６．可解群

これまでに述べたことによってついにガロア理論の一つの峰を極めることになった．

この章では，新たな群についての用語として**可解群**を導入し，いよいよガロア理論の最初の精華である「５次以上の代数方程式の不可解性」（**アーベル・ルフィニの定理**）を説明しよう．この峰からの眺望としてこれ以上のものはないであろう．ここでの主役はまたしても正規部分群である．

まずは，可解群の例をあげる．

３次対称群 G_3={１，(12)，(13)，(23)，(123)，(132)}において，この群は正規部分群 A_3={１，(123)，(132)}を含んでおり，A_3はもちろん部分群として単位群 E={１}を含んでいる．これらの集合としての包含関係は，

$$G_3 \supset A_3 \supset E \qquad [23]$$

となっている．この包含関係ではすべて右の部分群は左の（部分）群の正規部分群である．一番右には単位群が来る．このような包含関係を示す列を群の**正規列**という．そしてさらに**おのおの隣同士の正規部分群から作られる剰余群（上の例では G_3/A_3 および A_3/E ）がすべて巡回群になるとき，この群を可解群というのである**．

G_3の正規列における剰余群では，まず G_3/A_3 が　巡回群であることは前章で述べたように G_2と同じものであることから一目瞭然である．また A_3 / Ｅは群表を作るまでもなく明らかに A_3自身とおなじものであり，A_3は明らかに巡回群である．ゆえに G_3は可解群である．

可解群という名称は，**方程式が代数的に解かれるならば，そのガロア群は可解群であるという**事実からきている．その対偶を取ると，「方程式のガロア群が可解群でないならば，その方程式は代数的には解けない」ということも示され，ここから五次以上の方程式の非可解性が構造的に明らかにされるのである．

方程式を（代数的に）解くということは，基礎体の元による四則を行ない，必要とあればその中のある数の累乗根を用いて体を拡大し，その拡大体の中に解がなければさらに累乗根を追加するという手順を有限回行なってついに方程式のすべての解に至るということを意味する．

四則を行なう対象はいうまでもなく体であり，以前に掲げた約束によれば基礎体の拡大時には１の虚数累乗根も含むことになっていたので，累乗根による体の拡大は，すべて正則である．群では，正則拡大体は正規部分群として表現されるから，この順次行なわれる拡大は，群としては正規部分群の列となって表現される．これが正規列である．剰余群とは，累乗根とそれを追加する体との関係をガロア群によって表現したもので，それが巡回群になるのは（１の虚数累乗根を含んだ）累乗根であることから当然である．

こうして代数的に解かれた方程式のガロア群は可解群でなければならないのである．

ガロアはすでに十代のときにこのことを発見し，その重大性を持って当時の学会に働きかけたのであるが，彼の論文を受け取った大学当局の怠慢と無理解とによって完全に無視された．当時の一流の数学者たちにとってガロアの発見があまりに超越していて理解できなかったとは思えないが，とにかく論文をまともに読むことさえ行なわれなかったようである．

ガロア自身は，おそらくこの理不尽な無理解が動機と思われるが，まもなく急進的な共和主義者として革命運動に参加するようになり，やがて仕組まれた決闘事件によって短い命を終えることとなった．彼の理論はその後の数学界に革命を呼び起こすことになり，代数学は，それまでの中心議題であった方程式の解法を離れ，群および体を初めとする代数系を研究対象とする数学へと発展していったのである．彼自身の理論が引き起こした数学界の革命について，ガロアは知る由もない．しかし，決闘前夜に書かれた遺書には，自分の理論の重要性を確信し，さらなる広大な領域への応用を願いながら時間のないことへの焦燥にあふれている．（矢ケ部巌著「数III方式ガロアの理論」（現代数学社）参考 1978 年）

さて，ではなぜ方程式が代数的に解けないということが起きるのであろうか．ガロア群が可解群であるとかないとかとは，そもそもいったい何を表現しているのであろうか?

方程式の係数に四則を行なうことは一つの体を確立することである．これが基礎体となる．一次方程式がこの中で解かれることは明白である．一次方程式にはガロア群などは必要ないが，あえてガロア群を考えるならばそれは一次対称群とでもよぶべき E=｛1｝(単位群）であろう．

二次方程式になると，四則とは異なる開平という計算方法が必要となるが，これが累乗根の最初である．基礎体のある数が開平されることで基礎体の中にはない数が現れてくる．これが超数である．基礎体と超数とによって新たな体（拡大体）が形成され，その中に解が含まれることが保証されれば二次方程式も可解となる．このとき，その方程式のガロア群にはどんなことが起きているか．超数によって拡大された体を基礎体と考えるなら一次方程式と同じ（可約になる）だが，もとの基礎体から考えるときには，その基礎体の数の中での超数のふるまいが重要になってくる．なぜなら累乗根はその深さによってより複雑になるからである．この複雑さを表現する手段がガロア群である．

ある数に四則を行ない，また累乗を行なってある値を得ることは，いわば一本の道を辿るだけであるが，方程式を解くことは，その逆に最後の値から遡ってもとの数に立ち返ることであり，そのための道は一本道ではない．それは複素数の世界における累乗根の多価性のためである．ある数の累乗根はその深さ（何乗根であるか）によって多くの値を持つことになる．例えば立方根には３つの値があり，n 乗根には n 個の値がある．これらの値は互いにまったく対等であり，お互いを区別するものは何もない．これを累乗根の対称性と呼ぼう．累乗根は互いに移り合う（映り合う）のだ．この累乗根の対称性はそれが追加された拡大体全体に及び，拡大体自身の対称性に発展する．

例えば基礎体Ｑ（有理数体）に超数 $\sqrt{2}$ を追加したとき， $\sqrt{2}$ にはそれとまったく同等な $-\sqrt{2}$ という共役数が存在し， $Q(\sqrt{2})$ という拡大体を構成したと同時に $Q(-\sqrt{2})$ という拡大体も構成される．その二つの拡大体を統一的に捉えることが正則ということであり，正則拡大体を統一的に把握，統御しようというのがガロア群なのである．ガロアの天才はここに集中される．ガロアは累乗根の対称性を拡大体の正則性によって捉え，それを群の正規部分群に反映させることで問題の核心をつかんだのである．

累乗根の対称性のもっとも鮮やかな表現は，１の n 乗根の幾何学的表現であろう．いわゆる複素数平面（複素数全体を xy 座標平面で表わしたもの）上では１の n 乗根は原点を中心とする半径１の正多角形の頂点を示す．この１が a になるとその半径は $|a|$ に拡大される．a の n 乗根を方程式で表わすと n 次の２項方程式になるが，これをさらに複雑な方程式にしていくと，この正多角形上の頂点はやがてガウス平面上を四方に散らばっていく．この散らばり方をとらえるのもまたガロア群である．

この累乗根の対称性は，あるところまで発展すると維持されなくなる．いわば対称性が破られるのである．それが一般の五次方程式の性質に反映されることで，神秘的な現象として人々の目に映る．４次までは解けてなぜ５次は解けないのか．５というわずかな次数においてその代数的可解性が保証されなくなることは，理論的にも歴史的にも多くの数学者の歓心を買い，それが数学の発展の原動力にもなった．その不思議さを解明したのがガロアであり，彼の創成したガロア理論であった．

では，なぜガロアは累乗根の対称性を解明できたのか．それは置換群の研究によるのである．置換とはものの置き換えという，まことに原始的な作用であるが，原始的であるからこそ対称性を表現するのにはうってつけだったのである．置き換えとは「すでに決められてある場所を取り替えること」であるから，ひとつの枠あるいは範囲を出ないので，もともと対称的であるといえる．例えば 12345 という順列はなんとなく「対称的」である．何となくというのは直感的な言い方ではあるが，あえて言葉でいえば「両端のから始めて中心に向かって順に足していくと同じ６になる」，しかし真ん中は３ではないかといわれるが真ん中は特別だと考えればよい．では 42153 はどうか．これも両端から足していくと７になり，真ん中の１は特別とすれば対称

的であるかもしれない．このとき初めの12345から42153への置換を考え，これを循環置換として(1453)と表現するとこの置換はある対称性を維持しているといえないだろうか．つまり12345から42153へ置き換えてもある対称性が維持されていると考えるのである．

こうした考え方によっていわゆるn次対称群が考え出されたとすれば，このn次対称群の研究によって5次方程式の非可解性も解明され，ひいては「5」という数の神秘性も明らかになるであろうことを，ガロアは見抜いたに違いない．

現代的なガロア理論の立場からこのことを証明すると次のようになる．

まず，一般の5次方程式はそのガロア群が5次対称群になることを前提とする．そして**2次以上のn次対称群G_nにはn次交代群A_nが正規部分群として存在すること**を前提とする．

このA_nについてそれが可解群であると仮定すると，A_nの正規列，

$$A_n \supset B \supset \ \ldots \ \supset E$$

が存在する．BはA_nの正規部分群で．しかも当然 $A_n \neq B$ でなければならないが，これが $n \geq 5$ のときには $A_n = B$ となってしまうことを示そう．つまりA_nには単位群以外の正規部分群がないのである．

A_nは交代群だからG_nの置換のうちの偶置換の全体から成る群である．よってその元は，1,2,3,4,5,…等の置換のうちの偶置換，例えば (12)(34) のように「2つの互換の積」をひとつのまとまりとしてそれが集まって成り立っている．

BはA_nの正規部分群であるから任意の置換 σ について $\sigma B \sigma^{-1} = B$ が成り立つ．そこでBには恒等置換以外の置換があるはずだから，それを例えば $(ab)(cd)$ とする．これに対して，A_nの任意の互換の積 $(xy)(zw)$ を考え，それを用いて次のような置換を作る．

$$\sigma = \begin{pmatrix} x\,y\,z\,w\,\ldots \\ a\,b\,c\,d\,\ldots \end{pmatrix}$$

この $x, y, z, w, \ldots$ とはもちろん1,2,3,4,…のうちのいずれかである．下の行の $abcd$ の並びは $(ab)(cd)$ のならびに依っている．この σ を用いて $\sigma(ab)(cd)\sigma^{-1}$ という計算をすると，

$$\sigma(ab)(cd)\sigma^{-1} = \begin{pmatrix} x\,y\,z\,w\,\ldots \\ a\,b\,c\,d\,\ldots \end{pmatrix}\begin{pmatrix} a\,b\,c\,d\,\ldots \\ b\,a\,d\,c\,\ldots \end{pmatrix}\begin{pmatrix} a\,b\,c\,d\,\ldots \\ x\,y\,z\,w\ldots \end{pmatrix}^{-1} = \begin{pmatrix} x\,y\,z\,w\,\ldots \\ y\,x\,w\,z\,\ldots \end{pmatrix} = (xy)(zw)$$

となる．これは $(xy)(zw)$ がBの元であることを示す． $(xy)(zw)$ はA_nの任意の元であるのに，それがBに属することになるから， $A_n \subset B$ となる．一方， $A_n \supset B$ であるから結局， $A_n = B$ という矛盾が起こるのである．すなわち，交代群A_nは可解群ではない．5次以上の対称群を可解群と仮定したから矛盾が起きたのだから，5次以上の対称群は可解群ではあり得ない．（「対称群が可解群ならば，交代群も可解群である」の対偶は「交代群が可解群でないならば，対称群も可解群でない」である．）よって5次以上の一般n次方程式は代数的に解くことはできないのである!

7．アーベル・ルフィニの定理

このように，ガロア理論に依ることで，かなり簡潔な議論によって５次以上の方程式の代数的非可解性を証明することができる．

同じ問題を，ガロアに先行して解いたアーベルによる証明方法で考えてみよう．ただ，これはアーベルの証明のガロア理論による翻案ということになるのかもしれない．．

与えられた方程式を，基礎体 Q 上既約な n 次方程式とする（ $n\geq 2$ ）．その解を $x_1, x_2, x_3, \ldots$ とすると，Q 上既約なので $x_1, x_2, x_3, \ldots$ は有理数ではない．そこで Q の中のある数 r を用いてその p 乗根（p は素数とする）によって拡大される．これが Q の超数 $\sqrt[p]{r}$ である．この超数 $\sqrt[p]{r}$ と Q の数には，解 $x_1, x_2, x_3, \ldots$ との関係においてある重要な違いがある．

方程式の解と係数の関係から，方程式の係数は解を用いた対称式で表わされる．対称式とは，式を構成する文字をどのように置換しても式の値を変えない式のことである．２次方程式 $x^2+ax+b=0$ の場合には解と係数の関係は $x_1+x_2=-a$，$x_1x_2=b$ と表わされる． x_1+x_2 や x_1x_2 が対称式である．そして基礎体のすべての数はこの $-a, b$ を用いて表わせるから（ $1=a/a, 2=(a+a)/a$ ...等々），基礎体のすべての数は解の対称式で表わされる[14]．従って基礎体 Q の数は（それを解の対称式から成っている数としてみるならば）解のどのような置換に対してもその値を変えないことになる．しかし，超数 $\sqrt[p]{r}$ は基礎体の数ではない．ここで超数について次の重要な定理を導入する．

【定理３】可解である方程式の解法に用いられる累乗根（超数）は，解の有理式で表わされる．

有理式とは整式による分数式のことで，解の有理式とは， $x_1, x_2, x_3, \ldots$ に付いての四則計算（根号を含まない）によって得られる式のことである．

この定理こそ，アーベルの慧眼によって得られた方程式の不可解性証明のための核心であった．その簡単な証明を【付録３】に載せたが，ここでそれを証明されたものとして用いるならば，あとは比較的容易に目的を達することができるのである．

【定理３】により $\sqrt[p]{r}$ は解のある有理式で表わされるから，それを $\sqrt[p]{r}=f(x_1, x_2, x_3, \ldots)$ と表わそう．この式に解の互換 (12) を行なえば $f(x_2, x_1, \ldots)$ に変わる．すると $f(x_1, x_2, \ldots)$ は対称式ではないので $f(x_1, x_2)\neq f(x_2, x_1)$ である．

以下では式の見やすさのために， $f(x_1, x_2, \ldots)$ を f ， $f(x_2, x_1, \ldots)$ を f' とする．

ところで $\sqrt[p]{r}$ (= f)は $x_1, x_2, x_3, \ldots$ の対称式ではなくても有理式だから，p 乗すれば r にもどり，従って f^p は $x_1, x_2, x_3, \ldots$ の対称式になる．一方の f' は p 乗するとどうなるか． $(f')^p$ というのは， f の x_1, x_2 を置換してから p 乗するという意味だが，それは f を p 乗してから置換しても同じことである[15]．そして f を p 乗すれば対称式に戻るから置換しても変わらない．ゆえに $(f')^p=f^p$ ，従って１の p 乗根を ε とすれば $f'=\epsilon f$ $(\epsilon\neq 1)$ となるが，この式に対してもう一度解の互換 (12) を行なうと， f' は元に戻るから $f=\epsilon f'$ となる．これを $f'=\epsilon f$ に代入すると $f'=\epsilon\cdot\epsilon f'=\epsilon^2 f'$ となるので $\epsilon^2=1$ でなければならない．すなわち p は２である．よって $\sqrt[p]{r}=\sqrt{r}$ ．さらに $\epsilon\neq 1$ より $\epsilon=-1$ ．よって，

$$f'=-f$$

となる．これは何を意味するか． f の x_1, x_2 だけを入れ替えた式は f の符号を替えただけの式に等しいという意味である．このように互換によって符号だけが変わる式を交代式という． $\sqrt{r}$ = $f(x_1, x_2, \ldots)$ は対称式ではないが，交代式なのである．

---

[14] これはどんな高次の方程式にも当てはまることである．ちなみに３次方程式 $x^3+ax^2+bx+c=0$ の解を x_1, x_2, x_3 とすれば，解と係数の関係は， $x_1+x_2+x_3=-a$， $x_1x_2+x_1x_2+x_1x_2=b$， $x_1x_2x_3=-c$ ．

[15] 例えば， $\{x_1(x_1-x_2)\}/x_2$ は x_1, x_2 の有理式だが，これを置換(12)を行なってから２乗しても，２乗してから置換しても同じ結果になる．

以上の結果をまとめると，拡大体 $Q(\sqrt{r})$ を，解 $x_1, x_2, x_3, \cdots$ の対称式および交代式の集まりとして考えることができる．$Q(\sqrt{r})$ の元は一般に $a+b\sqrt{r}$ と表わせるが，このうち a, b は $x_1, x_2, x_3, \cdots$ の対称式，$\sqrt{r}$ を $x_1, x_2, x_3, \cdots$ の交代式とすれば，$Q(\sqrt{r})$ の元は「対称式＋対称式×交代式」という式の集まりと見ることができる．

ところで交代式は互換によって符号が変わるとしても，もう一度互換を行なうとまた符号が変わって元に戻る．互換を２度行なうとは偶置換のことであるから，結局 $Q(\sqrt{r})$ の元は偶置換によってはまったく値を変えないということができる．

さて次に，$n \geq 3$ の場合を考える．この方程式の解が $Q(\sqrt{r})$ のなかで得られることはない[16]．そこで，さらに拡大が行なわれる．今度は $Q(\sqrt{r})$ のなかのある数 s が選ばれ，その q 乗根 $\sqrt[q]{s}$ が追加される（q も素数）．こうして体 $K = Q(\sqrt{r}, \sqrt[q]{s})$ が構成される．この体 K は解の置換に対してどのように振る舞うだろうか．

前述の議論によって $Q(\sqrt{r})$ のどの元も解の偶置換によってはその値を変えることはない．解が 3 つ以上あるので例えば (123) のような長さ 3 の巡回置換が存在するが，これは (123)=(12)(13) のように偶置換である．だから $Q(\sqrt{r})$ の元にこれを行なっても値は変わらないが，これを新たな超数 $\sqrt[q]{s}$ に行なった場合には違う値に変わらなければならない．そうでなければ超数ではないことになる．

【定理３】によればこれも解 $x_1, x_2, x_3, \cdots$ の有理式で表わされるので，

$$\sqrt[q]{s} = g(x_1, x_2, x_3, \cdots) \quad .$$

とする．この式に偶置換 (123) を行なえば $g(x_2, x_3, x_1)$ に変わる．すなわち，

$$g(x_1, x_2, x_3)|(123) \neq g(x_2, x_3, x_1) \qquad [24]$$

ここでも見やすさを求めて，$g(x_1, x_2, x_3, \cdots)$ を g ，$g(x_2, x_3, x_1, \cdots)$ を g' としよう．以下，f ，f' のときと同様な議論を進める．

g は q 乗すれば s に戻り，対称式になる．g' を q 乗することは，g にまず置換 (123) を行なってから q 乗することであるが，これは q 乗してから置換しても同じなので，結局 $(g')^q = g^q$ となる．従って１の q 乗根をλとすれば，

$$g' = \lambda g \quad (\lambda \neq 1) \qquad [25]$$

となる．すなわち，g に置換 (123) を行なうということは「g に１の q 乗根λを掛ける」ということである．以前に，巡回置換 (123) の位数は３であるということを述べたが，それは何回同じ置換を続けると恒等置換になるかということであった．そこで式[25]の両辺にあと２回 (123) を行なってみよう．そうすれば左辺の g' は恒等置換を行なったことになるから g に戻るはずである．一方，右辺にはλが２回掛けられるから，

$$g = \lambda^3 g \quad . \qquad [26]$$

となって，$\lambda^3 = 1$ となり，$\lambda \neq 1$ から λ とは１の虚数立方根ωのことであり，素数 q は３であることがわかった．

仮に，方程式の次数がちょうど４のときには，巡回置換として (1234) や (1423) などが挙げられるが，これらは，

$$(1234) = (12)(13)(14), \quad (1423) = (14)(12)(13)$$

のように奇置換であり，偶置換には $(ab)(cd)$ のタイプのものしかない．ゆえに上記の議論に不都合は起きない．すなわち４次方程式までは，解かれたと仮定しても矛盾は起きないのである．

しかし，$n \geq 5$ の場合，つまり５次以上の方程式においては事情が異なる．解が５つ以上あるときには巡回置換には (13245) や(32154) のような長さが５以上のものが存在する．

[16]既約３次方程式が $Q(\sqrt{r})$ の中に解を持たないことは，背理法で説明できる．

$$(13245)=(13)(12)(14)(15),\ (32154)=(32)(31)(35)(34)$$

$\sqrt[3]{s}$ を有理式で表わした式を前と同様 g とする， g は偶置換によって変わるのだから，(13245) でも変わるはずである．それを改めて g' としよう．

$$g(x_{1,}x_{2,}x_{3,}x_{4,}x_{5},...)|(13245)=g(x_{3,}x_{4,}x_{2,}x_{5,}x_{1},...)=g' \quad . \qquad [27]$$

前回同様 g も g' も 3 乗すれば解の対称式になってしまうから，結局，置換 (13245) を行なっても g には 1 の 3 乗根 ω が掛かるだけである．すなわち，

$$g'=\omega g \quad . \qquad [28]$$

ところで，巡回置換 (13245) は長さ 5 であるから同じ置換をあと４回繰り返すと恒等置換になる．それを式[28]に行なえば，左辺の g' は g に戻るが，右辺には ω が 4 つ掛けられるので，

$$g=\omega^{5}g$$

となり， $\omega^{5}=1$ より， $\omega=1$ となる．式[28]の ω は 1 であることになる．このことは，5 つの解の巡回置換によっては g は値が何ら変わらないことを示す．

同様のことが偶置換 (32154) でも起きる．これも 5 回繰り返すと g' が g になるからだ．

なぜこの 2 つの偶置換を出したかというと，この 2 つの置換の積は先ほどの (123) なのである．

$$(13245)(32154)=\begin{pmatrix}12345...\\34251...\end{pmatrix}\begin{pmatrix}12345...\\51234...\end{pmatrix}=\begin{pmatrix}12345...\\23145...\end{pmatrix}=(123) \quad .$$

しかし，(13245) によっても，(32154) によっても g が変わらなければ，その積である (123) でも変わらないはずである．これが式[24]と矛盾するのである！．

方程式の解が 2 , 3 個のとき，あるいは解が 4 個のときも，解の偶置換のもっとも長いものは 3 であり，それは 3 回続けて行なう（置換の 3 乗）ことで恒等置換になるが，それは上述の ω を 3 乗すると 1 になることと矛盾しない．ω は虚数のままでいられる．が，解が 5 個以上になると長さ 5 の偶置換が出てきて，これは 5 乗しないと恒等置換にならないのに，ω は 3 乗で 1 になる．だから解が 5 つ以上になると， $Q(\sqrt{r})$ はそれ以上の拡大を許されないのである．

5 次以上の方程式が代数的に解かれ得ないという一見神秘的に見える出来事は，実はこのような他愛もないことがその理由だったのである．

以上がアーベルが証明した５次以上の方程式の代数的非可解性である．

以上の議論をガロア理論の立場から分析すると，次のようにいえるのではないか．

3 次以上のどんな方程式でも，それが Q 上既約であれば，平方根の次に 3 乗根を求めなくてはならないが，すでに平方根を Q に追加したとき，その拡大体は解の置換に対して自由ではなくなっている．その体は偶置換にのみ（累乗根の）対称性を保っているが，奇置換に大しては不変ではいられない．それもさらなる次の 3 乗根の追加になると，5 つ以上の解の偶置換では解の対称性は維持されないのである．

これによって 5 次以上の対称群をガロア群とする代数方程式の一般的な解法（ただ一つの公式によってすべての方程式を解くこと）は不可能となったが，個々の方程式にはそれぞれ固有のガロア群が存在し，それがもし 5 個以上のものからなる置換群でも，そのなかに長さ 5 以上の巡回置換がなければその方程式は代数的に解ける可能性を持つことになる．事実，代数的に解かれる 5 次以上の方程式は無数にあるのである．すべてはガロア群の解明によってのみ，5 次以上の方程式の可解性の判定を行なうことができるのである．

7. 付録

（注：ここでの証明はすべて簡易的なものである．正確・厳密なものはぜひ専門書を参照してほしい）

【付録１】 整式 $f(x)$，$g(x)$ の最大公約数を $d(x)$ とするとき，ある整式 $h(x)$，$j(x)$ が存在して，

$$h(x)f(x)+j(x)g(x)=d(x)$$

が成り立つ．

【証明】

証明は，ユークリッドの互除法で説明する．必要な記号として整式 $f(x)$ の次数を表わす「 $\deg f$ 」を導入する． $f(x)=x^3+x^2+x+1=0$ ならば， $\deg f$ =3 である．また以下ではすべて x の整式なので $f(x),g(x),d(x)$ などを f,g,d と略記する．他も同様．

整式 f，g について $\deg f \geq \deg g$ と仮定する．まず， f を g で割ったときの商を q_1 ，余りを r_1 とし，次に， g を r_1 で割った商を q_2 ，余りを r_2 とし，さらに， r_1 を r_2 で割った商を q_3 ，余りを r_3 とする....

これらの繰り返しを「ユークリッドの互除法」という．

こうして続けていくと， $\deg g>\deg r_1>\deg r_2>\deg r_3>...$ となり，次数は非負の整数だからいつかは 0 になって， n 回目についに割り切れたとする．

$$\begin{aligned}
&f=gq_1+r_1, \quad (\deg g>\deg r_1) && ...(1)\\
&g=r_1q_2+r_2, \quad (\deg r_1>\deg r_2) && ...(2)\\
&r_1=r_2q_3+r_3, \quad (\deg r_2>\deg r_3) && ...(3)\\
&\quad\vdots\\
&r_{n-2}=r_{n-1}q_n+r_n, \quad (\deg r_{n-1}>\deg r_n) && ...(4)\\
&r_{n-1}=r_nq_{n+1} && ...(5)
\end{aligned}$$

ここで式(5)から， r_n は r_{n-1} の約数であるが，式(5)を一つ上の式(4)に代入すれば，

$$r_{n-2}=r_nq_{n+1}q_n+r_n=r_n(q_{n+1}q_n+1)$$

となって， r_{n-2} も r_n を約数として持つことになる．以下同様にして順次上に昇っていけば，終には式(1)の中で f，g がともに r_n を約数として持つことがわかる．すなわち r_n は f，g の公約数である．

次に， r_n が f，g の最大公約数でないと仮定して，最大公約数を r' とすれば $\deg r'>\deg r_n$ である．r' が f，g の公約数なら式(1)から r' は r_1 の公約数でもあり， r_1 の公約数なら式(2)から r_2 の公約数でもある，...，以下同様にして式(5)まで来れば r' は r_n の約数にもなる．よって $\deg r' \leq \deg r_n$ となり， $\deg r'>\deg r_n$ と矛盾する．従って r_n は f，g の最大公約数 d である．よって式(5)は $r_{n-1}=dq_{n+1}$ となる．ユークリッドの互除法とはこのようにして最大公約数を求める方法である．

さて，式(1)から， $r_1=f-gq_1$ で，これは「 $r_1=h_1f+j_1g$ 」の形である（ $h_1=1$，$j_1=-q_1$ ）．

これを式(2)に代入すると，

$$g=(f-gq_1)q_2+r_2=f \quad \therefore r_2=g-(f-gq_1)q_2=-q_2f+(1+q_1q_2)g$$

となって「 $r_2=h_2f+j_2g$ 」の形になる．さらに式(3)にこの r_1，r_2 を代入すると，

$$\begin{aligned}
(f-gq_1)&=\{-fq_2+g(1+q_1q_2)\}q_3+r_3\\
\therefore\ r_3&=(f-gq_1)-\{-fq_2+g(1+q_1q_2)\}q_3\\
&=(f-gq_1)+fq_2q_3-gq_3(1+q_1q_2)\\
&=(1-q_2q_2)f+\{-q_1(1+q_2q_3)-q_3\}g
\end{aligned}$$

となって， $r_3=h_3f+j_3g$ の形になる．以下これを式(4)まで繰り返せば，「 $r_n=h_nf+j_ng$ 」になる．すなわち， $d(x)=h(x)f(x)+j(x)g(x)$ となる $h(x)$，$j(x)$ が存在する．（証明終わり）

参考のために初等整数論における同じ定理を証明する．それは「整数 a，b の最大公約数を d とするとき，ある整数 p，q が存在して， $ap+bq=d$ が成り立つ」というものである．

証明は以下の通り．

『与えられた整数 a,b に対して x,y を変数として $k=ax+by$ という数を考える．まず，$a=a'd,b=b'd$ とおけば， $k=a'dx+b'dy=d(a'x+b'y)$ ．ゆえに k は d の倍数である．

次に， k の中で正で最小のものを k_0 とすると， $k_0=d$ となることを示す．

まず，任意の x,y にたいして k は k_0 の倍数となることを示す．

もし k が k_0 の倍数でなければ k は k_0 で割り切れないから， $k=qk_0+r$，$(0<r<k_0)$ となる余り r があることになる．このとき， $k=ax+by$，$qk_0=q(ax_0+by_0)$ を使って，

$$r=k-qk_0=(ax+by)-q(ax_0+by_0)=a(x-qx_0)+b(y-qy_0)=ax'+by'$$

となって k_0 より小さい r が $ax+by$ の形で表わされるという矛盾が起きる．ゆえに k は k_0 の倍数である．

a 自身は， $a=a\cdot1+b\cdot0$ となるから k_0 の倍数である． b も同様．すなわち k_0 は a,b の公約数である．一方， k_0 は d の倍数でもあったから k_0 は a,b の公約数の中で最大のものでなければならない．ゆえに k_0 ＝ d ．』

【付録２】複素数を係数に持つ n 次方程式は（重複も含めて）n 個の解を持つ（代数学の基本定理）

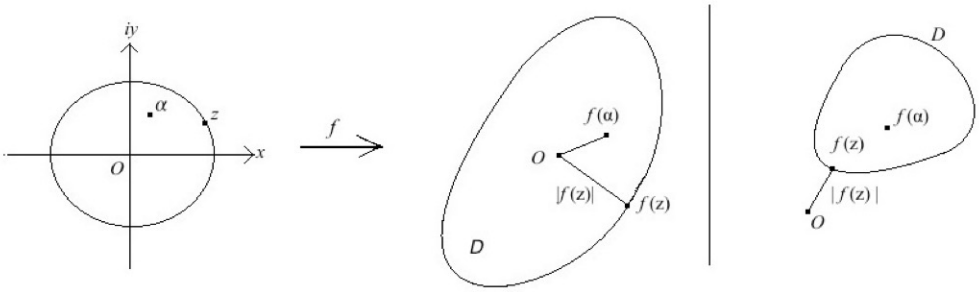
（18 世紀に K.F.ガウス等によって証明されたこの命題は，代数学の基本定理といいながら，かなりの解析学の知識を必要とする．それはこの小論の目指すところではない．ここでは高木貞治著「代数学講義」に出ている証明を換骨奪胎(?)したものを紹介する[注]．）

【証明】

まず，方程式が「少なくともひとつの解を持つ」ことを示す．それを z とすれば，$x-z$ によって方程式を整除することで $n-1$ 次の新たな方程式が得られる．これもまた少なくとも一つの解を持つからさらに整序を続ければ最後には n 個の解が得られて証明が終わる．

複素数平面については既知とし，さらに，与えられた方程式 $f(x)=0$ を複素数を変数とする関数と考えれば，$y=f(x)$ は x の値を連続的に与えることによって複素数平面上を連続的に動くことも前提とする．

次に任意の複素数 $x=\alpha$ を取ったとき，もし $f(\alpha)=0$ なら α が解になってしまうから，$f(\alpha)\neq 0$ とする．複素数平面上で α の位置を示す点（点 α という）を特定すればそれに対する $f(\alpha)$ の点も平面のどこかに特定される．$f(\alpha)\neq 0$ であるから点 $f(\alpha)$ は原点ではない．次に原点を中心として適当な半径の円を描き，この円の中および周上の任意の点に対応する点 $f(z)$ が描く領域を D とする．このとき円の大きさによっては，領域 D の中に原点 O が含まれる場合と含まれない場合がある．



仮に右図のように原点 O が領域 D の中に含まれないならば，$f(z)$ の原点からの距離すなわち $|f(z)|$ の最小値は領域の境界上にあることになる．一方，中の図のように原点 O が領域 D の中に含まれるならば，$|f(z)|$ の最小値は 0 である．$|f(z)|=0$ すなわち $f(z)=0$ となる複素数 z が存在することになる．

つまり，点 z が左図の円周上を一周したとき，それに対応する点 $f(z)$ の原点からの距離 $|f(z)|$ が $|f(\alpha)|$ よりも大きいようにすることができればいいのである．そのためには円の中に点 α が入るようにし（α が円内にあれば $f(\alpha)$ も D の中に入れておける），さらに円の半径を大きくすればよい（円はいくらでも大きくできる）．こうすれば，点 z が円全体（内部と円周上）を移動したときに $|f(z)|$ の値が一番小さくなる（=0）のは，明らかに z が円周上にあるときではない．つまり，円の内部のどこかの点 z に対して点 $f(z)$ が原点となるところがあるのである．（証明終わり）

(2014/07/22)

[注] 従ってこれは高木先生の著書中の証明そのものではなく，似て非なるものである．

【付録３】可解である方程式の解法に用いられる累乗根（超数）は，解の有理式で表わされる．

（この定理をもっと詳しくいうと，基礎体 $Q = Q_1$ に最初に追加する超数は，Q_1 のある元 r_1 の平方根 $\sqrt{r_1}$ で，拡大された体を $Q_2 = Q_1(\sqrt{r_1})$ とし，次に Q_2 に追加する超数は Q_2 のある元 r_2 の立方根 $\sqrt[3]{r_2}$ で，拡大された体を $Q_3 = Q_2(\sqrt[3]{r_2})$ とし，…等々と続けていくのであるが，こうして最後に $Q_m = Q_{m-1}(\sqrt[m]{r_{m-1}})$ に至って，与えられた方程式の解のすべて $x_1, x_2, \ldots, x_n$ が代数的に得られたとする．このとき，これらの超数はどれも解 $x_1, x_2, \ldots, x_n$ の有理式（分数式）で表わすことができるということである．ただしすべての超数は素数次の累乗根であり，途中の体 $Q_{l-1}(\sqrt[l]{r_{l-1}})$ は１の l 乗根をもすべて含むことを条件とする．）

【証明】

まず実際の例を２次方程式で見ておこう．以下では方程式はすべて基礎体上既約であるとする．

２次方程式の場合は簡単で，与えられた方程式を $x^2+ax+b=0$ とすると，超数は解の公式に出てくる $\sqrt{a^2-4b}$ である．２つの解を x_1, x_2 とすると，

$$x_1=\frac{-a+\sqrt{a^2-4b}}{2},\quad x_2=\frac{-a-\sqrt{a^2-4b}}{2}$$

とおける，この式から $\sqrt{a^2-4b}=x_1-x_2$ が出てくる．これが超数 $\sqrt{a^2-4b}$ を解 x_1, x_2 の有理式で表わしたものである．

次に３次方程式の場合を証明しよう，与えられた方程式を

$$x^3+ax+b=0 \qquad \ldots(1)$$

とおく（すべての３次方程式はこの形になる）．この方程式の基礎体を有理数体 $Q = Q_1$ とする．Q_1 の超数を $\sqrt{r_1}$ として拡大体 $Q_2 = Q_1(\sqrt{r_1})$ を作る．この体には３次方程式の解は含まれないので，さらに Q_2 の超数 $\sqrt[3]{r_2}$ から拡大体 $Q_3 = Q_2(\sqrt[3]{r_2})$ を作ったとする．そしてその中で３つの解 x_1, x_2, x_3 が（代数的に）得られたとすると，このうちのひとつ，例えば x_1 は Q_2 の元 a_2, b_2, c_2 とその超数 $\sqrt[3]{r_2}$ から

$$x_1=a_2+b_2\sqrt[3]{r_2}+c_2(\sqrt[3]{r_2})^2 \qquad \ldots(2)$$

と表わされる（**【定理２】**による）．

x_1 は方程式(1)の解であるから，$x_1{}^3+ax_1+b=0$ となる．これに(2)を代入して展開するのであるが，式を見通しよくするために $\sqrt[3]{r_2}$ を R とする．

$$(a_2+b_2+c_2R^2)^3+a(a_2+b_2+c_2R^2)+b=0 \quad .$$

これを展開･整理するのだが，$R^3=r_2$ で，これは Q_2 の元になるから，結局，R の次数は２を超えることはない．よって

$$a'+b'R+c'R^2=0 \quad (a', b', c'\in Q_2) \qquad \ldots(3)$$

となるはずであるが，$R\neq 0$ であるため，式(3)が成り立つためには $a'=b'=c'=0$ でなければならない．

次に，１の３乗根をωとして，式(2)の右辺の $R=\sqrt[3]{r_2}$ の替わりにωR を代入したものを x' とすると，

$$x'=a_2+b_2(\omega R)+c_2(\omega R)^2$$

となる．これをやはり式(1)に代入･展開･整理すれば R のときとまったく同じ結果になり，

$$a'+b'(\omega R)+c'(\omega R)^2=0 \qquad \ldots(4)$$

となるが，これは式(3)の結果から $a'=b'=c'=0$ であるので，結局，$x'^3+ax'+b=0$ を満たす．ゆえに x' は方程式(1)の解のひとつ，すなわち，$x'=x_2$ である．さらに今度は式(2)にω^2R を代入したものを x'' として同じことを繰り返せば，x'' も方程式(1)の解であることになる（$x''=x_3$）．これで解が３つそろった．すなわち，

$$x_1=a_2+b_2R+c_2R^2$$
$$x_2=a_2+b_2(\omega R)+c_2(\omega R)^2=a_2+b_2\omega R+c_2\omega^2R^2$$
$$x_3=a_2+b_2(\omega^2 R)+c_2(\omega^2 R)^2=a_2+b_2\omega^2 R+c_2\omega R^2$$

となる．ここで $x_1+x_2+x_3$ を行なうと，$\omega^2+\omega+1=0$ も使って，

$$x_1+x_2+x_3=3a_2+b_2(1+\omega+\omega^2)+c_2(1+\omega^2+\omega)=3a_2$$
$$\therefore\ a_2=\frac{1}{3}(x_1+x_2+x_3)$$

となる．つまり Q_2 の元である a_2 が３つの解 x_1,x_2,x_3 （と Q_2 の元）で表わされた．

次に b_2 も x_1,x_2,x_3 で表わすには，$\omega^2x_1+\omega x_2+x_3$ を行なえばよい．要するに b_2 の係数をそろえると他の項の係数が $\omega^2+\omega+1$ になって消滅するのである．

$$\omega^2x_1+\omega x_2+x_3=a_2(\omega^2+\omega+1)+3b_2R+c_2R^2(\omega^2+1+\omega)=3b_2R$$
$$\therefore\ b_2R=\frac{1}{3}(\omega^2x_1+\omega x_2+x_3)$$

この二つの結果から R を導けば，

$$R=\frac{1}{3b_2}(\omega^2x_1+\omega x_2+x_3)$$

となって超数 $R=\sqrt[3]{r_2}$ を x_1,x_2,x_3 の有理式で表わすことができた．

これでまだ終わりではない．今，解 x_1,x_2,x_3 で表わされたのは Q_2 の超数 $R=\sqrt[3]{r_2}$ であり，Q_1 の超数である $\sqrt{r_1}$ はまだ x_1,x_2,x_3 で表わされていない．しかしここまで来れば $\sqrt{r_1}$ を x_1,x_2,x_3 で表わすのは容易い．

上の説明で Q_2 の元である a_2,b_2 が解 x_1,x_2,x_3 の有理式で表わされることがわかった．従って Q_2 のすべての元は x_1,x_2,x_3 の有理式で表わされるわけである．

今 $Q_2=Q_1(\sqrt{r_1})$ の任意の元を $a_1+b_1\sqrt{r_1}\quad(a_1,b_1\in Q_1)$ とすれば，それが x_1,x_2,x_3 のある有理式に等しいわけだから

$$a_1+b_1\sqrt{r_1}=f(x_1,x_2,x_3)\qquad(a_1,b_1\in Q_1)$$

とおくことができる．これから，

$$\sqrt{r_1}=\frac{f(x_1,x_2,x_3)-a_1}{b_1}$$

となって，超数 $\sqrt{r_1}$ を解 x_1,x_2,x_3 の有理式で表わすことができた．

以上は３次方程式の場合であるが，これを n 次に拡張することで一般的な証明にすることができる．【証明終】

【付録４】参照図書（順不同）

以下はこの小論執筆に当たって直接参照したもののみ掲げた．著者並びに出版社に篤く感謝したい．

○淡中忠郎　著「代数学新講」

株式会社養賢堂　昭和 41 年 4 月 10 日第 12 版発行

○稲葉榮次　著「新数学シリーズ 7 群論入門」

株式会社培風館　昭和 47 年 9 月 30 日初版第 20 刷発行

○ポストニコフ　著　日野寛三　訳「ガロアの理論」

東京図書株式会社　1976 年 6 月 30 日第 13 刷発行

○奥川光太郎　著「代数学」（基礎数学講座 1 巻）

共立出版株式会社　昭和 46 年 6 月 20 日初版 22 刷（合本）発行

○中村亨　著「ガロアの群論　方程式はなぜ解けなかったのか」ブルーバックス B-1684

株式会社講談社　2010 年 7 月 16 日第 3 刷発行

○小島寛之　著「天才ガロアの発想力　ー対称性と群が明かす方程式の秘密ー」

株式会社技術評論社　2010 年 10 月 15 日初版第 2 刷発行

○矢ケ部巌　著「数III方式　ガロアの理論　アイデアの変遷をめぐって」

株式会社　現代数学社　　1978 年 4 月 20 日　2 版発行

○高木貞治　著「代数学講義」

共立出版株式会社 1994 年 6 月 10 日改訂新版 25 刷発行

○高木貞治　著「初等整数論講義」

共立出版株式会社 1994 年 7 月 1 日第 2 版 28 刷発行

【あとがき】

何十年もの夢だったガロア理論の解明を何とか実現した。200 年も前の二十歳の青年の思想を、現代の若者がコツコツ追いかけて老年になってやっと理解するなどとは、まったく笑止の他はない．

私は 1947 年の生まれで，生家が貧しく母も早く亡くし，父の仕事もままならない中で高校進学も諦めてしまったのだが，中学生生活はそれなりに楽しかった．学年が上がるごとに勉強の楽しさを知るようになり，特に数学に目覚めた．図書室の数学書などをわからないまま読み耽り，その中でアーベルやガロアという名前に出会った．

数ある数学理論のなかでも，ガロア理論は，そのドラマチックな成立過程もさることながら，五次方程式の非可解性やギリシア三大図形問題など数百年に渡る人類的課題を数行で片付けてしまうといった胸のすく威力を持っている．この威力を自分のものにしたいというのが念願となった．

中学卒業後も数学好きは変わらなかった．いくつかの画期があったが，なかでも高木貞治著「初等整数論講義」との出会いは今も忘れられない．高木先生の本で数学を志した人は数知れないと思うが，遅まきながら自分もその一員となった．もし高校·大学に進学できていれば当然もっと早く高木先生を知ったとは思うが，その方がよかったかどうかはなんともいえない．

私の次の課題は「類体論」である．高木貞治著「代数的整数論」を，私は生前に理解できるだろうか，はなはだおぼつかない話である．

2014 年 8 月 9 日　長崎原爆の日に

福沢正男