

ガロアとキリングにおける群の構造

杉浦光夫

本稿では、ガロアとキリングにおける群の構造へのアプローチを比較する。両者の取組み方には大きな相違が見られる。

その原因の一部は、ガロアは可解群、キリングは単純群という、研究対象の違いに基づく。またガロアは、方程式論を作り出した人であるのに対し、キリングは群論が定着した後には、リーの仕事と土台にして研究を行ったという状況の相違がある。そのアプローチの相違にもかかわらず、この二人は極めて独創的なやり方で、新しい数学を生み出した。ここからは、その軌跡を辿ってみたい。

1 ガロア

代数方程式の理論において、ラグランジュ以降根の置換の考察が有効であることが次第に知られるようになっていった。

一方それと共に、既知量から有理演算によって得られる量と、高次方程式の根として得られ有理演算では得られない量の差異が明確になって行き、今日の体の概念の原型が形成されていった。

ガロアは、その有名な論文「方程式が累根で解けるための条件について」[7]の冒頭で有理量の定義をしている:

「方程式の係数および方程式に添加された量といくつかの任意に与えられた量との有理式として表わされるすべての量 (*toute quantité*) を有理量と呼ぶことにする。」

つまりこれらがその時点において既知と考えられる量である。ここで注意すべきことは、「有理式として表わされるすべての量」を考慮するという、外延的、集合的な考え方がなされている点である。ここでは、「四則演算が定義され、いくつかの演算規則をみる可集合」としての一般的、抽象的な体の定義はなかりが、「ある大きな体(例えば複素数の全体)の中で、いくつかの与えられた元から生成される部分体」と今日呼ぶものがはっきり把握されていることがわかる。

こうして出発点において既知とされる有理量の全体は、体を作り、それが今日基礎体と呼ばれようである。

ガロアは、 m 個の根を持つ代数方程式 $f(x) = 0$ に対し、それまで単に m 個の文字の置換(すなわち m 次対称群 S_m の元)と考えられていた根の置換を、上述の有理量の概念と結びつけてより精密にし、始めて方程式 $f(x) = 0$ のガロア群と今日呼ばれるものを、いわゆるガロア分解式を用いて定義した。このときガロア分解式のヒリ方を変えても、置換群としては同じ

ものが得られる。このガロア群の基本的な性質を、ガロアは第I節の定理で証明している。それは次のような内容である。

定理 n 個の根 $a, b, c, \dots$ をもつ方程式が与えらるゝとせよ。

このとき次の性質をみたす文字 $a, b, c, \dots$ の順列の群が常に存在する:

1° この群の置換によって不変である根の[有理式]は、すべて有理的に既知である。

2° 逆に、根の[有理式]で、有理的に決定し得るものは、すべてこれらの置換で不変である。

ここでガロアは、「有理式が不変である」というのは、根の間の置換によって式の形が変わらぬ」というだけでなく、その数値としての値が変わらぬことをいう」との註をつけている。

実際にこの定理の条件によって、 $f=0$ のガロア群は完全に定まるのである。

このことは論文に明記されてはいないけれども、ガロアは知っていたと思われる。

今日の言葉で言えば、与えられた方程式 $f(x)=0$ の根の全体を基礎体 K に添加した体を L とするとき、体 L の自己同型写像が K の各元を個別的に固定するものの全体が作る群が、ガロア拡大 L/K のガロア群 $G = G(L/K)$ である。 G の各元 σ は、 K の元を固定するから、 K 係数多項式 f は σ で不変であり、

従って σ は、方程式 $f=0$ の根の置換 σ を引き起す。この σ の作用群がガロアのいう置換群である。今日ガロアと σ とを同一視するのが普通である。

さてガロアは、方程式 $f=0$ が冪根のみを用いて解けるかどうかを定めよのに、 $f=0$ のガロア群 G を用いた。具体的には、補助方程式 $g=0$ の根を基礎体 K に添加した体を M とするとき、 M 上の $f=0$ のガロア群は、最初の $G=G(L/K)$ の部分群 $H=G(L/M)$ に縮小する。こうしてガロアは自然に部分群の概念に導かれたのである。特に $g=0$ の根全部に添加した場合として、ガロアは正規部分群の概念に出会ったのである。

オIII節の定理は、この言葉を用いるとき、次のように言い表わされる。

定理 補助方程式 $g=0$ の根全部を添加したとき、 $f=0$ のガロア群は、初めの群 G から、その正規部分群 H に縮小する。

次のオIV節には、この定理が述べられている (証明なし)。

定理 一つの方程式に、その根のある有理式の値を添加するとき、方程式の群はこの有理式の値を不変に留めた順列以外は含まないように小さくなる。

以上の準備の後、いよいよガロアは代数方程式 $f=0$ はどのような場合に冪根だけで解けるかという問題をオV節で

考える。

方程式 $f=0$ が冪根だけで解けるとは、 $f=0$ のすべての根が、基礎体 K に有限個の冪根を添加した体 L に含まれるということがある。すなわち K の拡大体の増加列

$$(1) \quad K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

があったとき、各 j に対し

$$(2) \quad K_j = K_{j-1}(\sqrt[m_j]{\alpha_j}), \quad \alpha_j \text{ は } K_{j-1} \text{ の元で } K_{j-1} \text{ の元を } m_j \text{ 乗ではるり、}$$

となるものが存在することを言う。

いま $a^{\frac{1}{mn}} = (a^{\frac{1}{n}})^{\frac{1}{m}}$ である。添加する冪根は素数乗根であるとしてよい。 $K(\sqrt[m]{a}, \sqrt[n]{b}) = K(\sqrt[m]{a})(\sqrt[n]{b}) = K(\sqrt[n]{b})(\sqrt[m]{a})$ であるから、上の(2)に現われる m_j 乗根は、 m_j の小さい方から順番に並べられるとしてよい。今 p を素数とし、 $K_j = K_{j-1}(\sqrt[p]{a})$ であると仮定

ガウスの円分方程式論 [8] の第 1 章) により、1 の原始 p 乗根 ζ のみをもつ円分方程式 $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$ は冪根のみで解ける $p-1$ 次方程式だから、それを解くのに必要な冪根は、 $q \leq p-1$ となる素数 q に対して q 乗根である。そこで上の(2)

における冪根の順序のとり方から、このような素根はすべて K_{j-1} に含まれており、従って a のすべての p 乗根は、一つの p 乗根 $\alpha = \sqrt[p]{a}$ と 1 の原始 p 乗根 ζ を用いて、

$$(3) \quad \alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^{p-1}\alpha$$

と表わされる。従って $K_j = K_{j-1}(\sqrt[p]{a})$ は、二項方程式 $x^p - a = 0$

のすべての根を含む。従ってⅢ節の定理により、 $G_j = G(L/K_j)$ は $G_{j-1} = G(L/K_{j-1})$ の正規部分群である。従って $2 \leq j$ とす

$$(4) \quad G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

という正規鎖が得られる。 $2 \leq j$ とす

$$(5) \quad [G_{j-1} : G_j] = p$$

であるから、剰余群 G_{j-1}/G_j は p 次巡回群という単群になる。

従って正規鎖 (4) は、今 G の 組成列 と呼ばれるものに外ならない。後にジョルダニは、このような剰余群が素数次巡回群となるような組成列を持つ有限群を 可解群 と名づけた。従

って累根のみで解ける代数方程式のガロア群は、可解群である

ことをガロアは証明したのである。逆にガロアは、 $f=0$

のガロア群 G が指数 p の正規部分群 H を持つときには、 p 乗根を添加することにより、ガロア群を G から H に縮小できる

ことを示した。従って $f=0$ のガロア群が可解群ならば、い

くつかの素数乗根を添加することと有理演算によって、 $f=0$

の根はすべて得られることになる、 $f=0$ は累根のみによって

解くことができる。そこで可解群という概念を用いると、ガ

ロアの結果は、次のように簡潔に述べることができる。

ガロアの定理 代数方程式 $f=0$ が、累根のみを用いて解く

ことができるための必要十分条件は、 $f=0$ のガロア群が可解

群となることである。

ガロアにとっては、群の構造はその直接の目標ではなく、
 彼が問題にしたのは、代数方程式の解の構造であった。しか
 しがロアは、解の構造をガロア群で統制するというアイディア
 を抱いた。このアイディアに基づいて、方程式を解くために補
 助方程式を解いて解を添加したときのカロア群の変化を記述
 することにより、ガロアは自然に、部分群、正規部分群、単
 純群、組成列などの概念に出会ったのであった。上述の素数
 巡回群だけでなく、ガロアは5次交代群が非可換単純群の
 最小次数のものであることを知っていた。このように多くの
 基本的な概念に出会うことができたのは、勿論ガロアの数学
 的センスがすぐれた居て本質的なものを見逃さなかったから
 であるが、一方では方程式論が群論と相性がよく、有限群論
 の種々の概念を實現する例を豊富に提供したという事情があ
 ったことを強調して置きたい。

ガロアが出会った上述の諸概念は、まづガロアの段階では
 名前もつけられていないが、後に群論の基礎概念として重要
 な役割を果たすことになる。しかしガロアには、それらが活躍
 する状況と見届けられる時間は残されていなかったのだった。

2. キリリング

キリリングが、有限次元連続変換群の構造について I-IV (1888-1890) [12] を書いたとき、既に組成列の概念はジョルダン [11] (1869) によつて導かれ、群が単純群による拡大を繰返しで得られることは認識されていた。一方リーは、有限次元連続変換群についての三つの基本定理によつて、そのような群 G とその引起す無限小変換達との関係を確立していった。 (リー [14]、ただしキリリングが [12] のオI部を書いてゐた時 [14] は未刊) が、その、エンゲル [6] を引用してゐる) リーのオニ、オ三基本定理の順定理は、今日の言葉で言へば、 G の無限小変換の一次結合の全体は、有限次元のリー環 (ワイル [20] の造語) を作るという内容を持つ。そしてその逆定理は、逆に有限次元リー環を作るように無限小変換達は、ある有限次元連続変換群から生ずることを述べてゐる。こうして有限次元連続変換群と、その無限小変換の作子 (R または C 上の) 有限次元リー環が一対一に対応するというのが、リーの理論の中心的内容である。

二つりことに注意しておく、オ一に連続変換群という名があふが、実はリーは群演算および空間への作用の双方に解析性を仮定してゐる (実は十分な回数を連続微分可能なら十分が

あることがわかった)。

もう一つはリーの理論は局所理論であり、リー群の群空間に作用する空間について、一つの座標近傍の中だけで考えていい。そのため今日の言葉で言えば、局所同型なリー群は同じものと考えるので、リー群とリー環の対応が成立つのである。

有限次元連続変換群 G の無限小変換 (基底) $X_1, \dots, X_r$ に対し、

リー基本定理により、括弧積について、

$$(1) \quad [X_i, X_j] = \sum_{k=1}^r c_{ij}^k X_k, \quad 1 \leq i, j \leq r$$

となる定数 c_{ij}^k が定まる。リーは定数 $(c_{ij}^k)_{1 \leq i, j, k \leq r}$ が、 G の局所的構造を定めることも見定めてくれた。しかしながら、この定数系 (c_{ij}^k) から、 G の構造についての具体的な情報を引き出す方法を、リーは持ち合わせていなかった。

一方キリングは、そのような方法を見出したのである。それは当時まだ新しい線型代数を用いるものであった。リーは、群 G の経数によって定まり、無限小変換の基底を固定して用いるが、キリングは基底の一次結合の全体を考え、それを線型空間として扱った。構造定数は基底を取換えると変わるのだが、キリングは都合により基底を選んで、無限小変換間の相互の関係が見易くできるようにすることを考えたのである。

もう少し詳しく言うと、キリングは複素リー環 $\mathfrak{g}$ の各元 X

に対し、 L 上の一次変換 $\text{ad} X: Y \mapsto [X, Y]$ を考え、一次変換の集合 $\text{ad} L$ のなすべく多くの元を同時に角化すること考えた。それが今言う所の、カルタン部分環によるルート空間分解を生み出したのであった。それを実行するためには、固有値、固有空間、一般固有空間等の概念が必要になって来る。

キリングは、行列式を主とする伝統的なやり方を用いているが、ここでは直接線型空間で考える。 $\text{ad} X$ の固有値 0 に対する一般固有空間 L_0 を

$$(2) \quad L_0 = \{Y \in L \mid (\exists n \in \mathbb{N}) (\text{ad} X)^n Y = 0\}$$

によって定義する。 $L_0 = L_0(X)$ の次元が最小となるような X を、

L の 正則元 とする。 X が正則元るとき、 $L_0 = L_0(X)$ は、 L の冪零部分環となる。そしてこのとき L は、 $\text{ad}_L L_0$ に属する同時一般固有空間の直和となる。しかしこのような一般論では、

一般固有空間の次元に大きな自由度があり、多くの場合が生ずる。そこでキリングは、考え得る最も簡明な場合に考察を集中するとし、[IV] の第 12 節の冒頭で、次の三つの仮定 (a), (b), (c) をみえる複素リー環 L の構造を決定すると宣言する。その三つの仮定は、現代的に言えば、次のようになる：

(a) カルタン部分環 $L_0 = L_0(X)$ は、極大可換部分環である。

(b) 0 以外の固有値に対する、 $\text{ad}_L L$ の同時固有空間の次元はすべて 1 である。

$$(c) \quad L = [L, L]$$

これは大胆な仮定であるが、キリリングは第I部6節で、 $PSL(l+1, \mathbb{C})$ のルート空間分解を求めて居り、これはリーが単純群であることを示している群があるから、これを一般の単純リー群のモデルにしたのでは有りかと思われろ。

この仮定の下で、 $\text{ad}_L L_0$ の同時固有値 $\alpha \neq 0$ を、 L_0 に関する L のルートという。これは勿論それが固有方程式 $\Phi(t) = \det(\text{ad}X - tI)$ の根となるからつづらぬ名前がある。

キリリングは、上の三つの仮定の下で L の構造を調べた。

このときルート α に対する $\text{ad} L_0$ の同時固有空間を L_α とすると、仮定1)により $L_\alpha = \mathbb{C}X_\alpha$ で、 α, β をルートとすると

$$(3) \quad \begin{cases} [H, X_\alpha] = \alpha(H)X_\alpha, & [X_\alpha, X_{-\alpha}] = H_\alpha \in L_0 - \{0\} \\ [X_\alpha, X_\beta] = \begin{cases} N_{\alpha, \beta} X_{\alpha+\beta}, & \mathbb{C} \ni N_{\alpha, \beta} \neq 0, \alpha+\beta \text{ がルートとなるとき} \\ 0 & \alpha+\beta \text{ がルートとならないとき} \end{cases} \end{cases}$$

となる。そこでルート α, β に対し $\alpha+\beta$ がルートとなるかどうか L の構造を規定する。さらに三重、四重、...の括弧積をとることを考えたと、自然に次の定義に行き着く。ルート α, β に対し、整数 $p \geq 0, q \geq 0$ が、次の(4)によって一意に定まる:

$$(4) \quad -q \leq m \leq p \text{ となるすべての整数 } m \text{ に対し } \beta + m\alpha \text{ はルートであるか } 0 \text{ に等しく, かつ } \beta - (q+1)\alpha, \beta + (p+1)\alpha \text{ はルートでない。}$$

このとき集合 $\{\beta + m\alpha \mid -\delta \leq m \leq \rho\}$ を、ルート β の α 列 といい、
 δ, ρ をその 左, 右の長さ とする。この名前がキリングがつけ
 られたのは 便宜上 用いることにする。キリングは

$$(5) \quad a_{\alpha\beta} = \rho - \delta$$

と決めた。

ワイル [19] 以後は、ルートはキリング形式 $B(X, Y) = \text{Tr}(\text{ad} X \text{ad} Y)$
 を用いて、内積の与えられ有限次元実ベクトル空間の $\mathfrak{g}$ のベ
 クトルと見る。この内積を用いるとき

$$(6) \quad a_{\alpha, \beta} = -2(\alpha, \beta) / (\alpha, \alpha)$$

となり、 α, β はそれぞれカルタニ整数に属するものが $a_{\alpha\beta}$
 である。この階数 $\dim L_0$ が k に等しうるとき、 k 個のルート $\omega_1,$
 $\dots, \omega_k$ が存在して、他のルートはこの ω_i 達の一次結合となる。

今簡単のため

$$(7) \quad a_{\omega_i \omega_j} = a_{ij}$$

と記すことにする。次の行列 (a_{ij}) は、今日カルタニ行列と
 呼ばれるもので属するものであるが、非常に特別な性
 質を持つ。それは

$$(A) \quad a_{ii} = -2$$

$$(B) \quad a_{ij} \text{ は非負整数 } (i \neq j)$$

$$(C) \quad a_{ij} = 0 \Rightarrow a_{ji} = 0$$

$$(D) \quad a_{ij} a_{ji} = 0, 1, 2, 3 \text{ のいずれか。}$$

などがある。 $l+1$ 次のカルタニ行列は、 l 次のカルタニ行列を含むから、 l の小さい方から、上の諸性質を用いてその形をきめて行くことが出来る。特に l が単純リー環のときは、そのカルタニ行列は、低次のカルタニ行列の直和となるもの。

このような既約なカルタニ行列の形を決定することにより、 l は成功した。それは彼が A, B, C, D と名づけた四つの無限系列と六個の例外的なものから成る。キリーニグは、これらのカルタニ行列に対応する単純リー環の存在することと主張したが、その証明は不完全であった。

しかしとにかく、(a)(b)(c) の三つの仮定をみたす複素単純リー環のタイプは、有限個しかないことがわかったのである。(この単純リー環のタイプとして知られる、 $SL(n+1, \mathbb{C})$ と $SL(n, \mathbb{C})$ のリー環は同型であるがパラメータ n の値を変えても、全く同様に扱うことが出来るので同じタイプであるとする。) これは以外な結果であった。

さらにキリーニグは、条件 (a)(b)(c) は、複素単純リー環に対しては常に成立つと考へ、その証明を [12] の IV 部で試みてゐる。

可換な 1 次元リー環を除けば、単純リー環は (c) をみたすことは明らかだから、(a) と (b) が問題になる。しかし彼の証明は不完全であるだけでなく、誤りを含むことが、エンゲルとウーラウフ [18] の研究で明らかになった (ホーキングス [9] 参照)。後に

任意)上の単純線型代数群は, ルート系が分類され, 複素単純リー群と同数なりあることを証明した。またシュヴァーレー [2] は, 任意の複素単純リー環 L と任意の体 K から, K 上の行列群として, いわゆるシュヴァーレー群を構成した。これは四つの例外を除き単純群であり, 特に K が有限体ならば有限群である。

このシュヴァーレー群が, 有限単純群の分類において重要な役割を果たす。

一方キリーニグの仕事は, カルタニを刺激して学位論文 [1] を書かせたが, [1] はカルタニ生涯のリー群研究の出発点として後の彼の研究に重要な影響を及ぼしたのである。特に有限次元既約表現の決定 (1913年), 実単純リー環の分類 (1914年) は, 直接 [1] の結果を用いて得られたものであり, 既約対称リーマン空間の分類 (1926・27年) は, 実単純リー環の分類とほぼ同値なのである。

リーによって始められたリー群論は, キリーニグによって, 構造論・表現論という二段階への扉が開かれたのである。

キリーニグは, 長らく Braunschweig という田舎町のギムナジウムの教師をしていたが, [12] は学会で認められ, 1900年に, カザンの数学・物理学会から, 第一回ロバチエフスキー賞を授与され, 1902年にモスクワ大学の正教授となった。

文 献

- [1] É. Cartan, Sur la structure des groupes de transformations finis et continus, Thèse, Paris, 1894, Oeuvres I-1, 137-287.
- [2] C. Chevalley, Sur certains groupes simples, Tôhoku Math. J. 7(1955), 14-66.
- [3] Sém. C. Chevalley, Classification des groupes de Lie algébriques, École Norm. Sup. Paris, 1958.
- [4] A. J. Coleman, The greatest mathematical paper of all time, Math. Intelligencer, 11-3(1989), 29-38.
- [5] H. M. Edwards, Galois Theory, Graduate Texts in Math. 101, Springer, 1984.
- [6] F. Engel, Ueber die Definitionsgleichungen der continuirlichen Transformationsgruppen, Math. Ann. 27(1886), 1-57.
- [7] É. Galois, Conditions de résolubilité des équations par radicaux, Oeuvres math. d'Évariste Galois, 33-50, Gauthier-Villars, Paris, 1897. 邦訳[16], 要訳[5].
- [8] C. F. Gauss, Disquisitiones arithmeticae, Leipzig, 1801. 高橋正巳訳「ガウス整数論」, 朝倉書店, 1995.
- [9] Th. Hawkins, Wilhelm Killing and the structure of Lie algebras, Archive for History of Exact Sciences 26(1982), 127-192.
- [10] S. Helgason, A centennial: Wilhelm Killing and the exceptional groups, Math. Intelligencer 12-3(1990), 54-57.
- [11] C. Jordan, Commentaires sur Galois, Math. Ann. 1(1869), 141-160.
- [12] W. Killing, Die Zusammensetzung der stetigen endlichen Transformationsgruppen I-IV, Math. Ann. 31(1888), 252-290, 33(1888), 1-48, 34(1889), 57-122, 36(1890), 161-189.
- [13] 梶田令二良, 「ガウスを語る」, 日本評論社, 1987.
- [14] S. Lie, Theorie der Transformationsgruppen, vol. 1, Teubner, Leipzig, 1888.
- [15] T. Molien, Ueber Systeme höherer complexer Zahlen, Math. Ann. 41(1893), 83-156.
- [16] 宇屋美賀雄, 「アーベル・ガウス群と代数方程式」, 共立出版, 1975.
- [17] 杉浦光夫, 「リーと Killing のカルタン構造概念」, 津田塾大学 数学・計算機科学研究部報 1 (1991), 76-103.
- [18] K. A. Umlauf, Ueber die Zusammensetzung der endlichen continuierlichen Transformationsgruppen, insbesondere der Gruppen vom Rang Null, Dissertation, Leipzig, 1891.

- [19] H.Weyl, Theorie der Darstellung kontinuierlicher halbeinfacher Gruppen durch lineare Transformationen I,II,III u. Nachtrag, Math. Zeits. 23(1925), 271-305, 24(1926), 328-376, 377-395, 789-791. Ges.Abh. II, 543-647.
- [20] H.Weyl, The classical groups, their invariants and representations, 1939, Princeton Univ. Press, Princeton.
- [21] 山下純一, カロアヘクイエ, 現代数学社, 京都, 1986.