

# ガロア逆問題に於ける linear rigidity と その応用 (survey)

伊原 康隆 (京大・数理研)

最近 “linearly rigid tuples” の研究が進んで、応用として、有限体  $F_q$  上の reductive linear groups に関する有理数体  $\mathbb{Q}$  上の Galois の逆問題が色々解かれているので、その紹介を試みます。  $q$  が linear group の階数に比べて小さければ必ずしも素数でなくてもよい、というのが最近の主な進展で、その前段階の基礎を築いたのは J. G. Thompson、この方向を切開いたのが H. Völklein とその共著者 K. Strambach [V][SV] など、そして N. Katz の Rigid local systems の研究 [K] との関連に気づきそれを線型代数化した M. Dettweiler、S. Reiter による一般化 [DR] などが主なものですが、ここでは主に [DR] に従って話を進めます。

## 1 問題と背景

$F_r = \langle x_1, \dots, x_r \rangle$  を階数  $r \geq 2$  の自由群とし、等式  $x_r \cdots x_1 x_0 = 1$  によって  $x_0 \in F_r$  を定める。又  $GL_n(K)$  を体  $K$  上の  $n$  次一般線型群、

$$\varphi : F_r \rightarrow GL_n(K)$$

を群の準同型射とする。  $\varphi$  は  $x_i$  の像  $t_i$  ( $0 \leq i \leq r$ ) で一意的に定まる。

$$\begin{aligned} \varphi &\longleftrightarrow r\text{-tuples } t_r, \dots, t_1 \text{ in } GL_n(K) \\ &\longleftrightarrow (r+1)\text{-tuples } t_r, \dots, t_1, t_0 \text{ in } GL_n(K) \text{ s.t. } t_r \cdots t_1 t_0 = 1. \end{aligned}$$

$\varphi$  が既約 (絶対既約) とは、  $\varphi$  が  $F_r$  の表現として既約 (絶対既約) なることとする。

$\varphi$  が *linearly rigid* (resp. *absolutely linearly rigid*) とは、別に  $\varphi' \longleftrightarrow (t'_r, \dots, t'_1, t'_0)$  で各  $i$  ( $0 \leq i \leq r$ ) に対して  $t'_i$  が  $t_i$  と  $GL_n(K)$  (resp.  $GL_n(\bar{K})$ ) で共役なら、ある (一つの)  $g \in GL_n(K)$  (resp.  $GL_n(\bar{K})$ ) によって一斉に

$$t'_i = g^{-1} t_i g \quad (0 \leq i \leq r)$$

となること、と定義する。ただし  $\bar{K}$  は  $K$  の代数閉包。(共役の条件の中に  $i=0$  も含まれているからこそ意味がある、という事に注意)。Absolutely linearly rigid (略 *a.l.r.*) なら linearly rigid (略 *l.r.*) になる。

$n=1$  なら  $\varphi$  は常に絶対既約で *a.l.r.*

$n \geq 2$  のとき、 $r=2$  なら絶対既約な  $\varphi$  はすべて *a.l.r.* となる事が初等的計算で確かめられる (§2 命題 1 参照)。だが、 $r > 2$  だとそうとは限らない。以後  $\varphi$  が絶対既約の場合を主に考える。

《問題》  $\varphi$ : (絶対) 既約かつ (absolutely) linearly rigid なものを全部構成する方法はないか?

[K]、[DR] は、これにある意味での解答を与えている。

[問題の背景] (1)  $\mathbb{F}_q$  上の被約線型群  $GL_n(\mathbb{F}_q)$ ,  $Sp_{2n}(\mathbb{F}_q)$ , ... 等を Galois 群にもつ  $\mathbb{Q}$  上の Galois 拡大体の構成に役立つ。

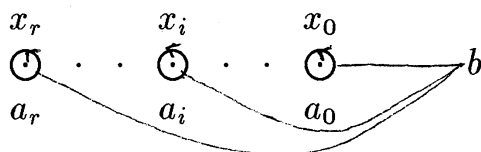
(2)  $K = \mathbb{C}$  のとき。 $r+1$  個の確定特異点を持ち、その外では非特異な  $\mathbb{P}^1_{\mathbb{C}}$  上の  $n$  階線型微分方程式であって、「local monodromy を保つ変形」を持たないもの (謂ゆる accessory parameter を持たない微分方程式) を求める問題そのものである。

B. Riemann 以来の問題である (2) の最近の発展が (1) に大きな影響を与えた [DR]。

[我々の問題と (1)(2) との関連]  $\mathbb{P}^1_{\mathbb{C}}$  上に  $r+1$  個の相異なる点  $a_0, \dots, a_r$  及び、それらと異なる基点  $b$  をとり、基本群

$$\pi_1 = \pi_1(\mathbb{P}^1_{\mathbb{C}} - \{a_0, \dots, a_r\}, b)$$

を考える。また下図の定める  $\pi_1$  の元を  $x_i$  ( $0 \leq i \leq r$ ) とすると、 $x_r \cdots x_1 x_0 = 1$  であり、 $\pi_1$  は自由群  $F_r = \langle x_1, \dots, x_r \rangle$  と同一視できる。



## [(1) との関連] 準同型射

$$\varphi: \pi_1 \rightarrow G \subseteq GL_n(\mathbb{F}_q) \quad t_i := \varphi(x_i) \quad (0 \leq i \leq r)$$

があると、この核と対応する  $\mathbb{P}_{\mathbb{C}}^1 - \{a_0, \dots, a_r\}$  の  $G$ -cover ( $G$  をガロア群とする有限正規連結被覆) がある。今  $a_0, \dots, a_r$  はすべて  $\mathbb{Q}$ -有理点とする。(もう少し弱く、それぞれは  $\mathbb{Q}$  上代数的でガロア置換によって全体として不変、でも可。) この  $G$ -cover は、代数曲線の代数的被覆とみるとき、 $\varphi$  に関する如何なる条件のもとで、 $\mathbb{Q}$  上定義されると云えるか? その為の十分条件の二つの主要な構成要素は実は:

(i)  $\varphi$ : 既約、かつ linearly rigid、

(ii)  $\{t_i\}_{i=0}^r$ : rational、即ち各  $tr(t_i)$  ( $0 \leq i \leq r$ ) は  $\mathbb{Q}$  上代数的で、ガロア置換によって集合  $\{tr(t_i)\}$  は保たれる、

である。これら二つが満たされても、まだ必ずしも十分とは云えないが、これらが最も基本的な条件なので、これらを満たすものを求め、それから更に残りの条件を確かめるという方法がとられている。上記  $G$ -cover が  $\mathbb{Q}$  上定義されれば、有理関数体  $\mathbb{Q}(t)$  上のガロア  $G$  拡大が出来るので、それを適当に特殊化して (Hilbert の既約性定理)  $\mathbb{Q}$  上の  $G$  拡大が作れるわけである。(i) を満たすものを見つけるのが一番困難、 $r$  が大きいものでないと (ii) が成立しにくいので、 $r$  が大きいものでしかも (i) を満たすものを作る必要がある。)

[(2) との関連]  $\mathbb{C}(t)$  係数の  $n$  階線型微分方程式  $S$  であって、 $a_r, \dots, a_0$  のみで確定特異点を持ちその外では非特異なものを考える。基点  $b$  での  $S$  の局所解の空間の底をとり、各  $\gamma \in \pi_1$  に沿ってそれらを解析接続する事によって  $\pi_1$  のモノドロミー表現

$$\varphi_S: \pi_1 \rightarrow GL_n(\mathbb{C})$$

が生じる。 $\varphi_S(x_i)$  ( $0 \leq i \leq r$ ) の Jordan 標準型を  $S$  の local data と考えると、

$$\varphi_S: \text{linearly rigid} \leftrightarrow \text{local data だけで } \varphi_S \text{ が } (GL_n(\mathbb{C}) \text{ 共役を除いて) 定まる。}$$

こういう  $S$  は今迄色々知られていて、その解は重要な特殊関数であった。

例えば、Riemann の  $P$  関数 ( $n = r = 2$ : この場合、前述のように、既約  $\rightarrow$  l.r.)。より一般の場合について、K. Okubo 氏等により日本でも盛んに研究されているようであるが、[DR] では高野一坂内 [TB] による Jordan-Pochhammer 方程式 ( $n = r$ ) の  $\varphi_S$  の具体的計算が大変有効に用いられている。

(1), (2) は謂わば  $\pi_1$  のそれぞれ Galois(etale)realization, de Rham realization の両側面なので、内的関連があったのは、むしろ当然だった、と云えよう。

## 2 Linearly rigid $(r+1)$ -tuples について

§1 のように

$$\begin{aligned}\varphi: F_r &\rightarrow GL_n(K), \\ \varphi &\leftrightarrow (t_r, \dots, t_1, t_0), \quad t_r, \dots, t_0 \in GL_n(K), t_r \cdots t_0 = 1\end{aligned}$$

とする。 $\varphi$  が絶対既約のとき、*a.l.r* である為の必要十分条件が簡単にわかる。ここで各  $i (0 \leq i \leq r)$  に対して、 $t_i$  の  $M_n(K)$  の中での centralizer ( $K$ -algebra) の  $M_n(K)$  内での余次元を  $\delta_i$  とおく。

**命題 1**  $\varphi$ : 絶対既約とすると常に  $2n^2 - \sum_{i=0}^r \delta_i \leq 2$  が成立ち、ここで等号が成立する事と  $\varphi$  が *a.l.r* である事が同値。

証明は直観的にもわかりやすく、容易。

この  $2n^2 - \sum_{i=0}^r \delta_i$  を  $\varphi$  の index of rigidity と呼ぶ。 $n = r = 2$  のときは、絶対既約性より  $\delta_0 = \delta_1 = \delta_2 = 2$  となり、この index=2、従って必ず *a.l.r* になる。

一般の  $(n, r)$  のとき、例えば (1つの)  $t_i$  の ( $n$ ヶの) 固有値がすべて相異なれば  $\delta_i = n^2 - n$  だが、一方、index=2 となるためには  $\delta_i (0 \leq i \leq r)$  の平均が  $\frac{2n^2}{r+1}$  位でないといけなないので、 $r$  が  $n$  に比べて大きいとき *a.l.r* になる為には、各  $\delta_i$  は十分小さく、従って各  $t_i$  の centralizer は十分大きく (即ち各  $t_i$  は " $n$  より低次元的" で) しかも全体としては絶対既約になっていないといけない。

Katz の原理 (一応 C 上): 与えられた  $(r, n)$  に対する既約で *l.r.* な  $\varphi_r$  は、同じ  $r$  で  $n = 1$  のものから、"middle convolution" と " $\Lambda$ -multiplication" の 2 つの操作を有限回くり返すことですべて得ることが出来る。

Dettweiler-Reiter: 一般の体  $K$  でこれを線型代数化した。

後者は、全く初等的である。以下これについて述べる。再び任意の

$$\begin{aligned}\varphi: F_r &\rightarrow GL_n(K), & t_i &= \varphi(x_i) \quad (0 \leq i \leq r) \\ & & t_r \cdots t_1 t_0 &= 1\end{aligned}$$

をとり、任意の  $\lambda \in K^\times$  と  $\varphi$  の組に対して “middle convolution”  $MC_\lambda(\varphi) : F_r \rightarrow GL_r(K)$  を次のように定義する。

まず  $\Phi' : F_r \rightarrow GL_{nr}(K) = GL_r(M_n(K))$  を

$$x_i \rightarrow \tilde{T}_i \quad (1 \leq i \leq r),$$

ただし、 $\tilde{T}_i$  は  $M_n(K)$  係数  $r$  次正方行列

$$\tilde{T}_i = \begin{pmatrix} I_n & & 0 & & \vdots & & \\ & \ddots & & & \vdots & & \\ & & \ddots & & \vdots & & 0 \\ & & & \ddots & \vdots & & \\ 0 & & I_n & & \vdots & & \\ t_1 - 1, \dots, t_{i-1} - 1, & \lambda t_i, & \lambda(t_{i+1} - 1), & \dots, & \lambda(t_r - 1) & & \\ & & \vdots & & I_n & & 0 \\ & & \vdots & & & \ddots & \\ & 0 & & & \vdots & & \\ & & \vdots & & \vdots & & \\ & & \vdots & & 0 & & I_n \end{pmatrix} \cdots i\text{行 (block row)}$$

で定める。(これは  $t_i$ : スカラーのときの高野—坂内行列 [TB] を元になっている。) 一方、 $K^{nr}$  (縦ベクトル) の中で

$$(Ker(t_1 - 1), \dots, Ker(t_r - 1))^{tr}$$

を  $\mathcal{K}$  とし、

$$\mathcal{L} = \bigcap_{1 \leq i \leq r} Ker(\tilde{T}_i - 1)$$

とおく。これらは  $\tilde{T}_i$ -stable である。各  $\tilde{T}_i$  が  $K^{nr}/(\mathcal{L} + \mathcal{K})$  に誘導する線型変換を  $T_i$  ( $1 \leq i \leq r$ ) とし、 $MC_\lambda(\varphi)$  を

$$MC_\lambda(\varphi) : F_r \rightarrow GL(K^{nr}/(\mathcal{L} + \mathcal{K}))$$

$$x_i \mapsto T_i \quad (1 \leq i \leq r)$$

によって定義する (表現の同値類は、一意的に定まる)。各  $\lambda \in K^\times$  に対する  $MC_\lambda$  は、 $K[F_r]$ -加群で  $K$  上有限次元なるもののなす圏からそれ自身への関手と見做せる。

定理 2 ([K][DR])  $\varphi$  は  $n > 1$  かつ絶対既約、又は  $n = 1$  で  $\#\{i; 0 \leq i \leq r, t_i \neq 1\} \geq 2$  とするとき、次の (i) ~ (v) が成立つ。

(i)  $MC_\lambda(\varphi)$  は絶対既約。

(ii)  $MC_1(\varphi) \simeq \varphi$ ,  $MC_\lambda(MC_{\lambda'}(\varphi)) \simeq MC_{\lambda\lambda'}(\varphi)$  ( $\lambda, \lambda' \in K^\times$ )。

(iii)  $\varphi$  と  $MC_\lambda(\varphi)$  は同じ index of rigidity を持つ。とくに

$$\varphi : a.l.r \leftrightarrow MC_\lambda(\varphi) : a.l.r.$$

(iv)  $MC_\lambda(\varphi)$  は  $\varphi$  への “braid action”, “dualization”, “inversion” と可換。

(v) すべての絶対既約で  $a.l.r$  な  $(r+1)$ -tuple  $\varphi$  は、 $n = 1$  の  $(r+1)$ -tuple から、 $MC_\lambda$  たちと  $\Lambda$ -乗法をほどこす操作を有限回くり返して得られる。ただし、 $K$  は  $t_i$  ( $0 \leq i \leq r$ ) のすべての固有値を含む (例えば  $K = \bar{K}$ ) とする。ここに、 $\Lambda$  乗法とは、

$(\lambda_r, \dots, \lambda_1) \in K^{\times r}$  に対して、 $\lambda_1 \cdots \lambda_r \lambda_0 = 1$  で  $\lambda_0 \in K^\times$  を定めたとき

$$(t_r, \dots, t_1, t_0) \rightarrow (\lambda_r t_r, \dots, \lambda_1 t_1, \lambda_0 t_0)$$

で得られる  $\varphi$  たち同志の間の変換。

このうち (v) の証明の要点を記す。

$\varphi \leftrightarrow (t_i)$ ,  $n > 1$ , 絶対既約かつ  $a.l.r.$  とするとき、

各  $i$  ( $0 \leq i \leq r$ ) に対して  $t_i$  の固有空間の余次元の最小値を  $n_i$ 、対応する固有値 (の一つ) を  $\lambda_i^{-1}$  とおくと、命題 1 と Scott のレンマにより、

$$\sum_{i=0}^r n_i < 2n, \quad \lambda = \lambda_r \cdots \lambda_0 \neq 1$$

を得る。このとき

$$MC_{\lambda^{-1}}(\lambda_r t_r, \dots, \lambda_1 t_1, \lambda^{-1} \lambda_0 t_0)$$

の次元  $< n$  となる。

特に、 $\varphi$  として  $\varphi = \varphi_{(a)} \leftrightarrow (t_r, \dots, t_0) = (a_r, \dots, a_0) \in K^{\times r}$

$$a_r \cdots a_0 = 1, \quad a_i \neq 1 \quad (\forall i)$$

をとり、 $\lambda \neq 1$ ,  $\lambda \neq a_0$  とするとき

$$MC_\lambda(\varphi_{(a)}) : F_r \rightarrow GL_r(K)$$

は絶対既約かつ *a.l.r.* これは

$K = \mathbb{C}$  のとき、Pochhammer differential equation と対応 (cf. [TB]).

$K = \mathbb{F}_q$  のとき、正規 Thompson  $(r+1)$ -tuple と対応

ここで Thompson  $(r+1)$ -tuple とは、

$$(t_r, \dots, t_0), \quad t_r \cdots t_0 = 1, \quad t_i \in GL_r(K) \quad (0 \leq i \leq r) \text{ で、}$$

既約かつ各  $t_i$  が余次元 1 の固有空間を有するもののこと。与えられた  $a_i, b_i \in K$  ( $0 \leq i \leq r$ ) に対して、 $t_i$  の固有多項式が  $(x-a_i)^{r-1}(x-b_i)$  なる Thompson  $(r+1)$ -tuple が存在する為の必要十分条件は

$$a_r \cdots a_0 \neq 1, \quad b_j \prod_{i \neq j} a_i \neq 1 \quad (0 \leq j \leq r), \quad \prod_i (a_i^{r-1} b_i) = 1$$

である。又これらが満たされるとき、そのような tuple は  $GL_r(K)$  共役を除いて一意的存在する (特に *l.r.*) ことが知られている。正規とは ( $\Lambda$ -乗法によって) 各  $a_i = 1$  ( $1 \leq i \leq r$ ) と仮定されたもののこと。

Völklein 等は、Thompson tuples とその  $\varphi(F_r)$  の分類を使って (以下の) 結果を出し、Dettweiler-Reiter は、 $n = 2$  の特定の “rational” (この為  $m > q$  が必要) *a.l.r.* な  $\varphi$  から  $M_{-1}(\varphi)$  等によって (以下の) 結果を出した。

(問)  $M_\lambda$  と  $\Lambda$ -multiplications の積の間に成立つすべての乗法的関係性を求めよ!

(筆者に興味あるが、現在答を知りません)。

### 3 主な応用上の結果

$\mathbb{Q}$  上の Galois 群として出てくることが *l.r.* tuples を用いて示せる有限体上の reductive linear groups の主な例は次のものである。

$$\begin{array}{ll} GL_m(q) & q : \text{odd}, < m \cdots m : \text{even} : \text{Völklein}, \\ PSO_{2m+1}(q) & q : \text{odd} < m, 7 < m \cdots \text{Dettweiler-Reiter}, \\ PSp_{2m}(q) & q : \text{odd} < m, 2 < m \cdots \text{Thompson, Völklein, Dettweiler-Reiter}. \end{array}$$

## References

- [DR] M. Dettweiler, S. Reiter, An algorithm of Katz and its application to the Inverse Galois problem. Preprint **99 – 47**, IWR, Heidelberg (1999).
- [K] N. Katz, Rigid local systems, Princeton Univ. Press.
- [SV] K. Strambach, H. Völklein, On linearly rigid triples, J. reine angew. math. **510** (1999), 57–62.
- [V] H. Völklein, Rigid generators of classical groups, Math. Ann. **311** (1998).
- [TB] K. Takano, E. Bannai, A global study of Jordan-Pochhammer differential equations, Funk. Ekvac. **19**.
- [S] J-P. Serre, Topics in Galois theory, Research Notes in Math.
- [MM] G. Malle, B.H. Matzat, Inverse Galois theory, Springer.
- [V] H. Völklein, Groups as Galois groups, An Introduction, Cambridge Studies in Adv. Math.
- その他,  
Aspects of Galois theory, London Math. Soc. LNS **256**, Cambridge Univ. Press.