix}0&1\\-1&\omega\end{pmatrix}$, $J:=-\begin{pmatrix}0&1\\1&0\end{pmatrix}$ とおく. §2 と同様に $D_N\cong<T,J>\subset\mathrm{GL}_2(k)$ で $T^n=-I_2$ となるから, $\mathrm{PGL}_2(k)$ に射影すると $<\overline{T},\overline{J}>\cong D_n\subset\mathrm{PGL}_2(k)$ となる. $L\in\mathrm{Emb}(D_N/<\tilde{\alpha}^n>,k(x)/k(c))$, $\mathrm{Gal}(L/k(c))=<\tilde{\alpha},\tilde{\beta}>\cong D_N$ とすると L は有理関数体 $k(x)$ の 2 次拡大であるから有理関数体, (超) 楕円関数体のいずれかであるが, ここでは有理関数体 $L=k(y)$ の解を求めることを考察する. すなわち y を $s(x)$ の分数 1 次式の平方根の形と仮定して $k(x)$ の自己同型

$$\alpha:x\mapsto T(x)=\frac{1}{\omega-x},\quad \beta:x\mapsto J(x)=\frac{1}{x}$$

が $k(y)$ の自己同型に延長される条件を考察する.

定理 4-2

$$x=x(y)\ :=\ \frac{(y+1)((\omega+2)y+\omega-2)}{4y},\tag{24}$$

とおき, 関数体 $k(y)$ の自己同型 $\tilde{\alpha},\tilde{\beta}$ を

$$\tilde{\alpha}(y)=\frac{-(\omega-2)y+\omega-2}{(\omega+2)y+2-\omega},\qquad \tilde{\beta}(y):=\frac{-(\omega+2)y-\omega+2}{(\omega+2)y+2+\omega}\tag{25}$$

で定める. このとき

$$<\tilde{\alpha},\tilde{\beta}>\cong D_N\quad\text{かつ}\quad\tilde{\alpha}|_{k(x)}=\alpha,\tilde{\beta}|_{k(x)}=\beta.$$

ここで, $k(y)^{<\tilde{\beta}>}=k(\tilde{s})$, $\tilde{s}^2=s/(s+\omega+2)$ および, $k(y)=k(x,\tilde{s})$ に注意すると, $G_N^*(X;c):=G_N(\dfrac{X^2-1}{\omega+2};c)$ が $1/\tilde{s}$ と $c=-\varepsilon{a_0}^2/a$ の代数関係を与える式となる. これで 定理 4-1 の (i) が示された.

(ii) を示す. $\mathrm{Gal}(L/k)=<\tilde{\alpha},\tilde{\beta}>\cong D_N$ とすると §3 と同じ議論 (正規底定理) から k 上2 次元の D_N-部分加群 $W\subset L$ で $W=kU+kV$,

$$\tilde{\alpha}\cdot\begin{pmatrix}U\\V\end{pmatrix}=-\begin{pmatrix}0&1\\-1&\omega_n\end{pmatrix}\begin{pmatrix}U\\V\end{pmatrix},\quad \tilde{\beta}\cdot\begin{pmatrix}U\\V\end{pmatrix}=-\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}U\\V\end{pmatrix}\tag{26}$$

なるものが存在する. ここで $T^n = -I_2$ から U, V は 2 次拡大 L/K の pure elements で $U/V \in K = L^{<\tilde{\alpha}^n>}$ となる. そこで §1 と同様に不変量

$$\gamma_*(L/k_1) = \gamma_*(U,V) \ := \ U^2 - \omega UV + V^2 \quad \in k^\times/\mathrm{N}_{k(\zeta)/k}(k(\zeta)^\times) \quad (27)$$

が定まる.

詳細は略すが, 関数体の場合は $U = U(y)$, $V = V(y) \in L = k(y)$ で関係式 (26) をみたすものを求めれば:

命題 4-1 以下の $U(y), V(y) \in k(y)$ は (26) をみたす.

$$U(y) := \frac{(y+1)((\omega+2)y+\omega-2)}{(\omega+2)y^2+2-\omega}, \qquad V(y) := \frac{4y}{(\omega+2)y^2+2-\omega}. \quad (28)$$

命題 4-2 関数体 $k(y)$ において $U = U(y), V = V(y)$ から y を消去すると 次の関係式を得る:

$$\gamma_*(U,V) \ := \ U^2 + V^2 - \omega UV \ = \ 1. \quad (29)$$

また (29) の下で $U = U(y), V = V(y)$ から y が定まる:

$$y \ = \ \frac{(\omega-2)V}{2U-\omega V-2}. \quad (30)$$

注意 定理 3-2 の証明で見た如く, 対 (U,V) は L/k に対して一意的ではなく, 全体で k 上 2 次元のベクトル空間をなす. $\gamma_*(U,V)$ はその上の二次形式をなすが, その値の mod $\mathrm{N}_{k(\zeta)/k}(k(\zeta)^\times)$ での類は一定である. ただし, $\zeta = \zeta_n = \omega_N^2$ (n :奇数), $\zeta = \zeta_N$ (n :偶数) とする.

従って, D_N-拡大 L/k が 上記の関数体モデルの specialization によって得られるための条件は $\gamma_*(U,V) = 1 \in k^\times/\mathrm{N}_{k(\zeta)/k}(k(\zeta)^\times)$. これで 定理 4-1 の (ii) が示された.

References

[B] E.V.Black : Deformations of Dihedral 2-Group Extensions of Fields, Trans. Amer.Math.Soc. 1999.

[HM] K. Hashimoto, K. Miyake : Inverse Galois Problem for Dihedral Groups , Number Theory and its Applications, ed. by K. Gyory and S.Kanemitsu, Kluwer 1999, 165-181

[JY] C. Jensen, and N. Yui : Polynomials with D_p as Galois Group, J. of Number Theory 15 (1982), 347-375.

[Le] H.W. Lenstra : Rational functions invariant under a finite abelian group, Invent. Math. 25 (1974), 299-325.

[Ma] B.H. Matzat : Konstruktive Galoistheorie, Lect. Notes in Math. 1284, Springer-Verlag, 1986.

[Mi] K. Miyake : Linear Fractional Transformations and Cyclic Polynomials, Proceedings of Jangjun International Conference of Mathematical Sciences 1996, Research Notes in Number Theory, Saga Univ. Fac. Sci. Engrg., Vol. 10, pp.45-52, Saga, 1997.

[Ne] E. Noether : Gleihungen mit vorgeschriebener Gruppe, Math. Ann. 78 (1916), 221-229.

[Ri] Y. Rikuna : Constructive Inverse Galois Problem for Cyclic Groups over Rational Function Fields, preprint.

[RYZ] G. Roland, N. Yui, and D. Zagier : A parametric family of Quintic Polynomials with Galois Group D_5, J. of Number Theory 15 (1982), 137-142.

[Sa] D.J. Saltman : Generic Galois Extensions and Problems in Field Theory, Adv. in Math. 43 (1982), 250-283.

[Se1] J.-P. Serre, Linear Representations of Finite Groups, Graduate Texts in Math. 42, Springer-Verlag, 1993.

[Se2] J.-P. Serre, Topics in Galois Theory, Research Notes in Mathematics 1, Jones and Bartlett Publ. 1992.

[Sm] G.W. Smith : Generic Cyclic Polynomials of Odd Degree, Comm. in Algebra 19 (1991), 3367-3391.

[SM] L. Schneps and D. Martinais : Polynômes à groupe de Galois diédral, Sémin. Théor. Nombres Bordx. (2) 4 (1992), 141-153.

[Sw] R. Swan : Noether's Problem in Galois Theory, Emmy Noether in Bryn Mawr (J.D. Sally and B. Srinivasan edit.), 21-40, Springer-Verlag, 1983.