数理解析研究所講究録
1130巻 2000年 157-173

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、リーの仕事を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かたで、新しい数学を生み出した。ここでは、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「方程式が冪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」を考えるという，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たす集合」としての一般的，抽象的な体の定義はないが，「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るものである。

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とり方を変えても，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　m個の根$a, b, c, \cdots$をもつ方程式が与えられたとせよ。このとき次の性質をみたす文字$a, b, c, \cdots$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らないというだけでなく，その数値としての値が変らないことをいう』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の自己同型写像で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 s を引起す。この s の作る群がガロアのいう置換群である。今日では σ と s 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るのに，$f=0$ 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 上での $f=0$ 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合ったのである。

第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。

次の第IV節には，次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する順列以外は含まないように小さくなる。

以上の準備の後に，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第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である。すなわち K の拡大体の増加列

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

であって，各 j に対し

(2) $$K_j=K_{j-1}(\sqrt[m_j]{\alpha_j}),\quad \alpha_j \text{ は } K_{j-1} \text{ の元で } K_{j-1} \text{ の元の } m_j \text{ 乗ではない},$$

となるものが存在することを言う。

いま $a^{\frac{1}{mn}}=(a^{\frac{1}{m}})^{\frac{1}{n}}$ だから，添加する冪根は素数乗根であるとしてよい。$K(\sqrt[m]{a},\sqrt[n]{b})=K(\sqrt[m]{a})(\sqrt[n]{b})=K(\sqrt[n]{b})(\sqrt[m]{a})$ だから，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んでいるとしてよい。今 p を素数とし，$K_j=K_{j-1}(\sqrt[p]{a})$ であるとする。

ガウスの円分方程式論（[8] 第7章）により，1 の原始 p 乗根 ζ のみたす円分方程式 $x^{p-1}+x^{p-2}+\cdots+x+1=0$ 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，$q\leqq p-1$ となる素数 q に対する 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 q 乗根はすべて K_{j-1} に含まれていることになる。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) $$\alpha,\ \zeta\alpha,\ \zeta^2\alpha,\ \ldots,\ \zeta^{p-1}\alpha$$

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。従ってこのとき

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

という正規鎖が得られる。このとき

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

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

従って正規鎖 (4) は，今日 G の組成列と呼ばれるものに外ならない。後にジョルダンは，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。従って冪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った。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り，$f = 0$ は冪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，冪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。しかしガロアは，解の構造をガロア群が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，方程式を解くための補助方程式を解いて解を添加したときのガ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合ったのであった。上述の素数次巡回群だけでなく，ガロアは5次交代群が非可換単純群で最小位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合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て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実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。

ガロアが出合った上述の諸概念は，まだ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すことになる。しかしガロアには，それらが活躍する状況を見届ける時間は残されていなかったのであった。

2. キリング

キリングが,「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) によって導入され, 群が単純群による拡大を繰返して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って, 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た。(リー[14]. ただしキリングが[12]の第I部を書いていた時[14]は未刊であったので, エンゲル[6]を引用している.) リーの第二, 第三基本定理の順定理は, 今日の言葉で言えば, 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いる。こうして有限次元連続変換群と, その無限小変換の作る(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な内容である。

二つのことを注意しておく. 第一に連続変換群というのであるが, 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いる(実は十分な回数だけ連続微分可能なら十分で

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，リー群の群空間についても作用する空間についても，一つの座標近傍の中ばかりで考えていた。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，リー群とリー環の一対一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 (の基底) $X_1, \cdots, X_r$ に対し，第二基本定理により，括弧積について，

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

となる定数 c_{ij}^{k} が定まる。リーは定数 $(c_{ij}^{k})_{1\leqq i,j,k\leqq r}$ が，G の局所的構造を定めることを見定めていた。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。それは当時まで新しかった線型代数を用いるものであった。リーは，群 G の径数によって定まる，無限小変換の基底を固定して用いたが，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るので，キリングは都合のよい基底を選んで，無限小変換達相互の関係が見易くな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 L の各元 X

に対し，L上の一次変換 $\mathrm{ad}\,X : Y \mapsto [X, Y]$ を考え，一次変換の集合 $\mathrm{ad}\,L$ のなるべく多くの元を同時対角化することを考えた。それが今日言う所の，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りているが，ここでは直接線型空間で考える。$\mathrm{ad}\,X$ の固有値 0 に対する一般固有空間L_0を

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

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<u>正則元</u>という。Xが正則元のとき，$L_0 = L_0(X)$は，Lの冪零部分環となる。そしてこのときLは，$\mathrm{ad}_L L_0$に関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ことにし，[12] 第II部 12節の冒頭で，次の三つの仮定(a), (b), (c) をみたす複素リー環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，$\mathrm{ad}_L L_0$ の同時固有空間の次元はすべて 1 である。

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

これは大胆な仮定であるが，キリングは第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た群であるから，これを一般の単純リー群のモデルにしたのではないかと思われる。

この仮定の下で，$ad_L L_0$の同時固有値$\alpha \neq 0$を，L_0に関するLの<u>ルート</u>という。これは勿論それが固有多項式$\Phi(t) = \det(adX - tI)$の根となるからつけられた名前である。

キリングは、上の三つの仮定の下でのLの構造を調べた。

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

(3) $$\begin{cases} [H, X_\alpha] = \alpha(H) X_\alpha, \quad [X_\alpha, X_{-\alpha}] = H_\alpha \in L_0 - \{0\} \\ [X_\alpha, X_\beta] = \begin{cases} N_{\alpha,\beta} X_{\alpha+\beta}, & \mathbb{C} \ni N_{\alpha,\beta} \neq 0, \ \alpha+\beta \text{がルートのとき} \\ 0, & \alpha+\beta \text{がルートでないとき.} \end{cases} \end{cases}$$

となる。そこでルートα, βに対して$\alpha+\beta$がルートとなるかどうかが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ると，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)によって一意的に定まる：

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

このとき集合 $\{\beta+m\alpha \mid -q \leq m \leq p\}$ を，ルート<u>βのα列</u>といい，q, p をその<u>左，右の長さ</u>という。この名前はキリングがつけたものではないが便宜上用いることにする。キリングは

(5) $$a_{\alpha\beta} = p - q$$

とおいた。

ワイル [19] 以後は，ルートはキリング形式 $B(X, Y) = Tr(adX\, adY)$ を用いて，内積の与えられた有限次元実ベクトル空間内のベクトルと見なされる。この内積を用いるとき

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

となり，α, β に対するカルタン整数に負号をつけたものが $a_{\alpha\beta}$ である。L の階数 $\dim L_0$ が k に等しいとき，k 個のルート $\omega_1, \cdots, \omega_k$ が存在して，他のルートはこの ω_i 達の一次結合となる。

今簡単のために

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

と記すことにする。k 次の行列 (a_{ij}) は，今日カルタン行列と呼ばれるものに負号をつけたものであるが，非常に特別な性質を持つ。それは

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

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

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

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

などである。$l+1$次のカルタン行列は，l次のカルタン行列を含むから，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できる。特にLが単純リー環のときは，そのカルタン行列は，低次のカルタン行列の直和とならない。このような既約なカルタン行列の形を決定することにキリングは成功した。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。キリングは，これらのカルタン行列に対応する単純リー環の存在することを主張したが，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。（ここでリー環のタイプというのは，$SL(n+1,\mathbb{C})$と$SL(n,\mathbb{C})$のリー環は同型ではないがパラメタnの値を変えるだけで，全く同様に扱うことができるので同じタイプであるという。）これは意外な結果であった。

さらにキリングは，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え，その証明を[12]第III部で試みている。

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，エンゲルとウムラウフ[18]の研究で明らかになった（ホーキンズ[9]参照）。後に

カルタン[1]は、任意の半単純リー環に対し(a)(b)(c)が成立つことを証明した。またカルタン[1]は、例外リー環の内階数4で次元52のものが二つあるとキリングが述べているのに対し、この二つのリー環は同型であり、例外リー環の個数は6個ではなく5個であることを示した。こうして複素単純リー環の分類は、キリング・カルタンの業績として数学史に残ることになった。勿論カルタン[1]の仕事は立派なもので、その価値は不滅であるが、キリングのイニシアティヴは忘れてはならない。

彼の仕事として特に重要なものとして次のものが挙げられる。

1° ルート空間分解という、新しい構造分析の手段の発見。
2° カルタン行列による複素単純リー環の分類法。
3° 複素単純リー環は、有限個のタイプに分類できることの発見。
4° 例外リー環という、未知の対象の可能性を指摘した。
5° 単純リー環と可換根基の半直線の構造を調べ、単純リー環の表現論への第一歩を踏み出した。

キリング・カルタンの複素単純リー環の分類は、複素単純リー群の分類のためになされたのであるが、その結果は極めて普遍的なものであることが、20世紀後半になって明らかとなった。すなわちシュヴァレー[3]は、任意の代数的閉体(標数は

任意)上の単純線型代数群は，ルート系で分類され，複素単純リー群と同数であることを証明した。またシュヴァレー[12]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。

このシュヴァレー群が，有限単純群の分類においても重要な役割を果す。

一方キリングの仕事は，カルタンを刺激して学位論文[1]を書かせたが，[1]はカルタン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った。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った。

リーによって始められたリー群論は，キリングによって，構造論・表現論という第二段階への扉が開かれたのであった。

キリングは，長らくBraunsbergという田舎町のギムナジウムの教師をしていたが，[12]は学会に認められ，1900年に，カザンの数学・物理学会から，第二回ロバチェフスキー賞を授与され，1902年にはミュンスター大学の正教授となった。

文　献

[1] É.Cartn, 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'Évarist Galois, 33-50, Gauthier—Villars, Paris, 1897. 邦訳[16], 英訳[5].

[8] C.F.Gauss, Disquisitiones arithmeticae, Leipzig, 1801. 高瀬正仁訳 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] 倉田令二朗, ガロアを読む, 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] 守屋美賀雄, アーベル・ガロア「群と代数方程式」, 共立出版, 1975.

[17] 杉浦光夫, リーとキリング・カルタンの構造概念, 津田塾大学 数学・計算機科学研究所報 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, ガロアへのレクイエム, 現代数学社, 京都, 1986.