ガロアの逆問題について

三宅　克哉（東京都立大学・理学研究科）

1．ガロアの逆問題の成立

例えば，有理数体に対して「絶対ガロア群は如何なる（有限）商群を持つか」という問題は現今でも代数的数論における最も重要な問題の一つである．ここで有理数体の絶対ガロア群とは有理数体の（複素数体における）代数的閉包の有理数体上のガロア群である．このように大きなガロア群を表に出した表現は，特に類体論のイデールによる表現が成功を納めて以来のことであろうか．類体論では，例えば，有限次代数的数体の最大アーベル拡大のガロア群が見事に記述できている．このガロア群は有限次代数的数体の絶対ガロア群の最大アーベル商群，すなわち，その閉交換子群による剰余群である．しかし当初はガロアの逆問題は素朴な形で提示されていた．すなわち，

ガロアの逆問題：与えられた有限群 G に対して，有理数体 $\mathbb{Q}$ 上のガロア拡大 $K/\mathbb{Q}$ であって，そのガロア群が G と同型なものが存在するか？

この問題の端緒は，1892 年のヒルベルトの既約性定理の論文 [Hi-1892] によって開かれた．ヒルベルトはこの定理の応用として，群 G が一般の対称群と交代群であるときは肯定的であることを示している．ところが，ことときは彼はまだ本格的には代数的数論には踏み込んでおらず，1894 年に初めて 3 本の代数的数論の論文を出版し，さらに 1896 年に，いわゆる「クロネッカー・ヴェーバーの定理：有理数体上のアーベル拡大は，円分体，すなわち，1 の冪乗根で与えられる」を証明した．次いで 1897 年にドイツ数学会から依頼された長大な「報文」が出版された．さらに 1898 年と 1899 年の 2 編の相対アーベル拡大についての論文によって彼の類体論の構想を提示し，さらに，大論文である相対 2 次拡大論を出版した．これによって一般の代数的数体において平方剰余の相互法則を示したのである．１９世紀冒頭からのガウスの問題提起に対するヒルベルトの答案であった．

ほぼ上記のような形でガロアの逆問題を正面切って論じたのは1918年のエミー・ネターの論文 [Noe-1918] であった（論文の最後に書き込まれた日付は1916年7月である）．ただし，1913年のノート [Noe-1913] ですでに，ネターの問題が肯定的であればヒルベルトの既約性定理を応用してガロアの逆問題の答えが得られることに言及している．

これらヒルベルト及びネターによる先駆的な仕事の後，多くの研究者の努力によって種々の有限群に対してこの問題が肯定的に解かれ，「有理数体の絶対ガロア群はすべての有限群を商群として持つ，すなわち，有限群はすべて有理数体上のガロア群になり得る」と予想されるに至った．このような個々の有限群に対するガロア拡大の存在性に関する研究がガロアの逆問題に対する研究の第一段階である．有限単純群の分類理論の完成に伴ってこの予想の正当性が確実視されている現在，ガロアの逆問題の第二の段階 ── 構成的研究 ── が注目されている．（例えば，イェンゼン，レデットと由井による [JLY-2002] を参照．）現在のガロアの逆問題に対する構成的研究は比較的小さな，あるいは構造が簡単な個々の有限群に対して上記の問題を考えるという形で行われており，最も構造が簡単な場合でも数論的に重要な応用を生み出している．現在までに，新しい巡回多項式族の発見，有限群の関数体への作用に関する種々のネター問題の解決，種々の有限群に対する生成的多項式の具体的構成，巡回拡大体のクンマー理論に対する基礎体の降下及び高次元化，等々の成果が得られている．この方面で先駆的な活動をした日本人として，例えば，増田勝彦，遠藤静男，宮田武彦などがあげられる．

2．ヒルベルトまでの４０年

ガロアの「全集」[Ga-1849] が1849年に出版され，特にドイツではクロネッカーやデデキンドがいち早くこれを吸収した．しかしガロアの逆問題が明確に意識されるまでには，まず，代数的数論が学問的な領域として確立されなければならなかった．

これに対してはガウスの「冪剰余の相互法則」という問題提起が大きい流れを示す．4次の場合の研究に不可欠なものとして，ガウスが彼の数体 $\mathbb{Q}[\sqrt{-1}]$ を，アイゼンシュタインが3次の場合に1の3乗根の体 $\mathbb{Q}[\sqrt{-3}]$ を導入し，クンマーが素数冪の円分体と，いわゆるクンマー拡大を導入し

た．特に，クンマーの「理想数論」は代数的数論の確立への流れを決定づけ，クロネッカーとデデキントがその任に着く．ここで強調されるべきことは，アーベルが残した幾つかのヒントと問題意識を的確に受け止めたクロネッカーの寄与である．特に楕円関数の虚数乗法をめぐる彼の数論的発見は代数的数論に大きな骨格を与えた．クンマーの「理想数論」の一般化（すなわち，イデアル論）と虚数乗法からもたらされる構造によって，ラグランジュやガウスの2元2次形式の類が虚2次体の数論の骨格に組み込まれた．

とはいえ，代数的数論が学問的な領域として確立されるのは1897年の彼の「報文」を俟つことになる．

もう一点は，「有限群」一般についての数学的な認知ということが問題である．

有限群の構造を意識して取り扱った最初の例は，フェルマによる彼の定理の「乗法的証明」であろうか．今風に述べれば，有限素体の0以外の元の乗法群において，各元の位数は群の位数を割りきる，というものである．彼は決して証明を明示していない．しかし，ほぼ一世紀後にオイラーが先ず加法的な証明を得，その後，乗法的証明を発見して，これを前者より上位に評価している．（有限環の可逆元の乗法群に対して拡張できることをその理由のひとつとした．）ヴェイユはフェルマも同様なステップを踏んだろうと，それなりの状況証拠をあげて推測している．因に，この証明法は，一つの元が生成する部分群によって群全体を剰余類に分けて個数を勘定するものである．また，ガウスは彼の『数論研究』（1801年）でオイラーの二種類の証明を与えて分析している．さらに2元2次形式の類が「形式の合成」によって可換群になることを指摘し，記号「＋」でその演算を表した．特に「アムビヒ類」の分析に際して，アーベル群の基本定理を示している．（位数は2の冪の場合ではあるが．）

群の概念に本質的な転機を与えたのは，方程式論において根の置換が取り上げられたことであろう．良く知られているように，「群」という語は，ガロアが彼の理論において，方程式に対応させた根の置換を一纏めにして（grouper），集めたものを普通名詞の「groupe」によって呼んだことによる．

近代的な方程式論はラグランジュの長大な論文 [La-1770, 71] に始まる．

彼は代数方程式の根のすべてを考え，それらの関数で，根の置換によって得られる関数の値の個数が小さくなるものを求めようとした．与えられた方程式の次数を n とすれば，n 個の根の置換全体は n 次対称群 $\mathfrak{S}_n$ を形作る．根の関数に対して，その値を変えないような置換の全体を H とし，その個数を h するとき，すべての置換によって得られる異なった関数値の個数が $n!/h$ $(= [\mathfrak{S}_n : H])$ であることを示している．しかも $n = 3, 4$ の場合にはこの値が n よりも小さく出来ることがそれらの根の公式の本質であるとみた．ところが $n = 5$ の場合には $n!/h = 2$ 以外にはこのような根の関数が見い出せず，結局根の公式は得られなかった．ルッフィーニは論文 [Ru-1799] によって $n = 5$ の場合に 5 次対称群 $\mathfrak{S}_5$ の「部分群」 H をすべて分類し，$5!/h$ が 2 以外はすべて 5 以上であることを見，さらに [Ru-1802] で 5 次以上の一般方程式の非可解性を検討した．

またコーシーも [Cau-1815] でラグランジュの問題を取り上げ，ラグランジュやルッフィーニの取り扱いを厳密に展開しようとした．これら先達の二名が単に permutation といっていたものを，permutation を順列とし，一つの順列からもう一つに写すことを置換 substitution と定義して「厳正化」を試みている．二つの順列を上下に二行に並べて表す現在も用いられている置換の表記法は彼に始まり，アーベル [Ab-1824], [Ab-1826] もコーシーに倣っている．

平野葉一は [Hira-2003] の第 10 章「代数方程式論から群論へ」で踏み込んだ興味深い考証を行っている．彼によるとこの 1815 年の段階ではコーシーは「置換群」の概念には至っていないと判断される．

以後の群論に関する際立った業績でに目に付くマテュー [Ma-1860, 61] やシロー [Sy-1872] も，それらを置換群として扱っている．またフランスでの最初のガロアの理論の解説であるジョルダンの [Jo-1870] も題名が示唆するように，あくまでも「根の置換」を一貫して扱っている．これに対してフロベニウスは 1887 年の論文 [Fr-1887] において，シローの定理を，現今の教科書にも見られるように，有限群の内部自己同型を用いて証明しており，置換群という視点から脱却しているといえるだろう．有限群論の最初の教科書は 1897 年に出版されたバーンサイドの [Bu-1897] の初版である．

3．エミー・ネター

エミー・ネター（1882-1935）は1907年にエルランゲン大学で学位を得た．「不変式論の王者」ゴルダンのもとで，3元4次形式についての長大な論文をまとめた．これの最後には330以上もの不変式の表が付いていた．一方不変式論のまったく新しい時代がヒルベルトによって展開されていた．彼は[Hi-1890]と[Hi-1893]によって，延々と記号が続く計算にはまったく拠らず，概念的，抽象的な方法による有限基底の存在証明を与えた．これらの論文には抽象的な体，環，加群についての基礎付けが含まれていた．

1910年にゴルダンが引退し，エルハルト・シュミットがエルランゲン大学に着任した．しかし翌1911年にはエルンスト・フィッシャーが彼に代わった．このフィッシャーこそがネターにヒルベルト的な方向への展開を促した人物である．1915年にはネターはゲッティンゲンに移る．（ディック[Di-1970]の邦訳書を参照した．）

ネターは1913年にフィッシャーとの交流から生まれたノート[Noe-1913]を表し，さらに[Noe-1915]としてまとまった論文を仕上げた．ここでは，多変数の有理関数体の部分体が有理関数体であるかどうか，すなわち，一変数の場合のリューロトの定理が多次元の場合にどうであるかを問題にしている．彼女は，リューロトやカステルヌオヴォ，エンリケス等の代数幾何学的なアプローチとは異なり，シュタイニツ[St-1910]（特に最後の第24節）に倣い，有理関数体の部分体に対する極小個数の生成元の存在性として問題を捉えた．特に[Noe-1913]において，次のネターの問題を提示している：

ネターの問題：数体を係数とするn次元の有理関数体に対し，与えられた有限群Gがn個変数の置換を通して体の自己同型写像として作用するとき，その固定体はまた有理関数体であるか？

そしてヒルベルトの既約性定理に触れ，この問題が肯定的であれば係数体の数体上で有限群Gに対するガロアの逆問題に肯定的な答えが得られることに言及している．

一方フィッシャーは1916年の論文[Fi-1916]で次の様な結果を得ている：有限アーベル群Aがn次元の線型変換群として表現されているとき，Aは，

n個の変数の線型変換によって定義されるn変数有理関数体の自己同型写像（クレモナ変換）としてクレモナ群に埋め込まれる．このようなAの二つの埋め込みに対して，それらの像は必ずクレモナ群の内部自己同型写像で移りあう．

フィッシャーはこの証明に当って，クレモナ群の内部自己同型写像を構成するために，有理整数環上の一般線型変換群のいわゆるモノミアル変換を通してのクレモナ群への埋め込みを利用している．

4．その後の歩みは．．．

- 1925年，Furtwänglerは$p = 3, 5, 7, 11$に対するp次対称群の推移的可解部分群について，それらがすべて有理数体上のガロア群として現れることを示した．（正則作用でのネター問題の肯定的解決による．）
- 1934年，Gröbnerは四元数群が有理数体上のガロア群として現れることを示した．（ネター問題の肯定的解決による．）
- 1937年，Scholz と Reichardtは奇素数pに対する有限p群はすべて有理数体上のガロア群として現れることを示した．
- 1954年，Shafarevichは，有限可解群はすべて有理数体上のガロア群として現れることを示した（ただし，1989年に証明が一部修正された）．

- 1969年と1970年にそれぞれSwan と Voskresenskiiは独立に，位数が47, 113, 223, 等の巡回群に対しては，有理数体上のネター問題は否定的であることを示した．
- 1974年，H. W. Lenstraは位数8の巡回群に対して有理数体上のネター問題は否定的であること，および，有限アーベル群に対して有理数体上のネター問題が肯定的に解けるための必要十分条件を示した．

- 1974年，Shihは2, 3または7のいずれかが平方剰余にならないような素数pに対して，PSL(2, p)は有理数体上のガロア群として現れることを示した．
- 1984年，Thompsonは「rigidity criterion」によってモンスター群が有理数体上のガロア群として現れることを示した．
- 以後，Matzatその他により，マテュー群M_{23}を除くすべての離散的

単純群が有理数体上のガロア群として現れることが示されている.

- 1982 年, Saltman は parametric polynomial, generic polunomial の概念を導入した（構成的に問題を展開）.
- 2002 年, Jensen, Ledet and Yui は構成的なアプローチにによるテキスト [JLY-2002] を出版した. 以上についての文献等の情報は, このテキストを参照されたい.

Reference

[Ab-1824] Abel, N.H.: Mémoire sur les équations algébriques, ou l'on démontre l'impossibilitéde la résolution de l'equation générale du cinquième degré, Œuvres d'Abel, t. I, pp.28--33.

[Ab-1826] Abel, N.H.: Deamonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré, Œuvres d'Abel, t. I, pp.66--87.

[Bu-1897] Burnside, W.: Theory of Groups of finite Order, Cambridge, Univ. Press, 1897; Second edit., 1911.

[Cau-1815] Cauchy, A.-L.: Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes manières possiblés les quantites qu'elle renferme, Œuvres de Cauchy, 2ème série, t. I, pp.64--90.

[Di-1970] Dick, A.: EMMY NOETHER, Birkhäuser Verl., 1970; ネーターの生涯, 静間良次監訳, 東京図書, １９７６.

[Fi-1916] Fischer, E.: Zur Theorie der Abelschen Gruppen, Math. Ann. 77 (1916), pp.81--88.

[Fr-1887] Frobenius, F.G. : Neuer Beweis des Sylowschen Satzes, Jour. r. angew. Math. 100 (1887), pp.179--181.

[Ga-1849] Galois, E.: Œuvres Mathématiques d'Evariste Galois, Liouville's Journal (1846).

[Hi-1890] Hilbert, D.: Über die Theorie der algebraischen Formen, Math. Ann. 36 (1890), 473--534; Gesam. Abhandl., Band II, pp.199--257.

[Hi-1892] Hilbert, D.: Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, Jour. reine angew. Math. 110 (1892), 104--129; Gesam. Abhandl., Band II, pp.264--286.

[Hi-1892] Hilbert, D.: Über die vollen Invariantensysteme, Math. Ann. 42 (1893), 313--373; Gesam. Abhandl., Band II, pp.287--344.

[Hira-2003] 平野洋一．西洋数学形成の諸断面，『数学の歴史』小川，平野共著，朝倉書店，２００３，第II部.

[JLY-2002] Jensen, Ch. U., Ledet, A. and Yui, N.: Generic Polynomials --- Constructive Aspects of the Inverse Galois Problem, Cambridge Univ. Press, Camebridge/New York/Melbourne/Madrid/Cape Town, 2002.

[Jo-1870] Jordan, C.: Traité des substitutions et des équations algébriques, Paris, 1870.

[La-1770, 71] Lagrange, J.-L.: Réflexions sur la résolution algébrique des équations, Œuvres de Lagrange, tom. III, pp.205--421.

[Ma-1860, 61] Mathieu, E.: Liouville's Journal 2èm Sér. t. V (1860), pp.9--42; ibid. t. VI (1861), pp.241--323.

[Noe-1913] Noether, E.: Rationale Funktionenkörper, Jahres Bericht 22 (1913), pp.316--319.

[Noe-1915] Noether, E.: Körper und Systeme rationaler Funktionen, Math. Ann. 76 (1915), pp.161--196.

[Noe-1918] Noether, E.: Gleichungen mit vorgeschriebener Gruppe, Math. Ann. 78, pp.221--229.

[Ru-1799] Ruffini, P.: Teoria Generale delle Equazioni, in cui si demonstrata impossibile la soluzione algebraica delle equazioni generali di grado superiore al quatro, Opere Matematiche di Ruffini, t. I, pp.1--324; *Appendice*: Rischiarimenti e risposte alle abbiezioni, *ibid.* pp.325--342.

[Ru-1802] Ruffini, P.: Della Insolubilita delle Equazioni algebraiche generali di Grado superiore al Quatro, Opere Matematiche di Ruffini, t. II, pp.1--50.

[St-1910] Steinitz, E.: Algebraische Theorie der Körper, Jour. reine angew. Math. 137 (1910), 167--309.

[Sy-1872] Sylow, L.: Théorèmes sur les groupes de substitutions, Math. Ann. 5 (1872), pp. 584--594.