ガロア理論の初等的解題（改訂版）

―― 鵜飼勇夫氏に感謝を込めて ――

福沢正男

1．ガロア理論の基本定理

19世紀初頭，**エヴァリスト・ガロア**[1]という，わずか20歳で夭逝した数学者の遺した一篇の論文が，数百年に及ぶ数学史上の難問を根底から解決し，後の数学界に革命をもたらしたという一大ロマンは，専門の研究者ばかりでなく，数学にあまり関心のない人々にとっても興味のある出来事であろう．彼の論文はかろうじて歴史の埋没から救い出され，死後十数年にしてやっと日の目を見るに至ったのである．

幸い，かつ当然なことに，後世の数学者たちの尽力によって，彼の思想は数学全般の中でもひときわ美しい体系を持つ「**ガロア理論**」として仕上げられ，今も発展を遂げている．そんな魅力的な理論をエッセンスだけでも賞味したいと誰しも思わないだろうか，精緻な証明を抜きにしてでも天才のひらめきがもたらす威力を味わってみたいものだと．それは簡単なことではないが不可能ではないであろう．この小論はその挑戦の試みである．

ガロア理論がその威力を如実に発揮するのは「**代数方程式の不可解性の問題**」とそれに付随する若干の「**作図不可能問題**」の解決であろう．一般の５次方程式が代数的に解かれ得ないこと，あるいは定規とコンパスによる一般角（例えば60度でも）の３等分が絶対にできないことなどに対して明快に解答を与える．ここではガロア理論の誕生の契機ともなった「代数方程式の可解性の条件」，すなわち方程式にはなぜ代数的に解けるものと解けないものがあるのかその謎を解くことでガロア理論の魅力の一端を伝えたいと思う．加えて若干の作図不可能問題にも触れることにしよう．

この小論の冒頭から「**ガロア理論の基本定理**」と呼ばれるものを掲げることは一見無謀に思えるが，それには小論であるがゆえに始めに目標を掲げ，目指す峰を常に視野に入れておこうという目論見がある[2]．一つ一つの用語が理解され，定理全体の意味がつかめたときには，その峰からの眺望に思わず感嘆を洩らすことになろう．ユークリッドは「学問に王道なし」と言ったといわれるが，我々は先人のおかげでこの「王道」をゆっくり楽しみながら登ることができる．

これを読む人の数学のレベルとしては高校数学Ⅱ～Ⅲの特に代数・複素数くらいを想定するが，もちろんそれだけでは十分ではないため，随時必要な定義や用語をなるべく平易な形で取り入れていくことになる．

というわけで，まず，天下り的に「ガロア理論の基本定理」を述べる．

【定理1】(ガロア理論の基本定理)　K を k の正則拡大体，G をそのガロア群とする．K/k の中間体と G の部分群は1対1に対応し，相対応する中間体の次数と部分群の位数は等しい．

---

[1] GALOIS，Èvariste (1811/10/25~1832/5/31)　岩波数学辞典第2版を参照した．

[2] ガロア理論は現代では「体とその自己同型群に関する双対定理」（岩波数学辞典第２版）という形で把握され，ガロアが最初に示した理論形態とはずいぶん異なっているといわれている．

この定理がなぜ「代数方程式の可解性」や「作図不可能問題」などという難解極まりない問題に対して威力を発揮するのかというと，こうした問題は，**体**と呼ばれるある集合の性質の問題に帰着され，さらにその体の複雑な性質を**群**と呼ばれる別の集合に反映させることによって解決できるからである．まさにこれがガロアの天才的着想である．基本定理のなかに「**正則拡大体**」とか「**ガロア群**」という語が出てくるのがそれである．

実際，ガロアに先行する夭折の天才数学者**アーベル**[3]は体の理論を駆使して五次方程式の代数的不可解性を証明したのであった．その証明の中には群の性質も取り入れられてはいたものの，その強力な一般的原理を確立するにはガロアの功績を待たなければならなかったのである．

以下において，まず体や群といった数学用語を順次説明しよう．そうすれば自ずから基本定理の意味するところが理解されるのである．

2．体とその次数

以下の用語の説明は平易を旨とし，必ずしも厳密ではないことをことわっておく．正確な数学的概念としては数学辞典等を参照されることを望むものである．

まず，体について．

体とは，数の集合で四則（加減乗除）において閉じているものをいう．

一般に，ものの集まりを集合といい，それに含まれている一つ一つのものを元（または要素）というが，体は元どうしの四則計算の答えがやはり同じ集合の元になるような集合をいうのである（もちろん0（ゼロ）で割ることは除く）．体は加減乗除について閉じていることを要求するため，対象は主に数の集合に限られる．方程式の（代数的）解法とは，その係数などに対する四則や累乗根等の計算によってその解を求めようとするのであるから，体という考えに到るのは自然であるといえよう．

例えば，分数全体の集合を考えたとき，普通これを有理数の集合という．分数±分数，分数×分数，分数÷分数などはいずれも答えがまた分数になる．すなわち体である．これを**有理数体**といい，数における体のなかでもっとも「小さい」ものである．この小論において重要な脇役の一人で，Q で表される．

同様に実数の集合，複素数の集合なども体である．それぞれを**実数体**R，**複素数体**C と呼ぶ．

こう考えると体はもうこれ以外にはないように思われるが，これらのいわば「自然」な体に対して人為的に構成される体を考えることができるのである．

それは，有理数でない数を1つまたは数個，有理数体Qに「付け加えて」やることで実現できる．例えば，$\sqrt{2}$ という有理数でない数[4]と有理数とを加減乗除してできるすべての数から成る集合をPとすると，

$$(1)\quad P=\{a+b\sqrt{2}\ \big|\ a,b\in Q\}.$$

と表されるが，この集合は体となる．例えば加法，乗法では，

$$\left(\frac{1}{2}+3\sqrt{2}\right)+\left(-\frac{2}{5}-\frac{1}{3}\sqrt{2}\right)=\frac{1}{10}+\frac{8}{3}\sqrt{2},$$

---

[3] ABEL，Niels Henrik（1802/8/5~1829/4/6）ガロアと同時代のノルウェーの数学者．26歳で逝去（岩波数学辞典第２版参照）．

[4] √2が有理数でないことを証明するには背理法を用いる（付録1）．

$$(2+3\sqrt{2})(3-5\sqrt{2})=-24-\sqrt{2}$$

等々．減法，除法についても同様．この体を，「有理数体Qに$\sqrt{2}$を付け加えて作った体」という意味でQの**拡大体**といい，$Q\left(\sqrt{2}\right)$と表す．逆にQを$Q\left(\sqrt{2}\right)$の**部分体**ということがある．

一般には，体Kが体kの拡大体であることをK/kと言う記号で表す．

体$Q\left(\sqrt{2}\right)$の任意の元は，a,bを有理数としてすべて$a+b\sqrt{2}$の形で表すことができる．いいかえると，1と$\sqrt{2}$にそれぞれ任意の有理数a,bを掛けて足せばどんな元でも表せる．このときの1と$\sqrt{2}$の組，

$$\left\{1,\sqrt{2}\right\}$$

のことを体$Q\left(\sqrt{2}\right)$の**ひとつの底**（または**基底**）という．「ひとつの」というのは，一般にa,bを0でない有理数とすれば，aと$b\sqrt{2}$を底とすることができるからである．従って底は何組でも取れるが，その組内の個数は決まっている．その個数（今の例では2）を体$Q\left(\sqrt{2}\right)$のQに対する**次数**といい，

$$(2)\quad \left[Q(\sqrt{2}):Q\right]=2$$

と表す．$Q\left(\sqrt{2}\right)$はQに対して**二次の拡大体**であるともいう．体の次数は，その拡大の程度を表すものと見ることができる．「基本定理」にも出ているように非常に重要な概念である．

さて，この1つの例で類推できるように，体はいくらでも存在する．容易に$Q\left(\sqrt{3}\right)$とか$Q\left(\sqrt{5}\right)$などが作られるのがわかるだろう．Qのある数からその平方根（一般には累乗根）を作り，それをQに追加することで新たな体を作ることができるのである．このようにある既存の体に対してその体には属さないある数を追加して拡大体を作るとき，追加する数をその体の**生成元**という．$Q\left(\sqrt{2}\right)$の生成元は$\sqrt{2}$である．

生成元は虚数単位の$i=\sqrt{-1}$やiと実数との積$2i$などでも可能である．iについては特別で，複素数体Cを，実数体Rにiを生成元とした$C=R(i)$と表すこともできる[5]．

3．代数学の基本定理

さて，これから代数方程式に対して**体の理論**を応用するのであるが，そこではどんな方程式にも必ず解が存在することを前提にしているので，まずその根拠を示す．それが「**代数学の基本定理**」といわれるものである．

---

[5] 複素数がこのようにして定義されるわけではない．

【定理2】（代数学の基本定理）複素数を係数とする n 次代数方程式は少なくとも１つの解を持つ．（ガウス）

この定理は方程式に関するものでありながら，その証明には解析学の方法を用いるのが普通であり，この小論の範囲を超えるものであるが，ここでは**高木貞治**著「**代数学講義**」（1994年改訂新版　共立出版株式会社）に出ている証明を【付録2】にわかりやすく（換骨奪胎して）述べておく．とりあえず承認して次に進まれても一向に差し支えない．

「代数学の基本定理」から直ちに次のことがいえる．すなわち，**全ての n 次代数方程式は n 個の解を持つ**．なぜなら「少なくとも一つ」の解を α とすればこの方程式は $x-\alpha$ と $n-1$ 次式とに因数分解されるが，この $n-1$ 次式もまた $=0$ と置くことによって基本定理により解を持つ．以下これを続けていけば次の等式が成り立つ．$f(x)=0$ を n 次代数方程式とし，a をその最高次の係数 $(\neq 0)$ とすれば，

$$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)=0.$$

このとき，$\alpha_1,\alpha_2,\cdots\alpha_n$ の中に同じ解（$\alpha_i=\alpha_j=\alpha_k$ 等）があるときには**重解**と呼ばれ，一つの解で同じものの個数を**重複度**という．従って「全ての n 次代数方程式は n 個の解を持つ」というのは解の重複度も含めていうのである．

4．方程式の解による拡大体

ここでも天下り的に次の定理の提示から始めよう．

【定理3】Q を有理数体とする．$f(x)=0$ を Q の元を係数に持つ n 次既約代数方程式，α をその一つの解とするとき，拡大体 $Q(\alpha)$ の元はすべて次のような α の $n-1$ 次の整式の形の式にただ一通りに書き表される．ただし $a,b,...,m$ は有理数（Q の元）である．

$$a+b\alpha+c\alpha^2+...+m\alpha^{n-1}\quad\cdots(3)$$

この定理の意味は，α が n 次方程式の解ならば，拡大体 $Q(\alpha)$ のどんな元も α の $n-1$ 次式で表されるということである．これは方程式の解から作られた拡大体の持つ著しい性質である．

【定理3】を証明する前にいくつかの補足と例証を述べる．

まず，方程式を解くには有理数体 Q はもちろん前提とされるが，もし方程式の係数に有理数でないものが含まれている場合にはこれらを追加した体を前提して考えることは当然である．この体を**基礎体**という．すなわち基礎体とは方程式を解くために前提とされる最小限の体である．仮に，$2x^2+3\sqrt{2}x-1=0$ のように係数の中に $\sqrt{2}$ が入っていたらその基礎体は有理数体に $\sqrt{2}$ を加えた $Q\left(\sqrt{2}\right)$ ということになるのであるが，この小論では，方程式の係数は有理数のみとする．

この前提条件は，ガロア理論のエッセンスをできるだけ簡明に述べるための方策なので，必ずしも**絶対的なものではない**.

補足の第二は，**既約方程式**の意味である.

方程式が基礎体の数だけではそれ以上低次の方程式に因数分解できないとき．その方程式を**基礎体上の既約方程式**という．既約でない場合を**可約**という．例えば，$x^4+5x^2+4=0$ は左辺が因数分解できるので既約ではないが，のちに取り上げる $x^4-16x^2+4=0$ では，左辺が有理数体上で因数分解できないので既約である.

方程式の解法とは既約方程式の解法のことに他ならない．これがガロア理論の対象である.

次に【定理3】を具体的に理解するために例を挙げる.

まず，第２章で掲げた拡大体 $Q\left(\sqrt{2}\right)$ の元が全て $a+b\sqrt{2}$ と表されるとしたのは実際の計算によってであったが，$\sqrt{2}$ は有理数体 Q 上の既約二次方程式 $x^2-2=0$ の（一つの）解であり，$a+b\sqrt{2}$ は確かに $\sqrt{2}$ の「一次式」になっているからこれはこの【定理3】の例証になる.

次に，$x^3-1=0$ を取り上げる．これは Q 上可約で，方程式としては次のようにして解かれる.

$$x^3-1=(x-1)(x^2+x+1)=0$$

$$x=1,\ \frac{-1\pm\sqrt{3}i}{2}$$

このうち，$x=\dfrac{-1\pm\sqrt{3}i}{2}$ は既約方程式 $x^2+x+1=0$ の解で，「**１の虚数立方根**」と呼ばれ，±の二つあるうちどちらかを ω（オメガ）で表すと，もう一方は ω^2 で表されるという著しい特徴を持つ．ゆえに普通どちらを ω とするかは特定されない．また，次のことが成り立つ.

$$\omega^3=1,\ \omega^2+\omega+1=0$$

いずれも $x^3-1=(x-1)(x^2+x+1)=0$ から導かれる性質である.

ω は代数方程式の解法に関する理論全般の中でも特別重要な数である.

今の場合，【定理3】でいう $f(x)=0$ として $x^2+x+1=0$ を，α として ω を取ると，拡大体 $Q(\omega)$ の元は,

$$a+b\omega=a+b\left(\frac{-1+\sqrt{3}i}{2}\right)\quad(a,b\in Q)$$

ということになるが，この式は次のように変形できる.

$$a+b\left(\frac{-1+\sqrt{3}i}{2}\right)=\left(a-\frac{1}{2}b\right)+\frac{b}{2}\sqrt{3}i=a'+b'\sqrt{3}i\qquad(a',b'\in Q)$$

すなわち，$Q(\omega)$ は $Q\left(\sqrt{3}i\right)$ と（集合としては）同じものと考えて差しつかえない.

$$Q(\omega)=Q\left(\sqrt{3}i\right).$$

$Q\left(\sqrt{2}\right)$も$Q(\omega)$もQの二次拡大体であるが，その元は生成元の一次式で表される．

もう一つ，拡大体の次数が３である場合を取り上げておく．それは，

$$x^3-2=0$$

である．

一般に，$x^n-a=0$（aは有理数とする）の形の方程式を「**二項方程式**」といい，nとaの値によっては可約であったり既約であったりする．二項方程式についてはのちに詳しく取り上げるが，ここでは$x^3-2=0$についてだけ，高校数学的に解を求めておく[6)]．

$x^3-2=0$とは，要するに２の立方根を求めることであるが，これは三次方程式なので解は３つある．実数関数$y=x^3-2$のグラフを書いてみれば，明らかに一つの実数解が存在することがわかるからその実数解を「$\sqrt[3]{2}$」で表そう．すると他の二つを１の虚数立方根ωを用いて，$\sqrt[3]{2}\omega$，$\sqrt[3]{2}\omega^2$で表すことができる．いずれも３乗すれば２になることがわかるだろう．これを用いてx^3-2を一次式に分解できる．

$$x^3-2=\left(x-\sqrt[3]{2}\right)\left(x-\sqrt[3]{2}\omega\right)\left(x-\sqrt[3]{2}\omega^2\right).$$

この右辺を展開して左辺になることを確認してほしい．

$\sqrt[3]{2}$は今後頻繁に登場するので見やすくするために$\theta=\sqrt[3]{2}$で表すことにする．

$x^3-2=0$は明らかにQ上既約である．これを【定理3】における$f(x)=0$をQ上の三次既約方程式とし，αとして$\theta=\sqrt[3]{2}$を取ってみよう．基礎体kの拡大体$k\left(\sqrt[3]{2}\right)$の元は【定理3】によれば，

$$a+b\theta+c\theta^2 \quad （a,b,c\in Q）$$

で表される．拡大体$k(\theta)$の底として$\left(1,\theta,\theta^2\right)$をとることができるので，次数は３である．そしてその元はθの二次式で表される．

補足の最後に，【定理3】を証明するために，次のような整式に関する定理を述べる．

【定理４】整式$F(x)$，$G(x)$の最大公約数を$d(x)$とするとき，ある整式$p(x)$，$q(x)$が存在して，

$$F(x)p(x)+G(x)q(x)=d(x)$$

が成り立つ．

この定理は，まず**整数**で理解してのち整式で考えるといいだろう．すなわち整数において，任意の整数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$ap+bq=d$が成り立つのである．例えば，整数$34,18$の最大公約数は2であるが，それに対して$34p+18q=2$となる整数p,qが存在することを保証

---

6) 三次方程式の一般的解法はこの小論では取り上げない．

するのがこの定理である（解の例： $p=-1,\ q=2$ ）．【定理４】の証明は末尾の【付録3】として掲載した．ここでは【定理４】を既知として先に進むことにする．

【定理3の証明】

拡大体 $K=k(\alpha)$ の任意の元は，体の説明で述べたように k の元と α との加減乗除の結果（＝分数式）として表されるから，どのような元も

$$\frac{a_1+b_1\alpha+c_1\alpha^2+\cdots}{a_2+b_2\alpha+c_2\alpha^2+\cdots}=\frac{F(\alpha)}{G(\alpha)} \quad \cdots(4)$$

のように表されるはずである．$F(\alpha),\ G(\alpha)$ はそれぞれ α の任意の整式である（もちろん $G(\alpha)\neq 0$ ）．【定理３】はこの式がどんな場合でも有理化され，しかも α の $n-1$ 次式になるということを示している．

今，$G(\alpha)$ の α を x に置き換えて $G(x)$ という整式を作り，$G(x)$ と【定理3】にある $f(x)$ との最大公約数[7]を考えると，仮定により $f(x)$ は Q 上既約なので最大公約数は 1 である．ゆえに【定理４】によってある整式 $p(x),q(x)$ が存在して，

$$G(x)p(x)+f(x)q(x)=1$$

が成り立つ．ここで α は $f(x)=0$ の解であるから $f(\alpha)=0$ である．ゆえに，上の式に $x=\alpha$ を代入すると，$G(\alpha)p(\alpha)=1$ となる．よって，

$$p(\alpha)=\frac{1}{G(\alpha)}$$

となる．これを(4)式に代入すれば，

$$\frac{F(\alpha)}{G(\alpha)}=F(\alpha)p(\alpha)$$

となって有理化された．

次にこの式が α の $n-1$ 次式になることを示す．そこで，また $F(\alpha)p(\alpha)$ の α を x に変えて，

$$c(x)=F(x)p(x)$$

と置き，$c(x)$ を $f(x)$ で割ったときの商を $h(x)$，余りを $r(x)$ と置けば，$r(x)$ は $f(x)$ よりも低い次数，すなわちせいぜい $n-1$ 次式の整式である．ゆえに

$$c(x)=f(x)h(x)+r(x)$$

となる．ここでまた $x=\alpha$ を代入すれば $f(\alpha)=0$ であるから，結局，

$$c(\alpha)=r(\alpha)$$

となって $c(\alpha)$ すなわち $k(\alpha)$ の任意の元は $n-1$ 次式の整式となることが示された．最後に $c(\alpha)$ がただ一通りに表されることを示すには，もし $c(\alpha)$ が２通りに表されたと仮定すれば，

$$c(\alpha)=c_1+c_2\alpha+c_3\alpha^2+\cdots+c_n\alpha^{n-1}=c_1'+c_2'\alpha+c_3'\alpha^2+\cdots+c_n'\alpha^{n-1}$$

---

[7] 整式についても約数・倍数・最大公約数・最小公倍数があることは既知とする．

と書ける．ここで中辺から右辺を引き算をしてみると，

$$\begin{aligned}&(c_1+c_2\alpha+c_3\alpha^2+\cdots+c_n\alpha)-(c_1'+c_2'\alpha+c_3'\alpha^2+\cdots+c_n'\alpha^{n-1})\\&=(c_1-c_1')+(c_2-c_2')\alpha+(c_3-c_3')\alpha^2+\cdots(c_n-c_n')\alpha^{n-1}\\&=0\end{aligned}$$

これが成り立つためには$c_1=c_1',c_2=c_2',c_3=c_3',\cdots,c_n=c_n'$でなくてはならない．ゆえに一通りとなる．【証明終】

【定理３】を証明するために多くのことを述べたが，これでようやく体に関する議論を先に進めることができる．

5. 正則拡大体

ここからはKがkの拡大体であることを示す記号としてK/kを多用する．

【定理3】によって，基礎体k上の既約なn次方程式$f(x)=0$の解$x=\alpha$から作った拡大体$K=k(\alpha)$の元はいつでも$a+b\alpha+c\alpha^2+...+m\alpha^{n-1}$の形をしていることから，底として$\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$をとることができ，その個数から体$K$の$k$に対する次数は$n$である．

$$[K:k]=n.$$

n次既約方程式の次数と，基礎体に解を追加してできる体の次数が一致することは方程式に体の理論を適用することの合理性を示しているといえる．そこからさらに発展してn次既約方程式$f(x)=0$のαによる拡大体K/kに対して$f(x)=0$のα以外の他の解，仮にα'とする．このα'における拡大体$K'=k(\alpha')$との関係を考えよう．もちろん$k(\alpha')$のkに対する次数も同じnである．さらに$k(\alpha)$と$k(\alpha')$の元のあいだに次のような1対1の対応をつけることができる．すなわち$k(\alpha)$の元

$$a+b\alpha+c\alpha^2+...+m\alpha^{n-1}$$

に$k(\alpha')$の元

$$a+b\alpha'+c\alpha'^2+...+m\alpha'^{(n-1)}$$

を対応させるのである．つまり各項の係数（有理数）が全く同じであるような対応である．この対応は単に元が1対1対応するだけでなく，元同士の加減乗除の結果もまた対応するのである．こうした対応を**体の同型対応**といい，係数が基礎体kの元のときは特にk **同型対応**という．

いくつかの例を挙げよう．

Q上既約な二次方程式$x^2-2=0$の解$\sqrt{2}$による拡大体$Q(\sqrt{2})$の元の一般形は$a+b\sqrt{2}$（$a,b\in Q$）であるが，これに対して同じ方程式のもう一つの解$-\sqrt{2}$による拡大体$Q(-\sqrt{2})$の元の一般形は$a+b(-\sqrt{2})=a-b\sqrt{2}$である．$Q(\sqrt{2})$の元$a+b\sqrt{2}$に対して$Q(-\sqrt{2})$の元$a-b\sqrt{2}$を

対応させれば，これはQ同型対応となる．実際，$Q\left(\sqrt{2}\right)$の元同士の和・差・積・商は，対応する$Q\left(-\sqrt{2}\right)$の元同士の和・差・積・商にそれぞれ対応する．

	$Q\left(\sqrt{2}\right)$の元：$a+b\sqrt{2}\,,c+d\sqrt{2}$	$Q\left(-\sqrt{2}\right)$の元：$a+b\left(-\sqrt{2}\right),c+d\left(-\sqrt{2}\right)$
和	$(a+c)+(b+d)\sqrt{2}$	$(a+c)+(b+d)\left(-\sqrt{2}\right)$
差	$(a-c)+(b-d)\sqrt{2}$	$(a-c)+(b-d)\left(-\sqrt{2}\right)$
積	$(ac+2bd)+(ad+bc)\sqrt{2}$	$(ac+2bd)+(ad+bc)\left(-\sqrt{2}\right)$
商	$\frac{ac-2bd}{c^2-2d^2}+\frac{-ad+bc}{c^2-2d^2}\sqrt{2}$	$\frac{ac-2bd}{c^2-2d^2}+\frac{-ad+bc}{c^2-2d^2}\left(-\sqrt{2}\right)$

ところで，体$Q\left(\sqrt{2}\right)$と$Q\left(-\sqrt{2}\right)$は，生成元が違いこそすれ，集合としてはまったく同じものだということはすぐにわかるのであるが，このことは，ひとつの集合が二つの異なる体を内部に形成しているということである．これは「体」という構成体が実は複雑な性質を有することを示唆している（もちろん，Qも内部の体の一つである）．

方程式$f(x)=0$の基礎体をk，n個の解を$\alpha_1,\alpha_2,\cdots,\alpha_n$とするとき，これらを互いに**共役数**という．これに因んで方程式$f(x)=0$の解による拡大体も$k(\alpha_1),k(\alpha_2),\cdots,k(\alpha_n)$と$n$個あるのだが，これらを互いに**共役体**と呼ぶことにする．先の体$Q\left(\sqrt{2}\right)$は，その共役体$Q\left(-\sqrt{2}\right)$を自身の中に持っているのである．

一般に，既約方程式の基礎体kに対して，方程式の解αによる拡大体$k(\alpha)$が全ての共役体を含むとき，この体$k(\alpha)$を「**正則拡大体**」と（あるいは**ガロア拡大体・ガロア体**とも）いう．この定義によって，体$Q\left(\sqrt{2}\right)$は正則拡大体である，あるいは体$Q\left(\sqrt{2}\right)$はQに対して正則であるという．正則拡大体はガロアの発見によるものである．

もうひとつの例として，先に取り上げた $x^3-2=0$ について考えよう．この場合は事情が多少複雑になる．前に述べたように$\theta=\sqrt[3]{2}$とする．

$x^3-2=0$の基礎体を有理数体Qとするならば，三つの共役体は $Q(\theta)$，$Q(\theta\omega)$，$Q\left(\theta\omega^2\right)$ であるが，これら互いの共役体は全く別の集合となる．$Q(\theta)$はωを含んでいないし，$Q(\theta\omega)$と$Q\left(\theta\omega^2\right)$も似て非なる集合で一致しない．互いに包含関係もない．従ってどれも正則拡大体とはいえない．

このような場合には，$Q(\theta)$にさらにωを追加して体を拡大するのである．これを，

$$Q(\theta,\omega)$$

で表す．これは基礎体Qに先にωを追加しておいて，あとからそれにθを追加しても結果は同じ体になる．すなわち，

$$Q(\omega,\theta)=Q(\theta,\omega)$$

しかし，これらの体ではその元の表現に微妙な違いがある．$Q(\theta,\omega)$の場合の各元は，先にθを追加して$Q(\theta)$を作っており，その後にωを追加するので，その一般の元は$Q(\theta)$の元を係数とするωの一次式となる．すなわち，$Q(\theta)$の元をA, Bとすれば$Q(\theta,\omega)$の元は，

$$A+B\omega$$

であるが，このA, Bは$Q(\theta)$の元だから，$a_1,b_1,c_1;a_2,b_2,c_2\in Q$として，

$$A=a_1+a_2\theta+a_3\theta^2,\ B=b_1+b_2\theta+b_3\theta^2$$

である．ひとつにまとめて書くと，

$$(1)\quad A+B\omega=\left\{a_1+a_2\theta+a_3\theta^2\right\}+\left\{b_1+b_2\theta+b_3\theta^2\right\}\omega$$

ということになる．

一方の$Q(\omega,\theta)$では，先にωを追加して$Q(\omega)$を作り，後からθを追加しているので，$Q(\omega,\theta)$の一般の元は，C, D, Eを$Q(\omega)$の元として，

$$C+D\theta+E\theta^2,\quad C,D,E\in Q(\omega)$$

となる．この場合のC, D, Eは$Q(\omega)$だから，

$$C=c_1+c_1\omega,\quad D=d_1+d_2\omega,\quad E=e_1+e_2\omega$$

である．これもひとつにまとめて書くと，

$$(2)\quad C+D\theta+E\theta^2=\left(c_1+c_1\omega\right)+\left(d_1+d_2\omega\right)\theta+\left(e_1+e_2\omega\right)\theta^2$$

となる．しかし，(1)，(2)とも実は同じ集合の別の表現になっている．何れにしても$Q(\omega,\theta)$，$Q(\theta,\omega)$は同じ体，しかも正則拡大体となっている．

$x^3-2=0$の場合，基礎体をQではなくて，初めから$k=Q(\omega)$としてもよい（kはω^2も含むので$Q\left(\omega,\omega^2\right)$とする必要はない）．$x^3-2=0$の三つの解 θ，$\theta\omega$，$\theta\omega^2$ にそれぞれ三つの拡大体$k(\theta)$，$k(\theta\omega)$，$k\left(\theta\omega^2\right)$が対応する．そうすると今度はこのうちのどれを取っても他の共役体を含むので，いずれもが正則拡大体になる．先の体$Q(\theta)$との違いは，基礎体kにすでに1の立方根ωを持たせていることである．

このように，一個の解によって正則拡大体を作ることはできなくても，Qに必要な生成元を追加することで，ついには正則拡大体を作ることができる．ゆえに結局はどのような方程式にもそれに対応する正則拡大体が存在する．

一般に，ただ一つの数を追加してできる拡大体を**単純拡大体**という．さらに，有理数体Qに既約方程式の解を何個か追加して正則拡大体を作るときに，それをただひとつの数を追加して同じ拡大体を作ることが可能であるが，それを簡潔に証明することができなかったことを理由に触れないことにする．

体の次数については次の定理が成り立つ.

【定理５】 k **を** Q **の拡大体，さらに** K **を** k **の拡大体とするとき，** K **の** Q **に対する次数** $[K:Q]$ **について,**

$$[K:Q]=[K:k]\times[k:Q]$$

が成り立つ.

【証明】

先ほどの $x^3-2=0$ の正則拡大体 $Q(\omega,\theta)$ の説明で述べたように，K/k の各元は k/Q の元を係数にして表現されるから，K/k の元の $[K:k]$ 個ある各項の各々に，$[k:Q]$ 個の k/Q の元が係数となるので，それらを展開したときの項数は $[K:k]\times[k:Q]$ になる．すなわち，

$$[K:Q]=[K:k]\times[k:Q]$$

となる．ややこしそうだが，言っていることは簡単なことである．【証明終】

例えば，$x^3-2=0$ の基礎体を $k=Q(\omega)$ とするならば，$K=k\left(\sqrt[3]{2}\right)$ の k に対する次数は３である．$[K:k]=3$．しかし，もし基礎体を Q にするなら $k=Q(\omega)$ は Q に対して二次の拡大体であるから $[k:Q]=2$ であり，ゆえに，$[K:Q]=[K:k]\times[k:Q]=3\times2=6$ となる.

以上の結果から，**既約方程式の解を基礎体に追加して正則拡大体を作ることができ，共役体はその部分体になる**ということがわかった.

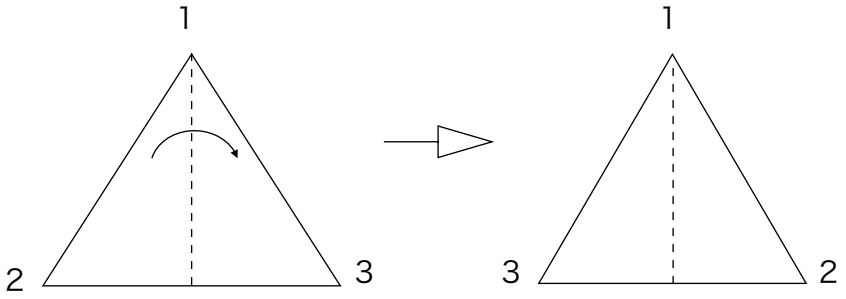
これで，「ガロア理論の基本定理」のうち，「Kを$\boldsymbol{k}$の正則拡大体」というところの説明を終えたことにする.

次は**ガロア群**についての説明に移るが，そのためにまず**群**についての一般論を述べる.

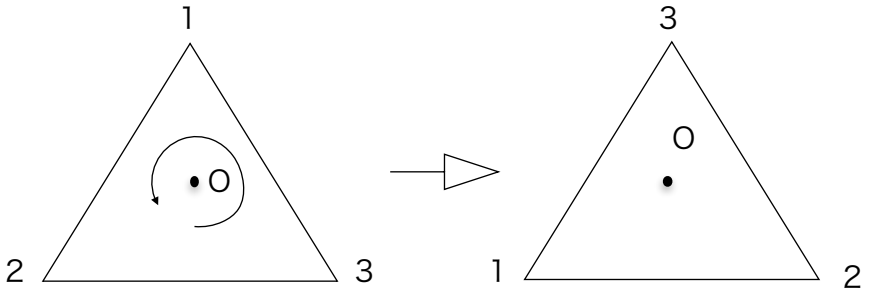
6. 群および置換群

群とは，ガロアが初めて使い出した数学用語で，数ではないもの（数でもよいが）の集合があるひとつの「演算」を満たしているとき，それを群と呼ぶ．群にもいろいろあるが，ガロア理論で群といえば**置換群**のことといってよい.

置換とはものの位置を置き換えることである．例えば正三角形を移動してまたそれ自身にぴったり重ねることを**正三角形の置換**ということにする．正三角形の各頂点を1，2，3とするとき，頂点1から対辺に垂線を引いて，この垂線を軸にして線対称移動させた時，正三角形はまた自分にぴり重なるのでこの対称移動は置換である．（下図左）



また正三角形の重心を中心として120°回転させることでも置換できる.



これらの置換の中に，正三角形をまったく「動かさない置換」も含むことにすると（これを**恒等置換**という），これらの置換には全部で6通りある．線対称による置換3つと重心を中心とした正120°の回転と正240°の回転，そして恒等置換．この6つの置換の集合が「群」という構造を持つことを示す.

この6つの置換を記号で表現してみよう．正三角形の置換は頂点を表す1,2,3という3つの文字を置き換えていると見ることもできる．よってこの6つの置換を正三角形という言葉を使わずに単に3つの文字123がこの順序から132に，あるいは312等々に換わることと表現しても同じことである.

実際の置換：123→123，123→132，123→213，123→231，123→312，123→321.

置換の表現： $\begin{pmatrix}123\\123\end{pmatrix}$, $\begin{pmatrix}123\\132\end{pmatrix}$, $\begin{pmatrix}123\\213\end{pmatrix}$, $\begin{pmatrix}123\\231\end{pmatrix}$, $\begin{pmatrix}123\\312\end{pmatrix}$, $\begin{pmatrix}123\\321\end{pmatrix}$.

置換の名前： σ_1 ， σ_2 ， σ_3 ， σ_4 ， σ_5 ， σ_6 .

(σ はギリシア小文字でシグマと読む) .

「置換の表現」では括弧の中の上の文字列を下の文字列に並べ替えて（置き換えて）いる．「置換の名前」は，例えば「置換σ_4」といった場合には「123→213」という「置換操作」を表すのである．したがって，

$$\sigma_1=\begin{pmatrix}123\\123\end{pmatrix},\sigma_2=\begin{pmatrix}123\\132\end{pmatrix},\sigma_3=\begin{pmatrix}123\\213\end{pmatrix},\sigma_4=\begin{pmatrix}123\\231\end{pmatrix},\sigma_5=\begin{pmatrix}123\\312\end{pmatrix},\sigma_6=\begin{pmatrix}123\\321\end{pmatrix}$$

と定義する．この6つの置換の集合にS_3という名前を付ける．(置換の順序は辞書式とした)

$$S_3=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6\}$$

置換が6つあるのにS_3と名付けるのは3個の「もの」の置換という意味である．ものは数字でなくてもABCでも定規・鉛筆・消しゴムでもよい．3つのものの置き換えや並べ替えを表現するのにこのS_3が使える．

さて，この$\sigma_1,\sigma_2,\cdots,\sigma_6$を使って，例えば $\sigma_2\otimes\sigma_4$ という「演算」を定義してみよう．⊗という記号には特に意味はない．

$\sigma_2\otimes\sigma_4$ とは，最初 123 と並んでいる文字列に対して，まず $\sigma_2=\begin{pmatrix}123\\132\end{pmatrix}$を行ない，続けて $\sigma_4=\begin{pmatrix}123\\231\end{pmatrix}$を行なうことを意味するものとするのである．つまり置換を連続で行なうのである．

実際には次のようにして置換の連続を「計算」する．

$$\sigma_2\otimes\sigma_4=\begin{pmatrix}123\\132\end{pmatrix}\begin{pmatrix}123\\231\end{pmatrix}=\begin{pmatrix}123\\213\end{pmatrix}=\sigma_3$$

計算の手順は，まず，1 はσ_2によって1 のままだが，σ_4 によって 2 に置き換わっているから結局 1 は 2 に換わる．同様に 2 はまずσ_2で 3 に，その 3 は次のσ_4で 1 に換わっているから結局 2 は 1 に換わっている．最後に 3 はσ_2で 2 に，その 2 はσ_4で 3 に換わっている．よって1→2，2→1，3→3と置換されたから，これは$\sigma_3=\begin{pmatrix}123\\213\end{pmatrix}$に当たる．

この置換の連続を先ほどの正三角形の移動に当てはめてみると，$\sigma_2\otimes\sigma_4$ とは，頂点 1 からの垂線による対称移動のあと，重心を中心とした正120°の回転移動を行なうことを表すから， 1 の頂点は 2 へ， 2 は 1 へ，3 はもとの位置に戻るから，結局頂点 3 からの垂線による対称移動を行なった結果と同じになるのでσ_3を1回行なったのと同じことになる．２つの置換の連続がひとつの置換で表されるのである．

こうして「置換」という操作の集合に「演算」を定義することができた．この演算によってS_3を**群**とすることができるのである．

一般に，群の定義とは次のようなものである．

【定義１】

集合Gの元のあいだに，あるひとつの演算が定義されていて，次の３つの条件，

Ａ：演算の成立とその一意性

Ｂ：演算の結合法則

Ｃ：逆演算が可能

が満たされるとき，Gを群と呼ぶ．

（参考：「群論入門」稲葉榮次著より　培風館「新数学シリーズ７」昭和47年).

ガロア理論の持つ深遠な美しさは，この群の持つ見た目の単純性と奥深さをその根拠としているといってもよいであろう．

一般に，**演算**とは「集合内の2つのものに同じ集合内の一つのものを対応させる決められた操作のこと」である．通常の数による加法や乗法はもちろん演算であるが，このように置換を連続させることも演算と考えることができるのである．

ここですぐあとの「**群表**」作成のために，置換の表現として「**巡回置換**」を取り入れる．

任意の置換，例えば$\begin{pmatrix}123\\132\end{pmatrix}$のように，1はそのまま，2は3に，3は2というように，2と3だけが入れ換わっているときには，単に(23)と表すことにする．1は変わらないので省略して２行表示を１行にするのである．つまり，(23)とは1は変わらず2は3に３は２に変わっているものと見るのである．

こうすると，$\begin{pmatrix}123\\213\end{pmatrix}$は(12)，$\begin{pmatrix}123\\321\end{pmatrix}$は(13)となる．このように2つのものだけが入れ替わっている置換を特に**互換**という．

そして，$\begin{pmatrix}123\\231\end{pmatrix}$のように，1は2に，2は3に，そして3は1に戻る，というように一巡して入れ替わっているときには，(123)と表すことにする．$\begin{pmatrix}123\\312\end{pmatrix}$なら，１→３→２→1と巡回しているので(132).

このような置換を**巡回置換**と（**循環置換**とも）いう．括弧の中の個数を巡回置換の**長さ**という．(132) は長さ３の巡回置換である．互換は長さ２のもっとも短い巡回置換である．巡回置換はどこから始めても同じなので，(123)=(231)=(312)であるが，見極めやすいように一番小さい数を最初に書くことにする．

巡回置換によって置換を表す場合には恒等置換は（誤解がなければ）１で表すこともある（括弧なし）．

この表記によれば，$N_3=\{\sigma_1,\sigma_2,\sigma_3\}$は，

$$N_3=\{1,(123),(132)\}$$

で表される．

この表現を使うと置換の積が求めやすくなる場合がある．例えば二つの置換の積，

(23)(123)

の場合には，1は始めの置換では変わらない（かっこの中にないものは変わらない）で，次の置換で2になっているので，2と書いておく．次の2は始めの置換で3に変わり，次の置換で1に変わっているので，続けて1と書く．最後の３は始めの置換で2に，次の置換で3になっているので３と書けば，213となる．これは$\begin{pmatrix}123\\213\end{pmatrix}$のことであるから，積は(12)となる．(23)(123)=213=(12)．（注意：途中の213は(213)のことではなく，$\begin{pmatrix}123\\213\end{pmatrix}$の下の行だけを書いたもの．）

実際の群においては，次のように「九九表」を作成することで群であることを確定するのが便利である．S_3の九九表を作ってみよう．

$\sigma_1=\begin{pmatrix}123\\123\end{pmatrix},\sigma_2=\begin{pmatrix}123\\132\end{pmatrix},\sigma_3=\begin{pmatrix}123\\213\end{pmatrix},\sigma_4=\begin{pmatrix}123\\231\end{pmatrix},\sigma_5=\begin{pmatrix}123\\312\end{pmatrix},\sigma_6=\begin{pmatrix}123\\321\end{pmatrix}$を巡回置換で表せば，

$\sigma_1=1,\ \sigma_2=(23),\ \sigma_3=(12),\ \sigma_4=(123),\ \sigma_5=(132),\ \sigma_6=(13)$ であるから（σ_1 のあるものは省略），表の各行を計算すると，

σ_2 行：$\sigma_2\ \sigma_2=(23)(23)=1=\sigma_1$，$\sigma_2\ \sigma_3=(23)(12)=231=(123)=\sigma_4$，

$\sigma_2\ \sigma_4=(23)(123)=213=(12)=\sigma_3$，$\sigma_2\ \sigma_5=(23)(132)=321=(13)=\sigma_6$，

$\sigma_2\ \sigma_6=(23)(13)=312=(132)=\sigma_5$．

σ_3 行：$\sigma_3\ \sigma_2=(12)(23)=312=(132)=\sigma_5$，$\sigma_3\ \sigma_3=(12)(12)=1=\sigma_1$，

$\sigma_3\ \sigma_4=(12)(123)=321=(13)=\sigma_6$，$\sigma_3\ \sigma_5=(12)(132)=132=(23)=\sigma_2$，

$\sigma_3\ \sigma_6=(12)(13)=231=(123)=\sigma_4$．

σ_4 行：$\sigma_4\ \sigma_2=(123)(23)=321=(13)=\sigma_6$，$\sigma_4\ \sigma_3=(123)(12)=132=(23)=\sigma_2$，

$\sigma_4\ \sigma_4=(123)(123)=312=(132)=\sigma_5$，$\sigma_4\ \sigma_5=(123)(132)=123=1=\sigma_1$，

$\sigma_4\ \sigma_6=(123)(13)=213=(12)=\sigma_3$．

σ_5 行：$\sigma_5\ \sigma_2=(132)(23)=213=(12)=\sigma_3$，$\sigma_5\ \sigma_3=(132)(12)=321=(13)=\sigma_6$，

$\sigma_5\ \sigma_4=(132)(123)=123=1=\sigma_1$，$\sigma_5\ \sigma_5=(132)(132)=231=(123)=\sigma_4$，

$\sigma_5\ \sigma_6=(132)(13)=132=(23)=\sigma_2$．

σ_6 行：$\sigma_6\ \sigma_2=(13)(23)=231=(123)=\sigma_4$，$\sigma_6\ \sigma_3=(13)(12)=312=(132)=\sigma_5$，

$\sigma_6\ \sigma_4=(13)(123)=132=(23)=\sigma_2$，$\sigma_6\ \sigma_5=(13)(132)=213=(12)=\sigma_3$，

$\sigma_6\ \sigma_6=(13)(13)=1=\sigma_1$．

この結果を表にすると以下の通り．

表-1

S_3	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

例えば，$\sigma_2\otimes\sigma_4$ を表に記入するには，見出し列から σ_2 を見つけ，見出し行から σ_4 を見つけてその行・列の交差するところに演算の結果 σ_3 を書き込む（表のハイライト参照）というようにして順次表を完成させる．

以後，$\sigma_a\otimes\sigma_b$ における $\otimes$ は簡単のため省略し，単に $\sigma_a\sigma_b$ と示す．その結果も「積」と呼ぶことにする．数の乗法に倣うのである．ついでに積を作ることを「かける」ともいうことにする．

この表によって S_3 が群であることを示そう．群の定義を見てほしい．

まず，「A：演算の成立」とは，全ての元同士について演算が可能である場合をいい，ひとつでも例外があれば成立とは言わない．また，一意性とは，演算の結果となる元がいつも一つに限ることをいう．これは表によって明らかである．

「B：演算の結合法則」とは，数の乗法でいう $(ab)c=a(bc)$ のことで，要するに演算の順序によって結果が変わらないことをいう．S_3 で，例えば，

$$(\sigma_2\sigma_3)\sigma_5=\sigma_2(\sigma_3\sigma_5)$$

でいうと，これは左辺では，まず積$\sigma_2\sigma_3$を行ない（$=\sigma_4$），それから$\sigma_4\sigma_5$を行っている（結果はσ_1）．一方，右辺では，まず$\sigma_3\sigma_5$を行なっておいて（$=\sigma_2$），その結果のσ_2に対して左側からσ_2の操作を行なって$\sigma_2\sigma_2$を実行する（結果はσ_1で左辺と等しい）．それが任意の元において常に成り立つというのが「結合法則が成り立つ」という意味である．

群の定義で重要なのは，「**交換法則**」は一般には成り立たないということである．数の乗法では $ab=ba$ は常識であるが，S_3 では，例えば，

$$\sigma_2\sigma_4\neq\sigma_4\sigma_2$$

である．左辺$\sigma_2\sigma_4=\sigma_3$であるが，右辺$\sigma_4\sigma_2=\sigma_6$となって交換法則は成り立たない．

交換法則の成り立つ群も存在する．それは「**アーベル群**」と（**可換群**とも）呼ばれる重要な群である．

最後の「C：逆演算が可能」とは，G の任意の2つの元σ_a，σ_bに対して，

$$\sigma_a\sigma_x=\sigma_b$$

が成り立つ元 σ_x が存在することである．

例えば，S_3の元σ_2，σ_3に対して，$\sigma_2\sigma_x=\sigma_3$が成り立つ$x$は 4 である．要するに，数の乗法に対する除法のように逆の計算が成り立つことであるが，×に対して÷というように逆演算を定義することはなく，$\sigma_a\sigma_x=\sigma_b$という方程式の解の存在を保証するのである．

この表から群の定義を全て確認することが可能である．群であることを確認した上は，この表を「**群表**」という．

いくつかの重要な群の用語・性質を述べる．

群の元の個数を群の**位数**という．位数が有限の群を**有限群**，無数の群を**無限群**という．有限群の例はこれから述べる置換群があるが，無限群の身近な例としては，整数全体の集合 Z に通常の加法を「演算」として定義したとき，Zは無限群になる．演算の一意性も結合法則も，逆演算も（もちろん減法）成り立つ．このことから群はいくらでもあることが類推されるであろう．

群表で著しいのは σ_1 である．数の1のようにどの元に掛けてもその元を変えない．置換の場合には恒等置換を表していたが，一般の群では**単位元**と呼ばれる．任意の元σ_nに対して，

$$\sigma_n\sigma_1=\sigma_1\sigma_n=\sigma_n$$

が成り立つ．

次に，逆演算が可能なことから任意の元σ_nに対して，

$$\sigma_n\sigma_x=\sigma_1$$

となるような元σ_xが存在するが，このσ_xをσ_nの「**逆元**」と呼んで，σ_n^{-1}で表す．よって$\sigma_n\sigma_n^{-1}=\sigma_1$．また表から$\sigma_n^{-1}\sigma_n=\sigma_1$も成り立つ．積が$\sigma_1$になっているところの行・列の見出し元は互いに逆元となっている（例：σ_3とσ_6）．逆元は数で言う「逆数」に当たるものといえる．

逆元を正三角形の置換で考えるとき，例えばσ_3 の逆元が同じ σ_3 なのは，σ_3 は頂点３から引いた垂線を軸とした線対称移動を表しており，もう一度同じ線対称移動を行なうと正三角形が元に戻る，つまり恒等置換と同じになるからである．またσ_4 の逆元がσ_5なのはσ_4が120°の回転を表すのに対して，それを元に戻す（恒等置換にする）移動は240°の回転（$=\sigma_5$）だからである．

S_3の部分集合が小さな群になっているものがある．例えば，表からσ_1とσ_2だけを取り出してみると，次のようになっている．これだけでも群の定義を満たしているので，これをS_3の**部分群**という．これを$H_1=\{\sigma_1,\sigma_2\}$としよう．

表-2

H_1	σ_1	σ_2
σ_1	σ_1	σ_2
σ_2	σ_2	σ_1

S_3の部分群は他にもあるのが表から容易にわかる．これらを，

$$H_2=\{\sigma_1,\sigma_3\},\quad H_3=\{\sigma_1,\sigma_6\}$$

とする．しかし，$\{\sigma_1,\sigma_4\}$や$\{\sigma_1,\sigma_5\}$は部分群ではない．積が閉じていないからである．

表-3

	σ_1	σ_4
σ_1	σ_1	σ_4
σ_4	σ_4	σ_5

表-4

	σ_1	σ_5
σ_1	σ_1	σ_5
σ_5	σ_5	σ_4

S_3の部分群にはもう一つ重要な部分群がある．それは$N=\{\sigma_1,\sigma_4,\sigma_5\}$である．

表-5

N	σ_1	σ_4	σ_5
σ_1	σ_1	σ_4	σ_5
σ_4	σ_4	σ_5	σ_1
σ_5	σ_5	σ_1	σ_4

他の部分群とNの違いを述べる前に，新しい記号表記を導入する．

一般的な群Gの部分集合Hの全ての元に対して，Gの任意の元σの左側からかけることによってできる集合（群になるとは限らない）を

$$\sigma H$$

で表すのである．これを「左**副群**」という．同様に右側からかけたものを$H\sigma$で表し，「右副群」という．左・右副群を単に副群ともいう．S_3での例を挙げると，部分群$H_2=\{\sigma_1,\sigma_3\}$に左から元$\sigma_4$をかけてできる集合は，$\sigma_4\sigma_1=\sigma_4$，$\sigma_4\sigma_2=\sigma_6$であるから，

$$\sigma_4 H_2=\{\sigma_4,\sigma_6\}$$

となる．同様に，$H_2\sigma_4=\{\sigma_4,\sigma_3\}$となる．この場合，$\sigma_4 H_2\neq H_2\sigma_4$である．

さて，部分群$N=\{\sigma_1,\sigma_4,\sigma_5\}$と他の$H_1$，$H_2$，$H_3$との違いは次の点にある．$N$は$S_3$の任意のの元$\sigma$に対して，

$$(1)\quad \sigma N=N\sigma\ ,$$

またはこの式の両辺の右側からσ^{-1}をかければ，$\sigma\sigma^{-1}=1$（恒等置換）であるから

$$(2)\quad \sigma N\sigma^{-1}=N$$

が成り立つのである．

（例：$\sigma_3 N=\{\sigma_3,\ \sigma_6,\ \sigma_2\}$，$N\sigma_3=\{\sigma_3,\ \sigma_2,\ \sigma_6\}$，$\therefore\quad \sigma_3 N=N\sigma_3$）．

(1)と(2)は同じ意味であるが，(2)の方がどちらかといえば使用頻度が高い．

σがNの元ならば当然であるが，S_3のどの元でも成り立つのである．このような性質を「**正則**」であるといい，正則な部分群を「**正規部分群**」という．もちろんガロアの発見による．正規部分群は正則拡大体と共にガロア理論の中で主役をなす概念である．

他に，恒等置換（単位元）σ_1だけからなる群$E=\{\sigma_1\}$やS_3自身も，S_3の部分群であるだけでなく，正規部分群でもある．EやS_3を，**自明な（正規）部分群**といい，Eは特に**単位群**ともいう．自明でない部分群を「**真の部分群**」ということもある．

これらS_3の各部分群の位数（元の個数）が，1個，2個，3個，6個というようにS_3の位数6の**約数**になっている．これは一般の群における重要な性質で「**ラグランジュの定理**」という．以下に証明を付す．

ガロアに先行するラグランジュは群という概念なしに不完全ながらこの定理を証明したそうである．

【定理６】群Gの部分群Hの位数はGの位数の約数である．（ラングランジュ）

【証明】

Gの位数をg，部分群Hの位数をhとする．Gの各元とHとの積（＝副群）を作ると，$\sigma_1 H$，$\sigma_2 H$,…等々g個の副群ができる．各副群はh個ずつの元を持つ．G_3の或る元σが副群$\sigma_a H$の元だとすると，$\sigma=\sigma_a\tau$となるHの元τがあるから$\sigma H=\sigma_a\tau H=\sigma_a H$．また，$\sigma$が$\sigma_a H$の元でなければ$\sigma H$の元はどれも$\sigma_a H$の元ではない．なぜなら$\sigma\tau$を$\sigma H$の元だとして$\sigma\tau=\sigma_a\tau'$と仮定すれば，これに$\tau$の逆元を右からかけて$\sigma\tau\tau^{-1}=\sigma_a\tau'\tau^{-1}$．よって$\sigma=\sigma_a\tau'\tau^{-1}$と

なって$\tau'\tau^{-1}\in H$であるから$\sigma\in\sigma_a H$となって矛盾する．これはつまりGの元がh個ずつの元を持ったg個の副群に，それぞれ全く同じかまたは一つも同じ元がないか，どちらかに分解されることになる．そこで互いに異なる副群の個数をj個とすれば，$g=hj$となって，hはgの約数となることが証明された．【証明終】

この証明の最後で，「Gの元がh個ずつの元を持ったg個の副群に，それぞれ全く同じかまたは一つも同じ元がないか，どちらかに分解される」なら$g=hj$となるのがイマイチわからない人のために（私もそうでした），三次対称群S_3とその部分群 H={1,(12)} で具体的に示そう．副群は，

A：1・H={1,(12)}，(12)H={(12),1}

B：(123)H={(123),(23)}，(23)H={(23),(123)}

C：(132)H={(132),(13)}，(13)H={(13),(132)}

の６つである．Aグループは，Hの元１と(12)をHにかけて作るもので，それはH自身である．それが２個できる．次にHの元でない(123)をHにかけてBグループを作る．すると(123)(12)=(23)であるから(23)Hと同じものになる．S_3で残っているのは(132)と(13)であるが，(132)Hの元(132)(12)は=(13)であるから同じCグループになる．以上で副群は３つのグループに分かれる．よって6=2×3.

副群の個数jのことを「HのGにおける**指数**」といい，$(G:H)$で表す.

また，H_1，H_2，H_3はそれぞれ元同士の積について交換法則が成り立っている．すなわちアーベル群である．位数が２である群はすべてアーベル群である．G_3の正規部分群Nは位数が３であるが，これもアーベル群である.

一般に，n個の「もの」の置換の全ては群を作る．この群を**n次対称群**といい，S_nで表す．S_nの位数は$n!=1\times2\times\cdots\times n$である．これまで見てきた$S_3$は**三次対称群**である．$S_3$は位数は$3!=6$，部分群は（自明なものも入れて）４個ある．ちなみに四次対称群S_4は位数は$4!=24$で，部分群は全部で30個ある.

S_nの部分集合が群であるとき，これを置換群と呼ぶ．S_nのnのが大きくなると部分群，つまり置換群の数は膨大なものになる.

7．体と群

体とか群などのような集合は，内部に「演算」と呼ばれる構造（代数的構造）を持っているので「代数系」と呼ばれる．ガロアはこの代数系の研究によってそれまでの方程式論を中心とした代数学に革命をもたらした．現在では，代数学とは代数系の数学理論のことを言う.

いよいよ体に群を適用することを考えよう.

ここで扱うのは**正則拡大体K/kの中での**部分体どうしによるk**同型対応**と，それを方程式の解の置換によって表現することである.

正則拡大体K/kの共役体を$L, L', \cdots$とするとき，ある共役体Lから他の共役体L'へのk同型対応が与えられると，LがL'に移り，L'もまた他の共役体に移る．しかしK自身は正則であるから集合としては変化しない．すなわち，共役体どうしのk同型対応はKそれ自身の内部での共役体の置換と考えることができる．これを正則拡大体の「k **自己同型対応**」（または**ガロア置換**）という．

正則拡大体Kのk自己同型対応は続けて行うことができる．結果は常に同じK自身である．このk自己同型対応を続けて行うことを，k自己同型対応の「**合成**」という．

例えば，前に$Q\left(\sqrt{2}\right)$が正則拡大体であることを述べたが，これはこの体が二次方程式$x^2-2=0$の２つの解$x=\pm\sqrt{2}$を生成元とする拡大体$Q\left(\sqrt{2}\right)$，$Q\left(-\sqrt{2}\right)$を２つとも含んでいるという意味であった．そのとき，体$Q\left(\sqrt{2}\right)$から体$Q\left(-\sqrt{2}\right)$へのQ **同型対応**を考えた．

$$a+b\sqrt{2}\to a+b\left(-\sqrt{2}\right)$$

という対応である．他にその逆のQ同型対応もある．さらに，$Q\left(\sqrt{2}\right)$はそれ自身の中に部分体としてQも持っており，QからQへのQ同型対応もある．だが，Qから$Q\left(\sqrt{2}\right)$へのQ同型対応はない．これは対応ではあるがQ同型とはいえない．

これらのQ同型対応を制御するために，正則拡大体$Q\left(\sqrt{2}\right)$のQ自己同型対応を定め，それによって部分体のQ同型対応を表すことにするのである．

方程式$x^2-2=0$の解は２個なので共役体も$Q\left(\sqrt{2}\right)$，$Q\left(-\sqrt{2}\right)$の２個である．よって，$Q\left(\sqrt{2}\right)$から$Q\left(\sqrt{2}\right)$自身へのQ同型対応をσ_1，$Q\left(\sqrt{2}\right)$から$Q\left(-\sqrt{2}\right)$へのQ同型対応をσ_2と定める．

$$\sigma_1 : Q\left(\sqrt{2}\right)\to Q\left(\sqrt{2}\right)$$

$$\sigma_2 : Q\left(\sqrt{2}\right)\to Q\left(-\sqrt{2}\right)$$

これはそのまま正則拡大体$Q\left(\sqrt{2}\right)$のQ自己同型対応となり，$Q\left(\sqrt{2}\right)$内での部分体の置換を引き起こす．σ_1は特に「**恒等写像**」と呼ばれ，$Q\left(\sqrt{2}\right)$全体ををそのまま自分自身に移すので，これによってその部分体である$Q\left(\sqrt{2}\right)$や$Q\left(-\sqrt{2}\right)$もそれぞれ自分自身に移る．また，これによって部分体QもQ自身に移る．

σ_2は$a+b\sqrt{2}\to a+b\left(-\sqrt{2}\right)=a-b\sqrt{2}$という$Q$同型対応を表しているから，$Q\left(\sqrt{2}\right)$を$Q\left(-\sqrt{2}\right)$に移し，逆に$Q\left(-\sqrt{2}\right)$は，$\sigma_2 : a-b\sqrt{2}\to a-b\left(-\sqrt{2}\right)=a+b\sqrt{2}$となって$Q\left(\sqrt{2}\right)$に移る．

さらに，$\sigma_2\sigma_2$を２回続けて行なうと，$Q\left(\sqrt{2}\right)$の元$a+b\sqrt{2}$は，

$$\sigma_2\sigma_2:\left\{a+b\sqrt{2}\to a-b\left(\sqrt{2}\right)\right\}\to a-b\left(-\sqrt{2}\right)=a+b\sqrt{2}$$

となって恒等写像σ_1を行なったのと同じことになる．ゆえに

$$\sigma_2\sigma_2=\sigma_1.$$

こうしてQ自己同型対応の集合$S_2=\left\{\sigma_1,\sigma_2\right\}$を作れば，$S_2$は$Q$自己同型対応の合成を演算として群となる．この$S_2$を方程式$x^2-2=0$の**ガロア群**という．群表は前述の「表-2」と同じものになる．

正則拡大体のQ自己同型対応を考えるには，方程式の解の置換が便利である．すなわち，S_2のσ_1は解$\sqrt{2}$は$\sqrt{2}$に（だから$-\sqrt{2}$は$-\sqrt{2}$に）置き換える，そしてσ_2は$\sqrt{2}$を$-\sqrt{2}$に（だから$-\sqrt{2}$は$-\left(-\sqrt{2}\right)=\sqrt{2}$に）置き換えることと考えるのである．よって，体から体へのQ同型対応が次のように解の置換に対応する．

$$\sigma_1:\sqrt{2}\to\sqrt{2}\,,\quad -\sqrt{2}\to-\sqrt{2}$$

$$\sigma_2:\sqrt{2}\to-\sqrt{2}\,,\quad -\sqrt{2}\to\sqrt{2}$$

すなわち，σ_1では$\sqrt{2}$も$-\sqrt{2}$も変わらない（恒等置換）が，σ_2では$\sqrt{2}$は$-\sqrt{2}$に，$-\sqrt{2}$は$-\left(-\sqrt{2}\right)=\sqrt{2}$に入れ替わる．こうすると$Q$同型対応をモノ（=解）の置換によって表現できるので，捉えやすくなる．すなわち，ガロア群を置換群によって表現できる．

さらにこれを次のように記号化する．まず，解$\sqrt{2}$を１で表し，解$-\sqrt{2}$を２で表す[8]と，σ_1は，$\begin{pmatrix}12\\12\end{pmatrix}$=1，$\sigma_2$は$\begin{pmatrix}12\\21\end{pmatrix}$=(12) で表せる．よってガロア群$S_2$は置換群となる（二次対称群でもある）．

$$S_2=\left\{1,(12)\right\}$$

ガロア群は，その母体となる正則拡大体の性質を強く反映するので，これを調べることでおおもとの方程式の可解性までをも解明することができるのである．「ガロア理論」とはこのガロア群の性質を知らべることに尽きるといっても過言ではない．

ガロア群の例を他にも見てみよう．

前に方程式 $x^3-2=0$ の解を３つとも含んだ正則拡大体を求めたが，それは基礎体を$k=Q(\omega)$とする$K=k(\theta)$いう三次の体であった（前述どおり$\theta=\sqrt[3]{2}$とする）．３つの共役体は，$k(\theta)$，$k(\theta\omega)$，$k\left(\theta\omega^2\right)$であった．この３つの共役体に基本となる同型対応を決定するのだが，今度は基礎体がQではなく$k=Q(\omega)$なのでk同型対応である．

$$\sigma_1:k(\theta)\to k(\theta)$$

---

[8] 1,2,3などでなく，a,b,cでも，イ,ロ,ハでも構わない．

$$\sigma_2 : k(\theta) \to k(\theta\omega)$$

$$\sigma_3 : k(\theta) \to k(\theta\omega^2)$$

例えば，$k(\theta\omega)$ から $k(\theta\omega^2)$ への k 同型対応とは，

$$a + b\theta\omega + c(\theta\omega)^2 \to a + b\theta\omega^2 + c(\theta\omega^2)^2 \quad (a,b,c \in k)$$

であるが，これは形としては「θ にかかっている ω が一つ増える」ことを意味しているので σ_2 になる．つまり体 $k(\theta\omega)$ に σ_2 を行なえば，$k(\theta\omega^2)$ に移るのである．

そしてこれら σ_1，σ_2，σ_3 も解の置換で表現することによって置換群として考えることができる．

$$\sigma_1 : \theta \to \theta$$

$$\sigma_2 : \theta \to \theta\omega$$

$$\sigma_3 : \theta \to \theta\omega^2$$

こうして $K = k(\theta)$ の k 自己同型対応を解の置換の集合，

$$N_3 = \{\sigma_1, \sigma_2, \sigma_3\}$$

によって表現できるようになった．すなわち，σ_1 は θ をそのままに（よって他の解も変わらない），σ_2 は θ を $\theta\omega$ に（ω を掛けるから $\theta\omega$ は $\theta\omega^2$ に，$\theta\omega^2$ は $\theta\omega^3 = \theta$ になる），σ_3 は θ を $\theta\omega^2$ に（ω^2 を掛けるから $\theta\omega$ は $\theta\omega^3 = \theta$ に，$\theta\omega^2$ は $\theta\omega^4 = \theta\omega$ になる）置き換える．ここでも解 θ を 1，$\theta\omega$ を 2，$\theta\omega^2$ を 3 と記号化することで，

$$\sigma_1 : 1 \to 1,\ 2 \to 2,\ 3 \to 3$$

$$\sigma_2 : 1 \to 2,\ 2 \to 3,\ 3 \to 1$$

$$\sigma_3 : 1 \to 3,\ 2 \to 1,\ 3 \to 2$$

よって置換の記号で

$$\therefore \sigma_1 = \begin{pmatrix} 123 \\ 123 \end{pmatrix} = 1,\quad \sigma_2 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = (123),\quad \sigma_3 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (132)$$

と表せる．$N_3 = \{\sigma_1, \sigma_2, \sigma_3\}$ は前に出てきた三次対称群の正規部分群と同じものである．群表は次の通り．

表-6

N_3	σ_1	σ_2	σ_3
σ_1	σ_1	σ_2	σ_3
σ_2	σ_2	σ_3	σ_1
σ_3	σ_3	σ_1	σ_2

ガロア群の例をもう一つ，次の方程式をあげる．

$$x^4-16x^2+4=0$$

これは基礎体Q上既約な四次方程式であるが，実は二次方程式が重なった**複二次式**の方程式なので高校数学でも解を求められる．$X=x^2$と置いて，

$$X^2-16X+4=0$$
$$X=8\pm2\sqrt{15}$$
$$\therefore x^2=8\pm2\sqrt{15}$$
$$\therefore x=\pm(\sqrt{5}\pm\sqrt{3})$$

よって四つの解は，

$$x=\sqrt{5}+\sqrt{3},\sqrt{5}-\sqrt{3},-\sqrt{5}+\sqrt{3},-\sqrt{5}-\sqrt{3}.$$

四つの解から共役体は$Q\left(\sqrt{5}+\sqrt{3}\right)$，$Q\left(\sqrt{5}-\sqrt{3}\right)$，$Q\left(-\sqrt{5}+\sqrt{3}\right)$，$Q\left(-\sqrt{5}-\sqrt{3}\right)$となるが，この中のどれでも一つ，例えば$Q\left(\sqrt{5}+\sqrt{3}\right)$を選べば，この体は以下のとおり他の解を全て四則計算で表せるので正則拡大体である．

$$\sqrt{5}-\sqrt{3}=\frac{2}{\sqrt{5}+\sqrt{3}},\quad -\sqrt{5}+\sqrt{3}=-\frac{2}{\sqrt{5}+\sqrt{3}},\quad -\sqrt{5}-\sqrt{3}=-\left(\sqrt{5}+\sqrt{3}\right)$$

$K=Q\left(\sqrt{5}+\sqrt{3}\right)$の$Q$に対する次数を求めよう．【定理３】によって$K$の元は，

$$a+b\left(\sqrt{5}+\sqrt{3}\right)+c\left(\sqrt{5}+\sqrt{3}\right)^2+d\left(\sqrt{5}+\sqrt{3}\right)^3,\quad (a,b,c,d\in Q)$$

で表されるが，これは展開して整理すると，

$$\begin{aligned}&a+b\left(\sqrt{5}+\sqrt{3}\right)+c\left(\sqrt{5}+\sqrt{3}\right)^2+d\left(\sqrt{5}+\sqrt{3}\right)^3\\&=(a+8c)+(b+18d)\sqrt{3}+(b+14d)\sqrt{5}+2c\sqrt{15}\\&=a'+b'\sqrt{3}+c'\sqrt{5}+d'\sqrt{15}\quad (a',b',c',d'\in Q)\end{aligned}$$

となるので，底として$\left\{1,\sqrt{3},\sqrt{5},\sqrt{15}\right\}$を取れるので次数は４となる．すなわち，$[K:Q]=4$．

正則拡大体$K=Q\left(\sqrt{5}+\sqrt{3}\right)$におけるガロア置換，すなわち$Q$自己同型対応は，以下のとおり．

$$\sigma_1:Q\left(\sqrt{5}+\sqrt{3}\right)\to Q\left(\sqrt{5}+\sqrt{3}\right)$$
$$\sigma_2:Q\left(\sqrt{5}+\sqrt{3}\right)\to Q\left(\sqrt{5}-\sqrt{3}\right)$$
$$\sigma_3:Q\left(\sqrt{5}+\sqrt{3}\right)\to Q\left(-\sqrt{5}+\sqrt{3}\right)$$
$$\sigma_4:Q\left(\sqrt{5}+\sqrt{3}\right)\to Q\left(-\sqrt{5}-\sqrt{3}\right)$$

これを解の置換として見てみよう．

σ_1は恒等置換，すなわちどの解も置き換わらない．

σ_2は$\sqrt{3}$の符号が変わるので，$\sqrt{5}-\sqrt{3}$は$\sqrt{5}+\sqrt{3}$に，$-\sqrt{5}+\sqrt{3}$は$-\sqrt{5}-\sqrt{3}$に，$-\sqrt{5}-\sqrt{3}$は$-\sqrt{5}+\sqrt{3}$に替わる．

σ_3は$\sqrt{5}$の符号が変わるので，$\sqrt{5}-\sqrt{3}$は$-\sqrt{5}-\sqrt{3}$に，$-\sqrt{5}+\sqrt{3}$は$\sqrt{5}+\sqrt{3}$に，$-\sqrt{5}-\sqrt{3}$は$\sqrt{5}-\sqrt{3}$に替わる．

σ_4は$\sqrt{5}$と$\sqrt{3}$の両方の符号が変わるので，$\sqrt{5}-\sqrt{3}$は$-\sqrt{5}+\sqrt{3}$に，$-\sqrt{5}+\sqrt{3}$は$\sqrt{5}-\sqrt{3}$に，$-\sqrt{5}-\sqrt{3}$は$\sqrt{5}+\sqrt{3}$に替わる．

よって，記号化により$\sqrt{5}+\sqrt{3}$を１，$\sqrt{5}-\sqrt{3}$を２，$-\sqrt{5}+\sqrt{3}$を３，$-\sqrt{5}-\sqrt{3}$を４とすれば，

$$\sigma_1=\begin{pmatrix}1234\\1234\end{pmatrix},\ \sigma_2=\begin{pmatrix}1234\\2143\end{pmatrix},\ \sigma_3=\begin{pmatrix}1234\\3412\end{pmatrix},\ \sigma_4=\begin{pmatrix}1234\\4321\end{pmatrix}$$

となる．そして集合$V_4=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$は群となる．

σ_1は恒等置換１でよいが，σ_2は1と２，3と4がそれぞれ独立して巡回しているのでこの場合は二つの互換の積で表され，σ_2=(12)(34)と表記される．同様にσ_3=(13)(24)，σ_4=(14)(23)となる．

一般に，どの置換も互換の積に分解できる（分解の仕方は一通りとは限らない）．

(123)=(12)(13)=(13)(23)，(132)=(13)(12)，(1234)=(12)(13)(14)，…

この時に偶数個の互換から成る置換を**偶置換**という．そして奇数個から成る場合は**奇置換**という．(123)や(132)は偶置換，(12)や(1234)は奇置換である．一般に長さmの置換は$m-1$が偶数か奇数かで偶・奇置換が判断できる．また，恒等置換１は偶置換とする．

よって，

$$V_4=\{1,(12)(34),(13)(24),(14)(23)\}$$

と表される．これは「**クラインの四元群**」と言われる特別な群で，群表は次の通り．今見たようにクラインの四元群は４つの偶置換から成っている．これはアーベル群である（アーベル群の群表は対角線に対して対称となるのが特徴）．

表-7

V_4	1	(12)(34)	(13)(24)	(14)(23)
1	1	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	1	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	1	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	1

方程式$x^4-16x^2+4=0$のガロア群はクラインの４元群である．

今，体$Q\left(\sqrt{5}+\sqrt{3}\right)$から他の共役体への$Q$自己同型対応をガロア置換としたが，これをどの体から行っても結果は同じとなるのは当然である．

一般に，方程式のガロア体（正則拡大体）における一つひとつのガロア置換に対して方程式の解のある置換が対応する．ただし，この逆は成り立たない．すべての解の置換に対応するガロア

置換があるとは限らない．ある方程式のガロア群がどういう群になるかはそれぞれの方程式の個性に依るものであり，一般的に論じることは困難である．

８．「基本定理」の証明

正則拡大体K/kが単純拡大体$K=k(\alpha)$である場合には，K/kの任意のガロア置換σは生成元αをその共役数に移し，その係数（＝kの元）は変えない．言い換えればσはKの部分体$k(\alpha)$をその共役体$k(\alpha')$に移すのである．K/kのガロア群Gは，$k(\alpha)$の共役体$k(\alpha')$の個数分だけのk同型対応から成る．

しかし，K/kの中間体L（$K\supset L\supset k$，$K\neq L, L\neq k$）がある場合には，ガロア群GはK/kに対してやや複雑な振る舞いをする．Lがkにない要素α（＝生成元）を持つように，KもLの拡大体であるからLにない要素βを持っている．これらの要素には，Gの元はそれを変えたり変えなかったりするのである．

正則拡大体K/kは，基礎体k**<u>の上に</u>**$k(\alpha)$を重ね，さらに**<u>その上に</u>**$L(\beta)$を重ねて作られる．

「Bの上にA」という場合は$B\subset A$を表すものとする．「Bの下にA」なら$B\supset A$である．以下同様.

（方程式の）基礎体kに対して，$L=k(\alpha)$，αの共役数を$\alpha=\alpha_1,\alpha_2,\cdots,\alpha_m$とすると，$L=k(\alpha)$からその共役体$k(\alpha_1),k(\alpha_2),\cdots$への$k$同型対応が$m$個存在する．

次に，Lを基礎体とする$K=L(\beta)$，βの共役数を$\beta=\beta_1,\beta_2,\cdots,\beta_n$とすると，$L(\beta)$からその共役体$L(\beta_1),L(\beta_2),\cdots$への$L$同型対応が$n$個存在する．

ところが，ガロア群Gは，下から積み上げられてくるのではなく，逆に一番上の正則拡大体K/kに対して初めて完成した形で現わされ，そこから**下に**降りながらその部分群によって中間体を反映していくのである．まず，Kとすぐ下の部分体Lとの関係がガロア群Gの部分群によって捉えられることを示す.

【定理５】よりK/kの次数は$[K:k]=[K:L][L:k]$であるから$[K:L]=m$，$[L:k]=n$とすれば，$[K:k]=mn$．Gの位数は体の次数に等しいので，$|G|=mn$である．

このmn個のk自己同型対応（ガロア置換）を$\sigma_{ij}(1\le i\le m, 1\le j\le n)$とするとき，$\sigma_{ij}$は$\alpha$をその共役数$\alpha_i$に移し，$\beta$をその共役数$\beta_j$に移す.

これによれば，Gの中にはLの元を変えないようなガロア置換がm個ある．その全部をHとすれば，$H=\{\sigma_{i1} \mid \sigma_{i1}\in G, 1\le i\le m)\}$である．$L$にこのガロア置換$\sigma_{i1}$を行なえば，それは$L$の共役体に移るが，その結果がまた$K$となるのは$K/k$が正則であることから当然である．ゆえに体$K/L$もまた正則拡大体であり，$K$の$L$同型対応は$K/L$の$L$自己同型対応（ガロア置換）である．そのガロア群が$H$となる．すなわち$H$は$G$の部分群である．

G から H を除いた残りのガロア置換はもちろん K/k の k 自己同型対応ではあるが，恒等置換を持たないので群にはならない．

ここでガロア理論の「基本定理」を再掲し，いよいよその証明を試みる．

これまで体と群について述べてきたことから，この定理の重大性が理解されてきたのではないだろうか．正則拡大体に対してそのガロア群が存在し，それが正則拡大体の性質を反映するのである．例えば正則拡大体の中間体の数を把握することはかなり困難であるが，ガロア群の部分群は直ちに求められる．そして基本定理によって中間体と部分群が 1 対 1 に対応するのであれば，中間体の数＝部分群の数ということになる．その他にも様々な体の性質をガロア群から得ることができるのである．

【定理1】(ガロア理論の基本定理)　K を k の正則拡大体，G をそのガロア群とする．K/k の中間体と G の部分群は1対1に対応し，相対応する中間体の次数と部分群の位数は等しい．

【証明】

基本定理の証明は二段に分かれる．最初に中間体に対応する部分群が決定され，次に部分群に対応する中間体が決定される．この両者が一致することで 1 対 1 の対応が証明される．

〔第一段〕

正則拡大体 K/k の任意の中間体を L とする．この L の元を全く動かさないような G の元が存在し，これらの全ては G の部分群となるからこれを H とする．

この H が体 K/L のガロア群となることはこの章の初めに述べた．

一方，H のどの元によっても全く動かない K の元の集合を L' とすれば，$L \subset L'$ が成り立つ（なぜなら H の元によって動かない K の元が L の元以外にもあるかも知れないから）．

次に，H のどの元によっても動かないものは L の元以外にはないことを示す．L' の任意の元を α とする．$\alpha \in L'$ であるから α は H のどの元によっても動くことのない K の元である．もしこの α が L の元でないならば，α によって拡大体 $L(\alpha)$ が生成され，$L(\alpha)$ から他の共役体への（恒等写像でない）L 同型対応（$=H$ の元）が存在することになる．つまり α が他の共役数に「移る」（＝動く）ことになる．これは α が L' の元であることと矛盾する．よって $\alpha \in L$．「$\alpha \in L'$ ならば $\alpha \in L$」より $L' \subset L$ となる．$L \subset L'$ と合わせて $L = L'$．以上で K/k の任意の中間体 L に対応する H が決定された．

〔第二段〕（以下では第一段と混同しないよう H と L の字体を変えてある．）

K の元で，〔第一段〕で決定された H に含まれるどのガロア置換によっても動かないものの全てを L とすれば，この章の初めに述べたように L は K/k の中間体となる．一方，今度はこの L を動かさないような G の元の全てを H′ とすれば H ⊂ H′ である（なぜなら H′ は H の元以外にも L を動かさないような G の元を持っているかもしれないから）．すなわち H は H′ の部分群である．

次に，この章の初めに述べたように，H′ は体 $K/$L のガロア群であり，その位数を h' とすれば，$h' = [K : \mathrm{L}]$ である．h' は $K/$L 上の既約多項式の次数でもある．

さて，K はL の上の体であるから，$K=\mathrm{L}(\gamma)$ となる生成元γ が存在する．ゆえに，H の位数をh とすれば，γ を解とする基礎体k 上のh 次代数方程式$f(x)=0$ が存在する．$f(x)=0$ はh 個の解$x=\gamma_1,\gamma_2,\cdots,\gamma_h$ を持つから（定理２），この左辺の多項式$f(x)$ を因数分解すると，

$$f(x)=(x-\gamma_1)(x-\gamma_2)\cdots(x-\gamma_h)$$

となる．さらにこれを展開すると，

$$f(x)=x^h-A_1x^{h-1}+A_2x^{h-2}-\cdots+(-1)^hA_h$$

となる．ここで$A_1,A_2,\cdots,A_h$ は解と係数の関係から$\gamma_1,\gamma_2,\cdots,\gamma_h$ の対称式になる[9]．

この展開式にH の任意の元（ガロア置換）を適用すると解$x=\gamma_1,\gamma_2,\cdots,\gamma_h$ にある置換が起きる．しかし$\gamma_1,\gamma_2,\cdots,\gamma_h$ は互いに入れ替わるだけなので，対称式である$A_1,A_2,\cdots,A_h$ は何ら変わらない．このことはγ の多項式$f(\gamma_i)$（$i=1,2,\cdots,h$）の係数がH の任意の元によっては動かないことを示す．つまり，$f(\gamma_i)$ の係数はL の元である．ゆえに$f(\gamma_i)$ はK/k の元であるだけでなく，K/L の元でもある．しかし「既約」多項式であるかは不明なので，K/L の次数$[K:\mathrm{L}]=h'$ に対しては$h\geq h'$ となる．一方，$\mathrm{H}\subset\mathrm{H}'$ であったから$h\leq h'$．よって，$h=h'$ となり，H=H′ が決定された．

以上の議論によって，K/k の中間体L とガロア群G の部分群の間に互いにただ一つの対応をつけることができる．【証明終】

基本定理の意味における中間体と部分群の対応を「**ガロアの対応**」と（ガロア対応とも）いう．

この例証として，方程式$x^4-16x^2+4=0$ のガロア体$K=Q\left(\sqrt{5}+\sqrt{3}\right)$ を取り上げる．

この体のガロア群はクラインの四元群$V_4=\{1,(12)(34),(13)(24),(14)(23)\}$ であった．V_4 の部分群は以下の５つである．

$E=\{1\}$　単位群

$H_1=\{1,(12)(34)\}$

$H_2=\{1,(13)(24)\}$

$H_3=\{1,(14)(23)\}$

V_4 自身

ここで，1,2,3,4とは方程式の解$\sqrt{5}+\sqrt{3}$，$\sqrt{5}-\sqrt{3}$，$-\sqrt{5}+\sqrt{3}$，$-\sqrt{5}-\sqrt{3}$ を指す．

E とV_4 は後にして，まずH_1 に基本定理の意味で対応するV_4 の中間体を特定しよう．ガロアの対応によれば，「V_4 の部分群の元であるk 自己同型対応（=解の置換）によってまったく変化しないK の元が作る集合が中間体として対応する」のであるから，まずH_1 の元１は恒等置換なのでK の元の全てが対応する．次のH_1 の元 (12)(34) とは，1と2が入れ替わり，3と4が入れ替わるこ

---

[9] 対称式については【付録４】を参照．

とであるから，$\sqrt{5}+\sqrt{3}$ は $\sqrt{5}-\sqrt{3}$ と，$-\sqrt{5}+\sqrt{3}$ は $-\sqrt{5}-\sqrt{3}$ と入れ替わることである．この置換は「$\sqrt{3}$ の符号が変わる」ことを示している．言い換えれば $\sqrt{5}$ の符号は変わらないのだから，もしこの体に $\sqrt{5}$ が含まれていれば，$a+b\sqrt{5}$ （$a,b,\in Q$）から成る体は置換 (12)(23) によって変わらない中間体といえるだろう．そして $\sqrt{5}$ は，

$$\sqrt{5}=\frac{\left(\sqrt{5}+\sqrt{3}\right)+\left(\sqrt{5}-\sqrt{3}\right)}{2}$$

であるから，K の元である．よって H_1 の二つの元 1，(12)(34)によって変わらない K の元，言い換えれば，H_1 にガロア対応する中間体は $Q\left(\sqrt{5}\right)$ である．

同様にして（以下では恒等置換 1 については省略する），部分群 $H_2=\{1,(13)(24)\}$ の元 (13)(24) では，$\sqrt{5}+\sqrt{3}$ と $-\sqrt{5}+\sqrt{3}$，$\sqrt{5}-\sqrt{3}$ と $-\sqrt{5}-\sqrt{3}$ が入れ替わっているが，これは「$\sqrt{5}$ の符号が変わる」だけで，$\sqrt{3}$ は変わらない．よって $a+b\sqrt{3}$ が予想され，実際，

$$\sqrt{3}=\frac{\left(\sqrt{5}+\sqrt{3}\right)-\left(\sqrt{5}-\sqrt{3}\right)}{2}$$

により，$\sqrt{3}\in K$ であるので，H_2 にガロア対応する中間体は $Q\left(\sqrt{3}\right)$ である．

次に，$H_3=\{1,(14)(23)\}$ を考える．置換 (14)(23) では $\sqrt{5}+\sqrt{3}$ と $-\sqrt{5}-\sqrt{3}$，$-\sqrt{5}+\sqrt{3}$ と $\sqrt{5}-\sqrt{3}$ が入れ替わる．$\sqrt{5}$ と $\sqrt{3}$ の両方の符号が変わっているが，$K=Q\left(\sqrt{5}+\sqrt{3}\right)$ の底は $\left\{1,\sqrt{3},\sqrt{5},\sqrt{15}\right\}$ であることを見て[10]，$\sqrt{15}$ は $\sqrt{5}\times\sqrt{3}$ によって作られる元なので，$\sqrt{5}$ と $\sqrt{3}$ の両方の符号が同時に変われば $\sqrt{15}$ の符号は変化しないことがわかる．よって H_3 にガロア対応する中間体は $Q\left(\sqrt{15}\right)$ である．もちろん，

$$\sqrt{15}=\frac{1}{2}\left(\sqrt{5}+\sqrt{3}\right)^2-4$$

であるから，$\sqrt{15}\in K$．

このように，多少技巧的ではあるが，ガロア群は $K=Q\left(\sqrt{5}+\sqrt{3}\right)$ に「埋もれて」いる体を見つけ出すことにも効果を発揮する．

最後に，K 自身を動かさないようなガロア対応の部分群は，単位群 E であり．また，V_4 自身にガロア対応する中間体は，全てのガロア対応によっても変わらない体であるから，基礎体 Q である．

以上から，$K=Q\left(\sqrt{5}+\sqrt{3}\right)$ には K や Q も含めて５つの部分体があることがわかる[11]．

---

[10] 21ページ参照．

[11] ガロア体が$Q(\sqrt{5}+\sqrt{3})$ではなく，$Q(\sqrt{5},\sqrt{3})$なら部分体$Q(\sqrt{5}),Q(\sqrt{3}),Q(\sqrt{15})$等は自明である．

８．二項方程式と巡回群

「基本定理」によって方程式の正則拡大体とそのガロア群との関係が確立した．次はガロア理論の最初の精華である方程式の代数的可解性の解明に議論が移るのであるが，その準備として前にも掲示した二項方程式をより一般的に取り上げ，そのガロア群を求める．

一般的な二項方程式は，

$$x^p - a = 0$$

で表されるが，ここでは p を素数，a を複素数とする．この方程式の解 $\alpha_1,\alpha_2,\cdots,\alpha_n$ は形式的に，

$$(1)\quad \alpha_i = \zeta^{i-1}\sqrt[p]{a} \quad (i=1,2,\cdots,n)$$

と表される[12]．$\sqrt[p]{a}$ は a の p 乗根のうちの一つを表す．また，ζ（ゼータ：ギリシア小文字）は，方程式 $x^p-1=0$ の解のうち，１でないもの一つを表す．$p=3$ のときには特に ω で表される．p がもし合成数４や６ならば，$x^p-1=0$ は有理数体上可約（因数分解可能）になり，p 乗する前に１になってしまうので，解の全てを(1)の形に表すことができない．ゆえに p は素数に限っておく．

このように，二項方程式の（形式的な）解法には１の虚数 p 乗根が必須なので，その都度基礎体に含めることが必要である．すなわち，

【定義２】（代数的解法）方程式の代数的解法では，係数等に対する四則計算と累乗根のみを用いる．その場合，必要に応じて１の累乗根を基礎体に含むものとする．

この定義における累乗根とは，二項方程式を解くことに他ならない．言い換えれば，代数的解法とは，四則計算と二項方程式を解くことの積み重ねということになる．

二項方程式の解で特徴的なのは，どの解でもそれに１の p 乗根 ζ（p は素数）を次々に乗じていくことで他の解全てを表現できるということである．

$$\alpha_2=\zeta\alpha_1,\ \ \alpha_3=\zeta\alpha_2,\ \ \cdots,\ \ \alpha_n=\zeta\alpha_{n-1},$$

$$\text{または，}\ \alpha_2=\zeta\alpha_1,\ \ \alpha_3=\zeta^2\alpha_1,\ \ \cdots,\ \ \alpha_n=\zeta^{n-1}\alpha_1.$$

このことはガロア群に如実に反映する．

二項方程式の解が $\alpha_i=\zeta^{i-1}\sqrt[p]{a}\ (i=1,2,\cdots,n)$ であれば，そのガロア置換は次のようになる．

$$\sigma_1:\sqrt[p]{a}\to\sqrt[p]{a}\ \text{（恒等置換）}$$

$$\sigma_2:\sqrt[p]{a}\to\zeta\sqrt[p]{a}$$

$$\sigma_3:\sqrt[p]{a}\to\zeta^2\sqrt[p]{a}$$

$$\vdots$$

---

12) 二項方程式は代数的に $A+Bi$（A,B は実数）の形にまで求めることが可能であるが，ここではふれない．

$$\sigma_p : \sqrt[p]{a} \to \zeta^{p-1}\sqrt[p]{a}$$

もちろん，$\sigma_1,\sigma_2,\cdots,\sigma_p$ の集まりはガロア群を形成する．これを $J=\left\{\sigma_1,\sigma_2,\cdots,\sigma_p\right\}$ とする．

ここで，σ_i とは ζ^{i-1} をかけることだから，$\sigma_i\sigma_i$ は ζ^{i-1} を２回かけることになる．$\sigma_i\sigma_i$ を指数のように σ_i^2 と表すことにすれば，一般に σ_i^n とは ζ^{i-1} を p 回かけることであり，

$\left(\zeta^{i-1}\right)^p=\left(\zeta^p\right)^{i-1}=1^{i-1}=1$ となるから結局（数の）１をかけることになる．すなわち，どの置換も p 回行うと恒等置換になるのである．σ_i でいうと，$\sigma_i{}^p=\sigma_1$ ということである．

$J=\left\{\sigma_1,\sigma_2,\cdots,\sigma_p\right\}$ で，例えば σ_2 を基にすると，

$$\sigma_3=\sigma_2{}^2,\sigma_4=\sigma_2{}^3,\cdots,\sigma_p=\sigma_2{}^{p-1}$$

となって，他の全ての元を σ_2 の累乗で表すことができる．

一般に，群 G のすべての元がある特定の元（**生成元**という）の累乗で表されるとき，G を**巡回群**という．正則拡大体 K/k のガロア群 G が巡回群となるとき，K/k を**巡回体**という．

次数が素数である二項方程式のガロア群 J は巡回群である．巡回群のいちばんの特徴はアーベル群となることである．なぜなら，$\sigma,\tau\in J$，生成元を $\sigma_0\in J$ とすると，$\sigma=\sigma_0^m,\tau=\sigma_0^n$ とおけるから，

$$\sigma\tau=\sigma_0^m\sigma_0^n=\sigma_0^{m+n}=\sigma_0^{n+m}=\sigma_0^n\sigma_0^m=\tau\sigma\ .$$

後に方程式の代数的可解性の問題に関係のある定理をここで証明しておく．

【定理７】巡回群の部分群は巡回群である．

【証明】

巡回群を G，その生成元を σ_0 とすれば，部分群 H の元の全てを，

$$\sigma_0{}^p,\ \sigma_0{}^q,\ \cdots,\ \sigma_0{}^r$$

で表すことができる．このとき，σ^0 は単位元とし，負の指数 σ^{-i} は $\sigma^{-i}=\left(\sigma^{-1}\right)^i$ のことと定めれば，この指数の組 $p,q,\cdots,r$ は，本来どんな整数にもなりうるのであるが，もし位数 n よりも大きかったり負数であれば，n で割った時の余りで表すことで，全ての指数の範囲を $0\le p,q,\cdots,r<n$ とすることができる．

例えば σ^{100} なら，$100=pn+r\ (0\le r<n)$ となる p,r により，$\sigma^{100}=\sigma^{pn+r}=(\sigma^p)^n\cdot\sigma^r=\sigma^r$ とすることができる．

$p,q,\cdots,r$ の中の最小のものを仮に p とすれば（他のものでも同様），その元を $\sigma=\sigma_0{}^p$ と表す．そして，他の指数は $p+x$ で表すことができる（文字は全て非負の整数）．

$$p=p+0,\quad q=p+q'\cdots,\quad r=p+r'$$

こうすれば，H の元 $\sigma_0{}^p,\sigma_0{}^q,\cdots,\sigma_0{}^r$ の全てを，σ の累乗で表すことができる．

$$\sigma_0{}^p=\sigma,\quad \sigma_0{}^q=\sigma^{p+q'}=\left(\sigma^p\right)^{q'}=\sigma^{q'},\quad \cdots,\quad \sigma_0{}^r=\sigma^{p+r'}=\left(\sigma^p\right)^{r'}=\sigma^{r'}$$

すなわち，巡回群Gの部分群Hは$\sigma=\sigma_0{}^p$を生成元とする巡回群である．【証明終】

例として，$x^5-a=0$のガロア群$J_5=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5\}$の群表を掲げておく．表はアーベル群の特徴として対角線に対して対称である．

下の表で，例えば$\sigma_3\sigma_4$とは1の5乗根ζを2回，続けて3回かけることだから結局5回かけることになり，従って5乗することだからそれは恒等置換に等しいのでσ_1となる．

表-8-1

	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5
σ_2	σ_2	σ_3	σ_4	σ_5	σ_1
σ_3	σ_3	σ_4	σ_5	σ_1	σ_2
σ_4	σ_4	σ_5	σ_1	σ_2	σ_3
σ_5	σ_5	σ_1	σ_2	σ_3	σ_4

9．剰余群と可解群

ここで，ガロア理論の第二の「基本定理」とでもいうべき重要な定理を証明する．

【定理8】K/kを正則拡大体，$G=G(K/k)$をそのガロア群とする．Kの中間体Lがkに対して正則であるとき，Lにガロア対応するGの部分群HはGの正規部分群である．

【証明】

Gの元で，Lを共役体L'に写すガロア置換をσとする．σによってLの任意の元αがα'に写ったとするとき，α'はL'の元となる．

$$(1)\quad \sigma:\alpha\to\alpha'$$

次に，基本定理により，Lにガロア対応するGの部分群Hがただ一つある．Hに対して置換の集合$\sigma^{-1}H\sigma$を考え，$\sigma^{-1}H\sigma=H$を示せば，Hが正規部分群となることが示される[13)]．

Hの任意の置換をτとし，置換の結合式$\sigma^{-1}\tau\sigma$を考え，これによってL'の元α'が動かないことを示す．仮にα'がβに写ったとすると，

$$(2)\quad \sigma^{-1}\tau\sigma:\alpha'\to\beta$$

と表せる．これをαから見れば，まず(1)のσによってα'に写り，次に(2)の$\sigma^{-1}\tau\sigma$によってβに写ったことになるから，σと$\sigma^{-1}\tau\sigma$の積$\sigma(\sigma^{-1}\tau\sigma)$を考え，これによって$\alpha$が$\beta$に写ったいうことにしてみよう．すなわち，

$$\sigma(\sigma^{-1}\tau\sigma):\alpha\to\beta$$

---

13) 15ページ参照.

となる．ここで，$\sigma\left(\sigma^{-1}\tau\sigma\right)=\left(\sigma\sigma^{-1}\right)(\tau\sigma)=\tau\sigma$ であるから結局は $\tau\sigma:\alpha\to\beta$．

ところで$\tau\sigma$ とはτ の後でσ をすることであるから，まずτ によってはα はα のまま，次のσ でα はα' に写る．すなわち，β とはα' のことである．$\tau\sigma:\alpha\to\alpha'$．

つまり，置換$\sigma\left(\sigma^{-1}\tau\sigma\right)$ とはσ で写ったα' をα' に写す，言い換えれば，$\sigma^{-1}\tau\sigma$ はα' を動かさないのである．ということは，L' の元α' は$\sigma^{-1}\tau\sigma$ によっては動かないのであるから，$\sigma^{-1}\tau\sigma$ の集まり$\sigma^{-1}H\sigma$ はL' のガロア群となる．一方，L は正則であるから$L=L'$．よって基本定理により$\sigma^{-1}H\sigma=H$．よってH は正規部分群である．【証明終】

ガロア理論の基本定理と上の【定理８】によって，正則拡大体とそのガロア群におけるガロアの対応では，正則拡大体には正規部分群が対応し，その逆も成り立つことになった．

以下では，この二つの定理を武器に方程式の代数的解法をガロア理論の立場から見てみることにしよう．そのため新たな記号として「**正則拡大体K/k のガロア群G**」を$G\left(K/k\right)$ と表すことにする．

基礎体Q 上のn 次既約方程式 $f(x)=0$ が代数的解法の過程を経て**解けたものと仮定**し，その時のガロア群を調べよう．以下では**式の見やすさのために**累乗根を３回追加して解が得られたと仮定する．

すなわち，有理数体Q に素数[14] p 乗根$\sqrt[p]{r}$ を追加して拡大体を作り（このとき１の虚数p 乗根ζ_p をQ に追加して基礎体を$k_0=Q\left(\zeta_p\right)$ とする．以下同様），$k_1=k_0\left(\sqrt[p]{r}\right)$ を得る．さらにk_1 にk_1 の中の或る数s のq 乗根$\sqrt[q]{s}$ をk_1 に追加して拡大体$k_2=k_1\left(\sqrt[q]{s}\right)$ を形成し，そしてk_2 にその中のある数t のr 乗根$\sqrt[r]{t}$ を追加して$K=k_2\left(\sqrt[r]{t}\right)$ を形成したとき，方程式のすべての解が得られたとするのである（基礎体は$k_0=Q\left(\zeta_p,\zeta_q,\zeta_r\right)$ になっている）．このとき体の次数の関係は，

$$\left[k_1:k_0\right]\left[k_2:k_1\right]\left[K:k_2\right]=p\times q\times r=pqr=\left[K:k_0\right]$$

となる．（注意：k_0 のQ に対する次数は含まれていない）

上述の解法の過程を進めた結果，K は基礎体k_0 に３つの累乗根を追加しているが，k_0 が１の累乗根を持っていることでk_0 に対して正則である．よってガロア群$G=G\left(K/k_0\right)$ が確定する．このとき各部分中間体の包含関係と体の次数，

$$(1)\qquad k_0\subset k_1\subset k_2\subset K$$
$$p\times\ \ q\ \times r\qquad\text{（体の次数）}$$

に対して，基本定理の意味で対応するG の正規部分群の列とその位数が対応する．正則拡大体に正規部分群が対応するため包含関係は逆向きとなる．

---

14) 素数の累乗根でないとガロア群が巡回群にならない．合成数の累乗根，例えば６乗根を追加したいときは，まず２乗根を追加してからさらに３乗根を追加する．

(2)　　$G \supset H_1 \supset H_2 \supset E$.

pqr　qr　r　　1　　（群の位数）

k_1 の k_0 に対する次数が p なので，最初のガロア群 $G_1(k_1/k_0)$ の位数は p，k_2 の k_1 に対する次数が q なので，次のガロア群 $G_2(k_2/k_1)$ の位数は q，K の k_2 に対する次数が r なので，ガロア群 $G_3(K/k_2)$ の位数は r，p,q,r は素数という前提なのですべて巡回群になる．

K の k_0 に対する次数は pqr なので，ガロア群 $G=G(K/k_0)$ の位数は pqr である．

一般に，群の包含関係 $G \supset H_1 \supset H_2 \supset \cdots \supset E$ で，中間の部分群がひとつ前の部分群の正規部分群になっているとき，これを「**群の正規列**」という．群の正規列は一通りとは限らない（例えば $G \supset E$ もひとつの正規列）．また，中間の部分群は一つ上の部分群の正規部分群でなければならないが，一番大きい G の正規部分群である必要はない．

すなわち，代数的に解ける方程式のガロア群は次の性質を持つ．

（1）方程式に付随するガロア体 K/k_0 にはガロア群 $G=G(K/k_0)$ が対応し，各部分中間体の包含関係の列にガロア群の正規列が（逆の包含関係で）対応する．

（2）ガロア体の各部分中間体 k_1/k_0，k_2/k_1，K/k_2 は二項方程式の解が（1の虚数累乗根とともに）追加されるので巡回体であり，その各ガロア群 $G_1(k_1/k_0),G_2(k_2/k_1),G_3(K/k_2)$ はいずれも巡回群である．

以上の**（1），（2）**の条件を満たすガロア群が「可解群」なのだが，条件**（2）**の３つのガロア群 $G_1(k_1/k_0)$，$G_2(k_2/k_1)$，$G_3(K/k_2)$ はガロア群 $G=G(K/k_0)$ とは別の群である．とはいえ，G と密接な関係があるのでこれを G 及びその部分群で表すことができれば，可解群を方程式論と切り離しても定義することが可能になる．それが「**剰余群**」（**因子群**，**商群**ともいう）である．そのヒントは群の位数にある．

まず，中間体 k_2 にガロア対応する部分群 H_2 とは，K の k_2 に対するガロア群であったので，その位数は r である．つまり，ガロア群 $G_3(K/k_2)$ とは部分群 H_1 のことで，位数は r である．

問題は次の $G_2(k_2/k_1)$ である．この群の位数は q でなければならないが，上記の群の包含関係を表す式②には位数 r の部分群はない．が，H_1 の位数 qr を H_2 の位数 r で割れば q になる．

ここで思い出されるのが「ラグランジュの定理」である．

ラグランジュの定理の証明で，群をその部分群を使って副群に分解することを用いたが，その副群の個数は親の群の位数を部分群の位数で割った値であった（これを指数といった）．つまり H_1 をその部分群 H_2 を使って副群に分けるならば，その個数が今必要な q になるのだから，ここで**副群どうしの積**を定義して新たな群を形成しようというのが剰余群の考え方である．

その考えに則って，群の部分集合 A，B の「積」を定義しよう．**A のそれぞれの元に B の全ての元をかけたものの集合を AB で表す**のである．集合であるから，もし同じものが出てきてもそれは一個とみなす．

例えば，三次対称群 S_3={1,(123),(132),(12),(13),(23)} の部分集合 A={(123),(13)} と B={(12),(23)} との積 AB とは，(123)(12)=(23)，(123)(23)=(13)，(13)(12)=(132)，(13)((23)=(123)より，AB={(23),(13),(132),(123)} となる．なお，BA={(13),(123),(12),(132)} なので，当然ながら AB≠BA.

この副群同士の積を使って新たな群を作るには，部分群は正規部分群でなくてはならない．例として，三次対称群S_3の正規部分群$N=\{1,(123),(132)\}$を使って剰余群を実際に作ってみよう．

まず，S_3を副群に分解すると，

$$1\cdot N=N,\ (123)N=N,\ (132)N=N,$$

$$(12)N=\{(12),(13),(23)\},\ (13)N=\{(13),(23),(12)\},\ (23)N=\{(23),(12),(13)\}$$

であるから，２種類の副群ができた．一つはNでよいが，もう一つを$A=\{(12),(13),(23)\}$としよう．この二つの副群で副群同士の積を行なうと，$NN=N$，$NA=A$，$AN=A$，$AA=N$ となる．

最後の AA=N はAA={(12),(13),(23)}・{(12),(13),(23)}であるから，

AA={1,(123),(132),(132),1,(123),(123),(132),1}={1,(123),(132)}=N

となる．

群表を作るまでもなく集合$\{N,A\}$は副群同士の積を演算として群を作る．単位元はN，$A^{-1}=A$である．これをS_3**の**N**による剰余群**といい，S_3/Nで表す（割り算の記号を援用している？）．剰余群S_3/Nの位数はS_3の位数をNの位数で割ったもの，つまりは副群の個数であるからNのS_3における指数$(S_3:N)=2$となる．

剰余群の条件は，群の正規列さえ前提すればいいので，方程式とは関係なしに定義される．すなわち可解群は一般には次のように定義される．

【定義３】群の正規列で，剰余群が全て巡回群であるものを可解列といい，可解列が一つでも可能な群を可解群という[15]**.**

可解群をこのように定義すれば，いろいろな群をあらかじめ可解群であるかどうかを調べておくことで，方程式の可解性をかなり一般的に論じることができるようになる．

さて，剰余群を定義したからには，話を方程式の解法に戻そう．

前の可解群の条件**（２）**によれば，ガロア体の各部分中間体k_1/k_0，k_2/k_1，K/k_2に対応するそれぞれのガロア群$G_1(k_1/k_0),G_2(k_2/k_1),G_3(K/k_2)$はいずれも巡回群でなければならないのだから，次の問題は対応する各剰余群，G/H_1，H_1/H_2，H_2/Eがこれらと「同じ」群であるかということが問題になる．

今までも，三角形の対称移動から三次対称群を見出したり，ものの置き換え（123の並べ替えなど）から置換群を提示してきたが，それらが全て群としては「同じ」ものであることは暗黙の了解によっていた．二つの群が「同じ」ものであることを正確に示すには「**同型対応**」を用いる．

---

15) 一つの群でも様々な正規列がある得るので，その中で一つでも条件を満たせばよい．

同型対応とは，一般には群のような構造を持った集合が「同じ」ものであることを示す方法のことである．群では，次の２つの条件が満たされた時，「**同型**」であるといい，同じ群として扱われる．

① 各元が１対１に対応すること．

② 演算の結果が対応すること．

例えば位数が３以下の群は全て同型である（証明は省く）．言い換えれば位数３以下の群は１種類しかない．一般に「位数がnである群は同型を除いて何種類あるか」とは**群論**の大きな課題となっているが，もちろんここでは触れない．

まず，ガロア群$G_1\left(k_1/k_0\right)$と剰余群G/H_1が同型であることを示そう．

$G_1\left(k_1/k_0\right)$とは基礎体k_0の上に最初に形成された体のガロア群であるから位数pの巡回群である．一方，G/H_1の位数は，指数$\left(G:H_1\right)$，すなわち$pqr\div qr=p$である．その元は$G\left(K/k_0\right)$をH_1によって分解した副群たちで，一つひとつの副群の中身は皆同じk_1のk_0自己同型対応を示している．

具体的に例を挙げると，正規部分群H_1の元σで作った副群$\sigma H_1\in G/H_1$は，以下のqr通りのk_0自己同型対応（ガロア置換）を持っている．

$$\sigma_1:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\right)$$

$$\sigma_2:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\omega\right)$$

$$\vdots$$

$$\sigma_r:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\omega^{r-1}\right)$$

(1)———————————————————————

$$\sigma_{r+1}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\right)$$

$$\sigma_{r+2}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\omega\right)$$

$$\vdots$$

$$\sigma_{2r}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\omega^{r-1}\right)$$

(2)———————————————————————

$$\sigma_{2r+1}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega^2\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\right)$$

$$\sigma_{2r+2}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega^2\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\omega\right)$$

$$\vdots$$

$$\sigma_{3r}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega^2\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\omega^{r-1}\right)$$

(3)———————————————————————

$$\vdots$$

$$\vdots$$

$$\sigma_{(q-1)r}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega^{q-1}\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\right)$$

$$\sigma_{(q-1)r+1}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega^{q-1}\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\omega\right)$$

$$\vdots$$

$$\sigma_{qr}:k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right),\quad k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega^{q-1}\right),\quad K\left(\sqrt[r]{t}\right)\to K\left(\sqrt[r]{t}\omega^{r-1}\right)$$

一番はじめのグループ①（区切り線(1)の上のr個）は，k_1/k_0やk_2/k_1は置換が起こらず，K/k_2 内のだけの置換r通りを表し，次のグループ②（区切り線(1)と(2)の間のr個）はやはりk_1/k_0の置換は起こらず，k_2/k_1では$k_2\left(\sqrt[q]{s}\right)\to k_2\left(\sqrt[q]{s}\omega\right)$を行ないながらグループ①と同じ$K/k_2$の置換$r$通りを行なう…．

このように，全てのσH_1内の置換ではk_1/k_0の置換は起きないで，全て$k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right)$のままである．だからと$\sigma H_1$はガロア群$G$の元のうち$k_1/k_0$の恒等置換を引き起こすもの全てが集まっているのである．よってσH_1は剰余群G/H_1の単位元となる．同型の条件①の，各元が1体1に対応するという意味で，ガロア群$G_1\left(k_1/k_0\right)$の単位元$k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right)$にごく自然に対応する．

G/H_1のσH_1とは異なる元，言い換えればH_1の元でないGの元σ'で作った副群$\sigma' H_1$では，上のσH_1の各元の$k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\right)$が$k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\omega^{i-1}\right)$に変わるだけで，やはり$qr$個のガロア置換をもっている．よってこれはガロア群$G_1\left(k_1/k_0\right)$の元$k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\omega^{i-1}\right)$に対応する．

以上の吟味の結果，ガロア群$G_1\left(k_1/k_0\right)$と剰余群G/H_1の元はこれらの対応によって1対1に対応する．

また，$G_1\left(k_1/k_0\right)$とG/H_1との演算の結果の対応も，どちらもk_0同型対応$k_1\left(\sqrt[p]{r}\right)\to k_1\left(\sqrt[p]{r}\omega^{i-1}\right)$を基にしていることから，簡単に対応させられる．$G_1\left(k_1/k_0\right)$の元$\sigma,\tau$に対して，それぞれ$\sigma,\tau$に対応する$G/H_1$の元$\sigma',\tau'$を対応させれば，ガロア置換の積$\sigma\tau$に副群の積$\sigma'\tau'$が対応する．よって同型の条件①，②が満たされ，$G_1\left(k_1/k_0\right)$と$G/H_1$は「同じ」群であることになった．

同様の議論で，$G_2\left(k_2/k_1\right)$とH_1/H_2も同型が認められる．

最後に，$G_3\left(K/k_2\right)$については，対応する剰余群はH_2/Eということになるが，H_2/EとはH_2のことに他ならない．位数ももともと同じr個である．あえて言えばH_2/EとH_2は同型である．

こうしてついに，方程式の代数的可解性の問題を群の性質によって判断するというガロア理論の最初の精華を掲げることができたのである．これはガロアの発見に依るものである．

【定理８】代数的に解かれる既約方程式のガロア群は可解群である．（ガロア）

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）

次に，或る群が可解群ならば，その部分群も可解群であることを証明しておこう．これは方程式のガロア群が一般には置換群であり，置換群はn次対称群の部分群であるからn次対称群の可解性を調べることで方程式の可解性の問題を一気に解決できるからである．特に，五次方程式の非可解性の最後の決め手になる命題でもある．

【定理９】可解群の部分群は可解群である．

【証明】

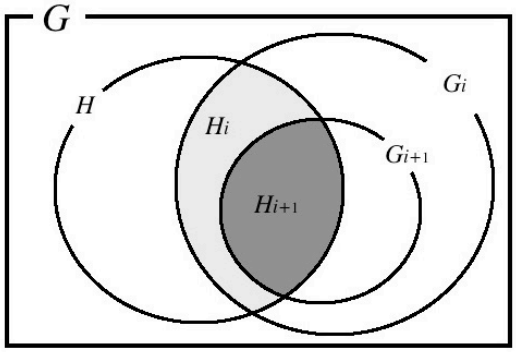
任意の可解群をGとすると，正規列，

$$G = G_0 \supset G_1 \supset \cdots \supset G_{r-1} \supset G_r = E$$

が存在し，各剰余群G_i / G_{i+1}が巡回群であるようにできる．

群Gの２つの部分群の共通部分はまたGの部分群であるから[16]，HとG_iとの共通部分群を$H_i = H \cap G_i$とおく．このとき，H_iとG_{i+1}（G_iの正規部分群）との共通部分群$H_i \cap G_{i+1}$をH_{i+1}とすると，

図-1



$$H_{i+1} = H_i \cap G_{i+1} = \left(H \cap G_i\right) \cap G_{i+1} = H \cap \left(G_i \cap G_{i+1}\right) = H \cap G_{i+1}$$

となる（図-1の濃いグレーの部分）．これは$H_0 = H \cap G_0$，$H_1 = H \cap G_1$，$H_2 = H \cap G_2$,…等々で成り立つ（H_0はHのこと，G_0はGのことである）．

H_iの任意の元をσとするとき，$\sigma G_{i+1} \sigma^{-1} = G_{i+1}$である（$G_{i+1}$は正規部分群）．もし，$\tau \in H_{i+1}$に対し，ある$\sigma$によって$\sigma\tau\sigma^{-1} \notin H_{i+1}$となるものがあれば，その$\sigma$は$H_i - H_{i+1}$（図-1の薄いグレーの部分）の元となるが，それではG_{i+1}が正規部分群であることに反する．よって$\sigma H_{i+1} \sigma^{-1} = H_{i+1}$．すなわち，$H_{i+1}$は$H_i$の正規部分群となる．

こうして，$H = H_0$，$H_1 = H \cap G_1$，$H_2 = H \cap G_2$…について，

$$H_0 \supset H_1 \supset \cdots \supset H_{r-1} \supset H_r = E$$

となる正規列が存在する．

16) 【付録５】参照.

最後に，G_iの部分群H_iとG_{i+1}の部分群H_{i+1}から成る剰余群H_i / H_{i+1}はG_i / G_{i+1}の部分群と同型になる（【付録６）参照）．よって，【定理７】によりH_i / H_{i+1}は巡回群G_i / G_{i+1}の部分群であるから巡回群となる．【証明終】

10．一般的な代数方程式のガロア群

これまでは初等的かつ具体的にガロア理論を紹介するために，方程式の基礎体をできるだけ有理数体Qに限るように進めてきた．この章では一般的な方程式を扱おうとするため，基礎体について改めて一言する．

以下の議論においては，全て基礎体は有理数体Qに必要な１の虚数累乗根を含めたものとする．すなわち，最初はQのみで議論を始めても，議論の途中で１の虚数累乗根が必要になった時はそれをQに含め，それを改めて基礎体とするのである．このように定めた基礎体を方程式の「**標準の基礎体**」ということにし，それをk_0で表す．また，扱う方程式の係数は有理数体Qの元のみとする．したがって１の虚数累乗根における共役体間のガロア置換はガロア群には含まないことにするのである．こうした処置は何よりも理論をスッキリさせ，結果としてガロア理論の美しさを我々初学者にも際立たせることになると信じるからでである．

この章での目標は，全ての標準の基礎体上の一般的なn次代数方程式のガロア群はn次対称群となることを示すことである．

そののちに，n次対称群は$n \leq 4$ならば可解群であり，$n \geq 5$ならば非可解群であることを示すことで，五次方程式が代数的に非可解であることが証明される．

【定理10】標準の基礎体上の一般的なn次既約代数方程式のガロア群はn次対称群である．

【証明】

標準の基礎体k_0に対して，係数が互いに無関係な既約方程式を$f(x)=0$とする[17]．二項方程式$x^5 - a = 0$などはxの最高次数以外の係数を０とするという「特別な」方程式なのでこれらは当てはまらないものとするのである．ただし，$f(x)=0$の最高次数x^nの係数は１としておく．

$f(x)=0$の解を$x_1, x_2, \cdots, x_n$とすれば，そのガロア体は基礎体k_0に方程式の解を全て追加することで形成される．それを$K = k(x_1, x_2, \cdots, x_n)$と表す．$K$の元は$k_0$の元を係数とする$x_1, x_2, \cdots x_n$の整式である（定理３）．一方，$K$のガロア群を$G = G(K / k_0)$とすれば，$G$の元（＝ガロア置換）は体$K$の元を他の元に写すが，それは基礎体$k_0$の元を変化させないもので，解$x_1, x_2, \cdots, x_n$の置換によって表されるのであった．これまでの例ではGが対称群そのものであったり，その一部である置換群だったりしたのだが，逆にもし解$x_1, x_2, \cdots, x_n$の**任意の**置換に対応するGの元が存在すれ

---

17) 「係数が互いに無関係」とは正確には「基礎体の上で代数的に独立」という．

ば，G は n 次対称群となる．なぜなら n 個の「もの」の置換の**全ての**集まりは n 次対称群となるからである．

解 $x_1,x_2,\cdots x_n$ の任意の置換を σ とし，この置換によって x_1 は x_1' に，x_2 は x_2' に，…，x_n は x_n' に写るとする．$x_1',x_2',\cdots,x_n'$ は $x_1,x_2,\cdots,x_n$ が置き換えられただけであるから全体としては同じものである．このとき，σ が基礎体 k_0 の元をまったく変えないで，$x_1,x_2,\cdots x_n$ の置き換えだけを起こすなら，それは体の置換に相当するものになるはずである．

さて，$f(x)=0$ の解が $x_1,x_2,\cdots,x_n$ ならば，多項式 $f(x)$ を x の一次式にまで因数分解して，

$$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n)$$

とすることができる．次にこれを展開した式を考える．

$$f(x)=x^n-Ax^{n-1}+Bx^{n-2}-\cdots+(-1)^nC.$$

このときの各 x^i の係数は当然基礎体 k_0 の元であるが，それは $x_1,x_2,\cdots,x_n$ の対称式で表わされる（付録４）．これは言い換えれば基礎体 k_0 の元のうち，有理数をすべて $x_1,x_2,\cdots,x_n$ の対称式で表すことができるということである．なぜなら，仮に x^{n-1} の係数が A になったとすれば，A は $x_1,x_2,\cdots,x_n$ の対称式 $A=x_1+x_2+\cdots+x_n$ であり，

$$0=A-A,\quad 1=\frac{A}{A},\quad 2=\frac{A+A}{A},\cdots$$

等々の計算によってすべての有理数を A で表すことができる．

K の任意の元は基礎体 k_0 の元と解 $x_1,x_2,\cdots,x_n$ の四則計算の結果（有理式という）によって表されるが，そのうち，有理数が $x_1,x_2,\cdots,x_n$ の対称式で表されるのであれば解 $x_1,x_2,\cdots,x_n$ がどのように置換されようと k_0 の元は変わることがなく，変わるのは k_0 の元以外の $x_1,x_2,\cdots,x_n$ の入れ替えだけである[18]．すなわち，解の任意の置換 σ は基礎体 k_0 の元を動かさないで，$x_1,x_2,\cdots,x_n$ のそれぞれに対応した中間体 $k_0(x_1),k_0(x_2),\cdots,k_0(x_n)$ 等の k_0 同型対応だけを示す．したがって任意の解の置換 σ に対応するガロア置換がガロア群 G に存在することになる．

n 個の解の全ての置換に対応するガロア置換が存在するのであれば，G は n 次対称群である．【証明終】

以上で（標準の基礎体上の）既約 n 次方程式 $f(x)=0$ のガロア群は n 次対称群となることが示された．その条件は係数に特別な関係がないことである．逆にいえば，係数間に何らかの関係があれば，それは解の対称式に関係して解の置換のいくつかを制限するので，そのガロア群は対称群そのものではなく，その部分群（＝置換群）になるのである．

この結論を出すために，有理数体Qに１の虚数累乗根を追加したときの次数pをn次方程式の正則拡大体Kに取り込んでいない．この次数pをKに取り込むとガロア群 $G(K/k_0)$ は三次対称群ではなく，位数npの置換群となってしまう．それでは理論としてスッキリしないというのが「標準の基礎体」を設定した理由である．

---

18) 基礎体の１の虚数累乗根は単独数としては方程式の解と無関係であり，σによって変わることはない．

方程式のガロア群が対称群となることがわかれば，次には対称群の可解性が課題となる．これについては次の定理が顕著である．

【定理11】$n \le 4$ のとき，n 次対称群S_n は可解群である．

群の可解性は一つでも例をあげればいいので，以下では実際の例を示すことで証明が終わるのだが，その前に，**交代群**について述べておこう．交代群自身には難しさはないが，その性質には謎が多い．

一般に，n 次対称群は同数の偶置換と奇置換から成っていて，偶置換だけの集合はその部分群になる．これを**n 次交代群**という（奇置換の集合は恒等置換がないので群にはならない）．三次対称群S_3 の正規部分群 A_3 は**三次交代群**である．二次対称群の場合は交代群は単位群になる．交代群の位数は対称群の位数の半分である．交代群は対称群の正規列をあげるときに重要な群となる．

$n=2$ のときは，$S_2 \supset E$ が可解列であることは自明である．

$n=3$ のとき，

$$S_3 \supset A_3 \supset E\,.$$

A_3 は S_3 の正規部分群 $\{1,(123),(132)\}$ で，三次交代群である．各剰余群，S_3/A_3 は位数２の，A_3/E は A_3 そのもので，それぞれ巡回群であるのは明らかである．よって S_3 は可解群である．

$n=4$ の場合はやや複雑さが増す．まず次の正規列が挙げられる．

$$(1)\quad S_4 \supset A_4 \supset V_4 \supset E.$$

この中の A_4 が**四次交代群**で，V_4 は前にも出たクラインの四元群である．剰余群S_4/A_4 は位数２であるからすぐ巡回群とわかるが，次の剰余群A_4/V_4 について見てみよう．それぞれの元を見ると，四次交代群 A_4 は偶置換の集まりだから，位数は12で，

$$A_4=\{1,(123),(132),(124),(142),(134),(143),(234),(243),(12)(34),(13)(24),(14)(23)\}$$

である．V_4 は，

$$V_4=\{1,(12)(34),(13)(24),(14)(23)\}\ \text{（位数4）}$$

であるから，$A_4 \supset V_4$ はすぐわかる．また，V_4 が正規部分群であるのを見るために，$\sigma \in A_4$ として $\sigma V_4 \sigma^{-1}$ が V_4 になるのか調べよう．σ が V_4 の元なら $\sigma V_4 \sigma^{-1}=V_4$ は当然である．V_4 の元以外の A_4 の元はすべて (abc) の形をしているから，これと V_4 の元 $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$ とで $\sigma V_4 \sigma^{-1}$ の計算をすると，

$$1.\ (abc)\{(ab)(cd)\}(abc)^{-1}=(abc)(ab)(cd)(acb)=cdab=(ac)(bd)$$

$$2.\ (abc)\{(ac)(bd)\}(abc)^{-1}=(abc)(ac)(bd)(acb)=dcba=(ad)(bc)$$

$$3.\ (abc)\{(ad)(bc)\}(abc)^{-1}=(abc)(ad)(bc)(acb)=badc=(ab)(cd)$$

この３つの積が全てV_4の元であることから，$\sigma \in A_4$のとき，$\sigma V_4 \sigma^{-1} = V_4$が成り立つのである．すなわち，$V_4$は$A_4$の正規部分群である．

実際には8×3＝24通りの計算が必要であるが，上の３つを確かめて，(abc)に順次長さ3の巡回置換(123)～(243)を代入したと考えれば，24通りすべてを計算したのと同じになる．

次は正規列(1)の剰余群を調べよう．剰余群はA_4 / V_4とV_4 / Eである．まず，A_4 / V_4について．

V_4のA_4における指数$\left(A_4 : V_4\right) = 12 \div 4 = 3$から，剰余群$A_4 / V_4$の位数は３である．$A_4 / V_4$の元は$V_4$の$A_4$における副群であるが，まず，$V_4$自身が$A_4 / V_4$の単位元になる．他の２つの副群を$B$，$C$とすると，これも以下の式の$(abc)$に順次長さ3の巡回置換を代入して求めることができる．

$$\left(abc\right)\left(ab\right)\left(cd\right) = adbc = (bdc).$$

(abc)=(123)のとき(bdc)=(243)，(abc)=(132)のとき(bdc)=(342)=(234)，…

これらの計算によって，(123)と(243)は同じ副群，(132)と(234)も同じ副群とわかる…[19]．こうしてB，Cが確定するまで計算を進める．こうして，

$$B = \left\{(123),(134),(142),(243)\right\}$$

$$C = \left\{(132),(143),(124),(234)\right\}.$$

$A_4 / V_4 = \left\{V_4, B, C\right\}$の群表は以下のとおり．

表-10

A_4/V_4	V_4	B	C
V_4	V_4	B	C
B	B	C	V_4
C	C	V_4	B

表を見てもわかる通り，$B^2 = C$，$B^3 = CB = V_4$となるので，A_4 / V_4は巡回群である．

さて，最後の剰余群V_4 / Eは，V_4自身と同型であるから，V_4そのものが巡回群であればよいのだが，すぐわかるようにV_4は巡回群ではない（どの元も累乗しても自分と単位元にしかならない）．

V_4は前に四次方程式$x^4 - 16x^2 + 4 = 0$のガロア群として登場したが，そのときのガロア体は，$Q\left(\sqrt{5} + \sqrt{3}\right)$すなわち$Q\left(\sqrt{5}, \sqrt{3}\right)$であった．つまり$Q\left(\sqrt{5}\right)$に$\sqrt{3}$を追加して二次の体を積み重ねていたのである．$V_4$はそれを反映しているのである．

そこで，今度は方程式とは無関係にV_4それ自身を「分割」してみよう．すなわち，V_4の部分群，

---

19) $(abc)B=(def)$Bなら，(abc)と(def)は同じ副群に属する．

$$V' = \{1,(12)(34)\}$$

を取り出すと，V' は V_4 の正規部分群[20]である．よって正規列(1)を次のように「変形」する．

$$(1)' \quad S_4 \supset A_4 \supset V_4 \supset V' \supset E.$$

こうすることで，剰余群が一つ増えるが，V_4/V'，V'/E はいずれも位数は２で，巡回群であることは自明となる．

以上の結果，四次対称群 S_4 の正規列(1)'は可解列であり，S_4 は可解群である．

【定理10】によって，全ての三次・四次方程式はそのガロア群が三次・四次対称群またはその部分群（置換群）になる．三次・四次対称群は可解群であり，また【定理９】によって可解群の部分群は可解群であるからその部分群である置換群も可解群である．ゆえに，

【定理12】全ての三次・四次方程式は代数的に可解である.

11．五次方程式の代数的不可解性

「代数的に解かれる方程式のガロア群は可解群である」という命題から，その対偶によって「ガロア群が可解群でない方程式は代数的には解かれ得ない」ことになる．これを用いて五次方程式すべてが代数的には解けないこと，正確には，**全ての五次方程式を一つの統一した方法（解の公式）で解くことはできない（アーベル・ルフィニの定理）**ことを証明しよう．このややもってまわった言い方は，五次方程式すべてが代数的に解けないのではなく，あるものは解けるが，あるものは解けないことからきている．

証明の道筋は以下の通り．

（１）五次方程式のガロア群が五次対称群となるものがあることを示す.

（２）五次対称群は可解群ではないことを示す.

上の二つの命題が成り立てば，代数的に解けない五次方程式があることになる.

（１）は10章ですでに示されている．すなわち，標準の基礎体上既約な n 次方程式のガロア群は n 次対称群であった．よって一般的な五次方程式のガロア群は五次対称群である.

（２）五次対称群 S_5 は可解群ではないことを示す.

これが示されれば，五次方程式の代数的非可解性が証明される．いわば最後の峰である.

【定理11】全ての五次方程式を一つの統一した方法（解の公式）で解くことはできない（アーベル・ルフィニの定理）

【証明】

五次方程式にはそのガロア群が五次対称群 S_5 になるものがある（定理10）.

---

[20] アーベル群の部分群はすべて正規部分群である．（$\sigma H = H\sigma$ より $\sigma H \sigma^{-1} = H$）

仮にこの方程式が（代数的に）解けたとするならば，そのガロア群は可解群であるから，ある可解列，

$$(1)\quad G = S_5 \supset A_5 \supset B \supset \cdots \supset E$$

が存在するはずである．ここでA_5はS_5の偶置換の集まりである五次交代群，

$$A_5 = \{1,(123),(124),(125),\cdots,(345),(354),(12)(34),\cdots,(25)(35),(12345),(12354),\cdots,(15432)\}$$

である．まず，正規列，

$$(1)'\quad G = S_5 \supset A_5 \supset E$$

は可解列にはならないことを確認しておこう．これが可解列ならば，A_5/Eが巡回群でなければならないが，A_5/Eと同型であるA_5が巡回群でないことは，(123)をいくら累乗しても(12345)が現れるはずはないことで明らかである．ということは，A_5/Eも巡回群ではあり得ない．よってS_5が可解群となるためには，A_5とEの間にBなる部分群が存在しなければならない，すなわち正規列は(1)でなければならないのである．当然$A_5 \neq B$かつ$B \neq E$である．

さて，【定理９】により，S_5が可解群ならA_5も可解群になるはずである．以下ではこれが成り立たないことを示す．すなわち，Bが存在するとすれば$A_5 = B$となってしまうことを証明する．そこでA_5に的を絞って議論を進める．

A_5の元は，恒等置換が１個，(abc)のパターンが20個，$(ab)(cd)$のパターンが15個，$(abcde)$のパターンが24個，合計60個ある．しかし，例えば(12)(34)=(123)(143)のように$(ab)(cd)$のパターンは(abc)の仲間である．また，$(abcde)$のパターンも$(abcde)=(ab)(ac)(ad)(ae)=(abc)(ade)$のようにやはり$(abc)$の仲間である[21]．したがって$A_5$の元はすべて$(abc)$のパターンから成り立っていると考えて良い（$A_5$は群なので$(abc)$と$(def)$が$A_5$の元ならばその積である$(abc)(def)$も$A_5$の元である）．$A_5 \supset B$であるから，$B$の元もすべて$(abc)$のパターンの元から成り立っていることになる．

BはA_5の正規部分群であるからA_5の任意の置換σについて$\sigma B\sigma^{-1} = B$が成り立つ．Bの恒等置換以外の任意の置換を(abc)とする．これに対して，A_5の元から(xyz)のパターンの元を適当に選んで，それを用いて次のような置換σを作る．

$$\sigma = \begin{pmatrix} xyzpq \\ abclm \end{pmatrix}$$

$(\ )$の中の文字x,y,z；a,b,cはいずれも1～5のいずれかで，p,q；l,mは選んだあとの余った数字である．並び方は(xyz)，(abc)と同じにする．ただし，σが偶置換であればそのままでよいが，奇置換になる場合はl,mを入れ替えることで偶置換に変えることができる[22]．以下，σを偶置換として，すなわち$\sigma \in A_5$として$\sigma(abc)\sigma^{-1}$を計算をすると，

---

[21] $(abcd)$のパターンは奇置換なのでA_5には存在しない．

[22] 偶・奇置換は，互換を一つ増やすか減らせば入れ替わることができる．

$$\sigma(abc)\sigma^{-1}=\begin{pmatrix}xyzpq\\abclm\end{pmatrix}(abc)\begin{pmatrix}xyzpq\\abclm\end{pmatrix}^{-1}=\begin{pmatrix}xyzpq\\abclm\end{pmatrix}(abc)\begin{pmatrix}abclm\\xyzpq\end{pmatrix}=yzx=(xyz).$$

$\sigma B\sigma^{-1}=B$ であるから $\sigma(abc)\sigma^{-1}=(xyz)$ は B の元を表す．すなわち，$(xyz)\in B$ となる．つまり，A_5 の全ての元の源となる (xyz) は B の元であることになり，$A_5\subset B$ となる．

一方 $A_5\supset B$ であるから $A_5=B$ となる．すなわち，A_5 は自身と E 以外の正規部分群を持たない（このような群を**単純群**という）．

【定理９】の対偶によれば，「群 G の部分群が可解群でないとき，G は可解群ではない」．よって，A_5 が可解群でない五次対称群 S_5 は可解群ではないので，五次方程式を一般的に解くための解の公式は存在しない．【証明終】

注：以上の証明は簡易的なものであり，必ずしも厳密・精緻なものではない．また，６次以上の場合には証明がもう少し複雑になるが，何れにしても５次以上の方程式には解の公式は存在しないのである．.

12．ガロア理論のまとめ

以上でガロア理論の最初の精華である「五次方程式の代数的非可解性」を証明するところまでやってきた．ここでこれまでの道のりを少し振り返ってみたい．

数千年にわたる数学の歴史の中で，19世紀初頭，代数学の分野に突然革命が起きた．もちろんそのための先人の理論的準備や社会的条件もある中での出来事であるが，それでもやはり，それはガロアという不世出の天才のみがなし得る革命であった．なによりも彼の死後数十年に渡ってもガロアを超える頭脳は現れていないことがそれを物語る．

四次まではなんとか解ける方程式が五次ではなぜ解けないのかという，一見神秘的にさえ見える出来事を，ガロアは「群」という単純極まりない，しかし底知れぬ深遠さを秘めた数学的概念を発見することで実に明快に解決し，偉大な遺産を後世の数学者たちに残して逝った．

方程式を解くとは四則の逆演算であるとの考え方もあるように，或る数 x に四則や累乗を行なって何かの値を得るとき，これはいわば一本の道を辿るだけであるが，その逆に最後の値から遡ってもとの数に立ち返ることが方程式を解くということである．そのための道は累乗根（$\zeta_n^i\sqrt[n]{a}$，ζ_n は１の虚数 n 乗根）が深いほど複雑になる．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．

例えば２という有理数からその平方根を得たとき，$\sqrt{2}$ の他にそれとまったく同等な $-\sqrt{2}$ という数が立ち現れる．累乗根 $\zeta_n^i\sqrt[n]{a}$ の各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自身に掛けられている１の（虚数）累乗根の累乗=ζ^i だけである．ζ^i は累乗の繰り返しによってまた自身に回帰するという性質を持つ．これを「**巡回性**」ということにしよう．この性質によって累乗根は互いに移り合う．この累乗根の巡回性は拡大体の中で各部分体の置換に及び，これがガロア群の剰余群に反映するのである．

累乗根の巡回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．正多角形の対称軸の多様さは累乗根の巡回性を見事に表現している．a の n 乗根を方程式で表わすと n 次の二項方程式になり，円の半径は $|a|$ に拡大する．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複素数平面上を四方に散らばっていき，やがて正多角形の対称性が失われていく．この散らばり方をとらえるのもまたガロア群である．

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 $G=E$（単位群）であろう．すなわち，基礎体を基礎体に移す「ガロアの対応」1個から成る群である．

二次方程式では，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．基礎体の或る数を開平すると基礎体の中にはない数（**生成元**）が現れる．基礎体と生成元とによって新たな体（拡大体）が形成される．この体の同型対応が解の置換によって表され，解の置換群すなわちガロア群として確定する．二次方程式のガロア群は二次対称群である．ここでは累乗根の巡回性は，解の中に出て来る平方根の正負符号の交代性という現象に現れる．

三次方程式になると平方根に続いて立方根が追加され，二次の体の上に三次の体が積み重ねられる．拡大体はより複雑なものになる．３つの解の置換によるガロア群も位数６の三次対称群となる．この三次対称群は，最初の平方根による拡大体の上では偶置換だけに制限され，したがって三次交代群として次の立方根の巡回性を保証しなければならないが，実は三次交代群はその本質が巡回群である．これによって三次交代群の剰余群が巡回群であることを如実に示す．ゆえに可解性が保証される．

次の四次方程式は二次・三次の拡大体の上にもう二つの二次体が追加される．それは４という次数が 2^2 という合成数であることに由来する．４つの解からなる四次対称群は最初の平方根によって位数12の四次交代群に制限される．この四次交代群にはクラインの四元群という特別の部分群が存在して，その剰余群が位数３になる．そのおかげ（？）で立方根の巡回性を保証して残りの二つの二次体をクラインの四元群に引き渡すことができ，結局，可解性が保証される．

しかし，五次方程式では，累乗根の巡回性にとって本質的な問題が生じる．代数学の基本定理により５つの解は存在するが，五次対称群が最初の平方根によって制限された五次交代群には立方根の巡回性を保証できないのである．五次交代群には真の正規部分群がなく，自身も巡回群ではないからである．したがって２つ目の累乗根である立方根は五次交代群の中で自身を巡回させることができない．

五次方程式が可解であると仮定して矛盾を導き，それによって非可解性を証明したのはアーベル（及びルフィニ）である．その道筋を大まかにいうと，平方根によって拡大された体の上での立方根は，（方程式の）３つの解の巡回置換によっては１の虚数立方根 ω の巡回と矛盾しないが，５つの解による巡回置換の５回の巡回によって $\omega^5=1$ となり，結局 $\omega=1$ となって矛盾が起きるというものである．これは「解けた」と仮定しているので，立方根の巡回が先に保証されているのであるが，そうすると５つの巡回置換の方が矛盾を起こすという論法である．ガロア理論流に言えば五次交代群が成立しないということである．

結局，五次方程式が代数的に解けないということは前章の結論にある通り，五次の（正確には五次以上の）交代群の単純性（真の正規部分群を持たないこと）にその本質があるのである．

高木貞治先生の「代数学講義」ではアーベルの考えに基づく証明の後，「要するに，五つ以上の変数の場合には$\phi(x_1,x_2,\cdots,x_n)$自身が交代式ではなくて，しかもϕ^qが交代式になるということが不可能なのである」と喝破されている．（1994年改訂版25刷 p.200）

ここでは証明はできないが，**素数次の交代群は全て単純群である**．実は二次・三次においても交代群は単純であったが，同時に（低次であることによる）巡回群であったため方程式の可解性には影響が及ばなかったのである．ここまで来ると，「五次以上の代数方程式が解けないようになっているのは，そもそも交代群というものが単純だからである」ということができる．

ガロア以降，俄然数学者たちが群やその他の代数系に目を向けるようになったのも宜なるかなである．

13．ガロア理論の応用

ガロア理論は，現代では「体の自己同型群に関する双対定理として把握され」（岩波数学辞典第２版・1975年）て，実際にガロアが遺した論文での表現とはかなり異なっているが，ガロア自身その理論が方程式論以外にも応用され得ることを確信していた．事実その通りで，その威力は非常に強力であり，かつ簡潔である．まさに天才のなせる技とはこのようなものかと目をみはるばかりである．何よりも長年数学者を悩ましてきた「超難問」が次々に解決されていくさまは痛快この上ないであろう．

その第１番目はもちろん五次方程式の代数的不可解性（定理11）であるが，それよりもっとポピュラーでインパクトのある問題として，定木とコンパスによる作図問題がある．一般角の三等分，立方体倍積問題，円積問題（ギリシア三大問題）など．現在でもまだこれらの問題について「ついに発見した」という論文が某大学に寄せられるという話を聞いたことがある．そのような人はぜひその情熱をガロア理論に向けていただきたいと願うばかりである．また，この小論でも簡易的な証明を紹介した「代数学の基本定理」（ガウス）もガロア理論による証明が可能である．

ここでは大して予備知識のいらない定木とコンパスによる作図の不可能な問題をいくつか紹介し，ガロア理論の威力を垣間見ることにしたい．

作図問題の予備知識：定木とコンパスで行われる作図は，それをxy平面上の**解析幾何学**として捉えれば全て二元二次方程式（円）と二元一次方程式（直線）の交点の座標を求めることに帰着する．すなわち，円と円，あるいは円と直線の交点を求める方程式は常に二次方程式である．したがって有限回の手段で得られた円及び直線の交点の座標は常に二次方程式の解である．そこで，作図の問題を方程式で表したものを「作図の方程式」ということにすると，作図可能とは，作図の方程式のガロア体に可解列が存在して，その全ての剰余群が位数２であること，言い換えれば，正則拡大体の有理数体に対する次数は２の累乗でなければならない，ということになる．これが肝要である．

以下はいずれも定木とコンパスによる作図問題である．

（1）一般角の三等分は不可能なことの証明

一般角どころか，60度でさえ不可能なことをガロア理論によって証明しよう．これがわかれば簡単に一般角にも応用ができる．

【定理13】60°の角を定木とコンパスで３等分する作図は不可能である．

【証明】

三角関数の３倍角公式，

$$(1)\quad \cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

にθ=20°を代入すれば，

$$\cos 60^\circ = 4\cos^3 20^\circ - 3\cos 20^\circ$$

ここで60°は作図上与えられているので，$\cos 60^\circ$=1/2を代入し，$x = \cos 20^\circ$とおけば，有理数体上の方程式，

$$\frac{1}{2} = 4x^3 - 3x$$

が得られる．したがって作図の方程式は，

$$(2)\quad 8x^3 - 6x - 1 = 0\,.$$

これが解ければ$x = \cos 20^\circ$が得られる[23]が，(2)は有理数体上既約な三次方程式であるから，ガロア体には３次の体が含まれる．すなわち次数が２の累乗ではないので作図不可能である．【証明終】

証明の内容の大半は作図の方程式を作る過程の説明で，実質の証明は最後の２行，方程式(2)は有理数体上既約な三次方程式であるから有理数体上２次の体の積み重ねではない，よって作図不可能というだけである．あまりに簡潔すぎて拍子抜けかもしれないが，ガロア理論が確立しているならばこれ以上いうことはないのである（あえていうならば，(1)が「有理数体上既約」であることを示すのがやや難しい）．逆に，方程式(2)の定数項を方程式が可約になるように定めれば３等分の作図が可能になる．例えば方程式(2)の定数項を０とするならば，$4x^3 - 3x = 0$となるから，

$$x\left(4x^2 - 3\right) = 0 \quad \therefore\ x = 0,\ \pm\frac{\sqrt{3}}{2}$$

となる．これは$x = \cos\theta = \pm\sqrt{3}/2$であるから，$\theta$は30°,120°．よって元の角$3\theta$は直角と360°である．$x = \cos\theta$=0の方は$\theta$は90°だから元の角$3\theta$は270°，確かにいずれも３等分できる．

以上から，一般角の３等分の作図問題は，方程式(2)の定数項の値によって式の左辺が有理数の範囲で因数分解できるかというわかりやすい問題に転化できる．

（２）立方体の体積を２倍にするための作図が不可能なことの証明

これは「デロスの問題」という別名もある有名な難問であるが，要するに立方体の体積を２倍にするには一辺を$\sqrt[3]{2}$倍にしなくてはならないということになる．この小論を読まれた方には，$\sqrt[3]{2}$が出てきた時点でもう作図不能なことが予測できるのではないかと思う．まさにその通りで，

---

[23] $\cos\theta$が作図可能な値（有理数と平方根からなる）で得られれば，角度としてのθも作図可能である．

もとの立方体の一辺を 1 とすればその体積は $1^3=1$ である．ゆえに２倍にする立方体の一辺を x とすれば，方程式は，$x^3=2$ となる．この方程式のガロア体は $Q\left(\omega,\sqrt[3]{2}\right)$ という Q 上６次の体であるから２の累乗ではない．ゆえに作図不可能である．

ギリシア三大問題のもう一つは「円積問題」（円と同じ面積の正方形の作図）であるが，これはこの小論のレベルを大きく超えるのでここに述べることはできない．作図不可能なことは確かである．

（3）正七角形の作図が不可能なことの証明

1 の n 乗根が複素数平面上で原点を中心とした正 n 角形の頂点の座標になることは前述したが（12章），これを利用して方程式 $x^7-1=0$ の解を全て求めれば正七角形の頂点が得られる．しかしこの方程式のガロア体はやはり２次体の積み重ねにはならないのである．$x^7-1=0$ より，

$$(x-1)\left(x^6+x^5+x^4+x^3+x^2+x+1\right)=0.$$

$x^6+x^5+x^4+x^3+x^2+x+1=0$ の両辺を x^3 で割って，

$$(1)\quad x^3+x^2+x+1+\frac{1}{x}+\frac{1}{x^2}+\frac{1}{x^3}=0.$$

$X=x+\frac{1}{x}$ とおけば，$x^2+\frac{1}{x^2}=X^2-2,\ x^3+\frac{1}{x^3}=X^3-3X$ であるから，(1)の式は，

$$(2)\quad X^3+X^2-2X-1=0$$

となって，X の三次方程式になる．これも有理数体上の既約方程式であるからガロア体が３次の体を含むので作図は不可能となる．ただ，(2)を代数的に解くことは理論的にはできるので，正七角形の頂点を座標として得ることは可能ではある．それはしかし実用的な方法とはいえない．

ちなみに正五角形は上と同様の計算で，$x^5-1=0$ より，

$$(x-1)\left(x^4+x^3+x^2+x+1\right)=0.$$

今度は $x^4+x^3+x^2+x+1=0$ の両辺を x^2 で割り，$X=x+\frac{1}{x}$ とおけば，

$$X^2+2X-1=0$$

となって，X の二次方程式になる．これは二次方程式を二つ解くことで全ての解が得られるのでガロア体も４次となり，次数が２の累乗なので作図が可能である（実際の作図はよく知られているので略す）．

作図の問題では，F.ガウスの「正十七角形の作図」がつとに有名である．1796年（ガロア生年の15年前），当時19歳のガウスがこの作図法を発見したという逸話については高木貞治著「近世数学史談」（共立出版株式会社 1996年復刻版）に詳しい．また，実際の作図法がやはり高木貞治著「初等整数論講義」（同上 1994年第２版）p.111に出ている．

以上の例では，ガロア群はほとんど姿を見せない．だが，「作図の方程式のガロア体に可解列が存在して，その全ての剰余群が位数２であること」というのは，紛れもなくガロア理論によることなしには得られない結論である．

【付録】

（注：ここでの証明はすべて簡易的なものである．概略を把握した上はぜひ専門書で正確・厳密なものを参照してほしい）

【付録1】$\sqrt{2}$ は有理数ではない．

【証明】仮に $\sqrt{2}$ を有理数と仮定すると，

$$\sqrt{2}=\frac{p}{q}\quad（p\text{は整数，}q\text{は自然数で互いに素}）$$

のような既約分数で表すことができる．両辺を２乗して変形すると，

$$2q^2=p^2$$

となるが，これから p^2 が偶数であり，従って p も偶数であることになる．ゆえに $p=2p'$ とおいてこの式に代入すると，

$$2q^2=4p'^2\quad\therefore q^2=2p'^2.$$

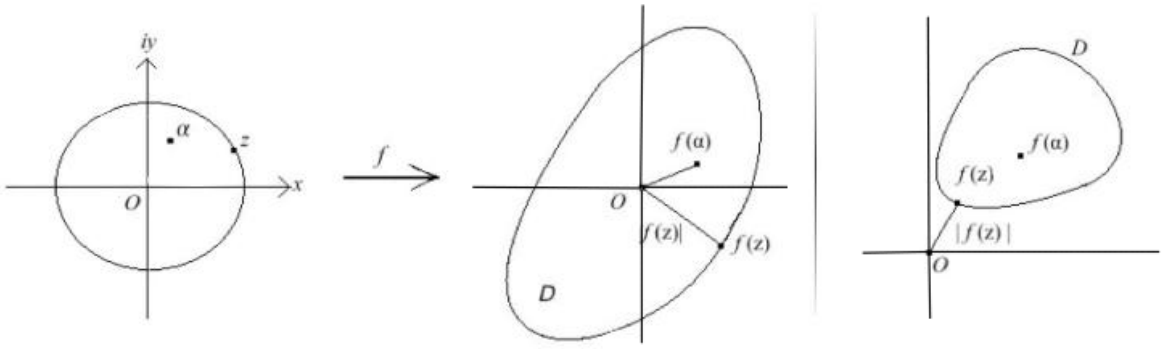
よって，q も偶数になる．p,q がともに偶数になれば互いに素であることと矛盾する．【証明終】

【付録2】「代数学の基本定理」の（簡易的）証明

複素数を係数に持つ n 次方程式 $f(x)=0$ は複素数の中に少なくとも一つの解を持つことを示すのであるが，それには**複素数平面**を前提とする（これについては既知とする）．複素数平面上で複素数 z の表す点を**点 z** という．さらに，与えられた方程式を，複素数を変数とする関数 $w=f(z)$ として考え，w は z の連続関数となることも前提とする．（このような数学を**複素解析**あるいは単に解析という．複素解析では独立変数は z，従属変数は w で表す．）

次に，二つの複素数平面を考え，一方を z の定義域用に，もう一方を $f(z)$ の値域用として考える．そして定義域用の平面に原点を中心として適当な半径の円を描き，この円の中の点及び円周上の点の表す数（複素数）を z の**定義域**とする．すると，それに対応する関数 $w=f(z)$ の**値域**が，円ではないかもしれないがやはり閉じられたある範囲として値域用の平面のどこかにできる．ここで重要なことは点 z が定義域の**円周上**を（連続的に）動くときには，点 $f(z)$ もやはり値域の**周上**を（連続的に）動き，円の内側を動くときには値域の内側を動くということである．

このとき，定義域の円の大きさや関数 f の係数によっては値域の中に原点 O が含まれる場合と含まれない場合が考えられる．



上の図は，最左図が x の定義域，右２つはいずれも $f(z)$ の値域を表している．中の図は値域に原点 O が含まれる場合，最右図は値域に原点 O が含まれない場合を示している．

もしこの**値域内に複素数平面の原点 O が含まれていれば，それに対応する点 z が定義域にあるはず**だから $f(z)=0$ が成り立つ．すなわち解が存在することになる．ゆえに問題はどのような方程式に対しても適当な定義域の円を描くことで，それに対応する値域の中に原点を含むことができるかということになる．実際それは可能で，定義域として大きな円を描けば，それに対して値域をいくらでも大きくできるので，いつかは原点を含ませることができる．**従って基本定理は証明された**ことになるのであるが，これではあまり大まかすぎるという人のためにもう少し詳しく説明しよう．

まず，定義域内に任意の複素数 $z=\alpha$ を取ったとき（最左図），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．次に，点 $f(z)$ と原点との距離を考えよう．これは式としては $|f(z)|$ で表される．（例えば複素数 $2-3i$ について，$|2-3i| == \sqrt{2^2+(-3)^2}=\sqrt{13}$ は点 $2-3i$ の原点からの距離を表す．）

仮に中の図のように，原点 O が値域の中に含まれているならば，関数 $|f(z)|$ の最小値は当然 0である．$|f(z)|=0$，すなわち $f(z)=0$ となる点 z が存在し，従って解が存在する．これが目標である．

さて，最右図のように原点 O が値域の中に含まれないならば，点 $f(z)$ の原点からの距離すなわち $|f(z)|$ が最も小さくなるのは点 $f(z)$ が領域の境界上にある場合である．このことを命題として次のように言い表すことができる．

命題１：「**原点 O が値域内にないならば，$|f(z)|$ が最小となる点 $f(z)$ は値域の周上にある**．」

この命題の**対偶**が重要である．それは，

命題２：「$|f(z)|$ が**最小となる点 $f(z)$ が値域の周上にないならば，原点 O が値域内にある**．」

命題１は正しいので命題２も正しい（対偶関係にある命題は同値である）．

この命題２を成り立たせるためには $|f(z)|$ が最小となる点 $f(z)$ が値域の周上にないようにすればよい．ということは，最左図で**点 z が円周上を１周する時，対応する点 $f(z)$ の原点からの距離がいつでも $|f(\alpha)|$ よりも大きい，すなわち $|f(z)|>|f(\alpha)|$ となるように，定義域の円の半径を取ればいい**のである．そうすれば値域の周上の $f(z)$ は最小点にはなり得ない（$|f(\alpha)|$ の方が小さくなるようにしたから）．その結果，命題２により値域内に原点 O があることになり，従って基本定理が成り立つことになるのである．

しかし，このためには，今一つの定理を前提しなければならない．それは，一般に複素数平面上の任意の連続関数 $w=f(z)$ で，z の値を自由に取ることで点 $f(z)$ の原点からの距離すなわち $|f(z)|$ の値をいくらでも大きく取ることができるというものである．これは感覚的にいえば，原点から「遠い」ところに点 z を取れば，それに対応する点 $f(z)$ も原点から「遠く」なるということである．当たり前のようであるが，これの（厳密な）証明はかなり面倒で，基本定理の証明が難しいのはこの定理のせいといえないこともない．従ってここでは「なんとなく」理解できればよしとしてほしい（換骨奪胎の所以である）．

この定理を承認すれば，晴れて「代数学の基本定理」が成り立ち，全ての代数方程式は複素数の範囲に（少なくとも 1 つの）解を持つことが証明された．【証明終】

【付録3】整式 $f(x)$，$g(x)$ の最大公約数を $d(x)$ とするとき，ある整式 $p(x)$，$q(x)$ が存在して，

$$f(x)p(x)+g(x)q(x)=d(x)$$

が成り立つ.

【証明】ユークリッドの互除法を用いる．必要な記号として整式 $f(x)$ の次数を表す「$\deg f$」を導入する．$f(x)$ が三次式ならば，$\deg f=3$ である．また以下ではすべて x の整式なので $f(x)$，$g(x)$ などを f，g 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，$\deg f > \deg r_1 > \deg r_2 > \deg r_3$ …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．

$$f = gq_1 + r_1 \quad (\deg f > \deg r_1) \qquad \cdots①$$
$$g = r_1q_2 + r_2 \quad (\deg r_1 > \deg r_2) \qquad \cdots②$$
$$r_1 = r_2q_3 + r_3 \quad (\deg r_2 > \deg r_3) \qquad \cdots③$$
$$\vdots$$
$$r_{n-2} = r_{n-1}q_n + r_n \quad (\deg r_{n-1} > \deg r_n) \quad \cdots④$$
$$r_{n-1} = r_nq_{n+1} \qquad \cdots⑤$$

最後の⑤で，r_n は r_{n-1} の約数である．これをひとつ前の④に代入すると，

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

となって r_{n-2} も r_n を約数に持つことがわかる．以下同様に順次上の式に代入していくと②及び①から f，g ともに r_n を約数に持つことがわかる．従って r_n は f，g の公約数である．

次にこの r_n が f，g の最大公約数であることを示す.

仮に 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，$\deg r' > \deg r_n$ となる．このとき①から r' は r_1 の約数になる．なぜなら r' は f，g の公約数だから．そして②から r' は r_2 の約数になる．…以下同様にして⑤まで来ることによって r' は r_n の約数になる．ということは $\deg r' \leq \deg r_n$ でなければならないから矛盾する．よって r_n は f，g の最大公約数 d である．

$$r_{n-1} = dq_{n+1} \qquad \cdots⑥$$

さて，次は①から順に下がって $d = fp + gq$ となる p,q があることを示す．①より，

$$r_1 = f - gq_1 \qquad \cdots①'$$

を②に代入すると，$g = (f - gq_1)q_2 + r_2 = fq_2 - gq_gq_2 + r_2$，よって，

$$r_2 = g - fq_2 + gq_1q_2 = f(-q_2) + g(1 - q_1q_2) \qquad \cdots②'$$

つまり，①'ではr_1を$fp+gq$の形に表し，②'ではr_2を$fp+gq$の形に表したわけである．次には②'を③に代入して…以下同様にして④までやってくると，r_nも$fp+gq$の形に表されるはずである．$r_n = d$であるから，

$$d = fp + gq$$

すなわち，

$$d(x) = f(x)p(x) + g(x)q(x)$$

となるような整式$p(x)$，$q(x)$が存在する．【証明終】

（付録の付録：上述の証明は整数の場合も同様に可能である．もともとユークリッドの互除法は整数における最大公約数の求め方から来ている．）

【付録４】

対称式とは，いくつかの文字からなる式で，その文字を置換しても元の式と同じ結果になるものをいう．例えば，x^2+xy+y^2は，xとyを入れ替えるとy^2+yx+x^2になるが，これは元の式と同じものであるから対称式である．また$a^3+b^3+c^3-3abc$などは，a,b,cのどの文字を入れ替えても（置換しても）同じ式になるのでやはり対称式である．

一般にn個の文字$a_1,a_2,\cdots,a_n$について次のn個の式を「基本対称式」という．

$$a_1 + a_2 + \cdots + a_n$$
$$a_1a_2 + a_1a_3 + \cdots + a_1a_n + a_2a_3 + a_2a_4 + \cdots + a_{n-1}a_n$$
$$\cdots\cdots$$
$$a_1a_2\cdots a_n$$

すなわち，$1 \le i \le n$とするとき，i個の文字の積の和である（同じ文字の積は含まない）．

a,b,cなら，$a+b+c$，$ab+bc+ca$，abcの三つが基本対称式である．

また，xの一次式$x-x_i$がn個の積を作っているとき（$1 \le i \le n$），

$$(x-x_1)(x-x_2)\cdots(x-x_n)$$

となるが，これを展開すると，

$$x^n - Ax^{n-1} + Bx^{n-2} - \cdots + (-1)^{n-1}Cx + (-1)^n D$$

となって，x^{n-1}, x^{n-2}, …, x, 1の係数A, B, …, C, Dがx_1, x_2, … , x_nの基本対称式になる（ただし交互に異なる正負の符号に注意！）．例えば，三次式なら，

$$(x-x_1)(x-x_2)(x-x_3)$$
$$= x^3 - (x_1+x_2+x_3)x^2 + (x_1x_2+x_2x_3+x_3x_1) - x_1x_2x_3 .$$

【付録５】

ある群の二つの部分群の共通部分は群である理由は以下の通り．

群Gの二つの部分群をG_1, G_2とし，$H=G_1\cap G_2$とする．少なくとも単位元は共通するので空集合ではない．また，Hが単位元以外の元σを持てば，$\sigma^{-1}\in H$である．なぜなら，もしσ^{-1}がHになければ$\sigma^{-1}\in G_1-H$または$\sigma^{-1}\in G_2-H$となってどちらの場合でもσ^{-1}が一方の部分群にないことになる．次に，$\sigma,\tau\in H$ならば，積$\sigma\tau$も同様にHに含まれる．これもHにないとするとやはりG_1-HかG_2-Hのどちらか一方にだけあることになって矛盾する．

以上から$H=G_1\cap G_2$は群である．

【付録６】

「G_iの部分群H_iとG_{i+1}の部分群H_{i+1}から成る剰余群H_i/H_{i+1}は，G_i/G_{i+1}の部分群と同型となる」ことを，一般的な群の性質として初等的に証明することができなかったので，以下のような「整数の加法による群」による説明を採用した．

整数の加法を群の演算に見立てると整数の集合は群になる．いま，おおもとの群Gとして整数の集合Zをとる．

$$Z=\{\cdots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \cdots\}.$$

G_iを２の倍数の集合として「$2Z$」と表すと，$2Z$はZの部分群となる．以下同様に，G_{i+1}は$2Z$の部分群として12の倍数の集合「$12Z$」とする．また，H_iもG_i（＝$2Z$）の部分群であるからこれを「$8Z$」としよう．そしてH_{i+1}はG_{i+1}（＝$12Z$）とH_i（＝$8Z$）の共通の部分群であるから「$24Z$」とする．一覧すると，$G_i=2Z$，$G_{i+1}=12Z$，$H_i=8Z$，$H_{i+1}=24Z$である．

このとき，剰余群G_i/G_{i+1}とは，$2Z$の$12Z$による剰余群である．これは2の倍数を6の倍数とそうでないものに分ける（副群とする）ことであるから，$12Z$，$12Z+2$，$12Z+4$，$12Z+6$，$12Z+8$，$12Z+10$の６つの元から成る．ただし$12Z+2$とは12の倍数に2を足したものの集合を表す．他も同様．

$$G_i/G_{i+1}=2Z/12Z=\{12Z,\ 12Z+2,\ 12Z+4,\ 12Z+6,\ 12Z+8,\ 12Z+10\}.$$

同様に，剰余群H_i/H_{i+1}は$8Z$の$24Z$による剰余群であるから，$24Z$，$24Z+8$，$24Z+16$の三つの元から成る．よって，

$$H_i/H_{i+1}=8Z/24Z=\{24Z,\ 24Z+8,\ 24Z+16\}.$$

ここで．G_i/G_{i+1}の部分群$\{12Z,\ 12Z+4,\ 12Z+8\}$からH_i/H_{i+1}への対応:$aZ+b\to 2aZ+2b$を与えると，

$$12Z\to 24Z,\quad 12Z+4\to 24Z+8,\quad 12Z+8\to 24Z+16$$

となる．この対応はG_i/G_{i+1}の部分群$\{12Z,\ 12Z+4,\ 12Z+8\}$とH_i/H_{i+1}との同型対応になる．すなわち元には元が，和には和が対応する．

以上が「G_iの部分群H_iとG_{i+1}の部分群H_{i+1}から成る剰余群H_i/H_{i+1}はG_i/G_{i+1}の部分群と同型となる」という意味である．

この説明のように，「整数の加法による群」は，群の様々な性質を明快に教えてくれるもので，他にも様々な利用法がある．

【改訂あとがき】

拙論「ガロア理論の初等的解題」の改訂を思い立って１年，やっと完成した．

初版には勉強不足から心残りがいろいろあって，それが今回の改訂の動機である．

改訂版では，そういう意味では心残りはない．完璧なものができたというつもりは全くないが，自分を納得させるだけのものにはなったと思う．

特にいくつかの証明では，参考にした文献に出ているものを丸ごと載せるのではなく，自分の考えに一番近いものを初等的に解釈して（換骨奪胎して）苦労して書いた．度々断っているように，あくまでも予備知識のいらないこととわかりやすさとを目指した．「初等的解題」とは当初からの変わらぬ目標である．

中には苦労して書いた内容と同じ考えを参考文献で見つけて意を強くしたものもある．例えば，一番参考にした淡中忠郎先生の著書「大学教科 代数学新講」（株式会社養賢堂 昭和41年）では可解群の因子群はアーベル群として定義されていたが，私は可解群の因子群（用語は「剰余群」とした）は巡回群で定義した．後で四次対称群の正規列に巡回群でないクラインの四元群V_4が出てきたときにハタと困ったが，V_4をさらに分解して二次体の積み重ねにすることを（散歩中に）思いついた！　後で他の参考文献（ポストニコフ著「ガロア理論」東京図書出版株式会社 1976年）で同じものを見つけたときにはとても嬉しかった．

巡回置換の計算などは慣れない人には面倒だろうが，省くことなくむしろ積極的に取り入れた．これを乗り越えないではガロア理論をうわべだけの理解で終わらせてしまうだろうからである．しかし式の計算などはできるだけ少なくし，次々に出てくる新しい用語の説明にページを費やしたつもりである．

それでもやはりガロア理論は難しい．基本定理など言葉で言えば二，三行だが，その中身は深淵である．わかってしまえばむしろ単純で当たり前なことが，そこへたどり着くまでに多くの困難を経験することは何事にもつきものである．そこを乗り越えるだけの魅力がガロア理論にはあることも強く訴えたい．

現代の数学では抽象性があまりに進みすぎて，社会一般との乖離が甚だしいように思う．なんとかその仲をとりもつことができないかとは街の一数学愛好家たる私の願いである．敬愛する高木貞治先生の「古典代数学は…むしろ却って新興代数学の階梯として，一層重大性を加えたものと思われる」（「代数学講義」序言）に同感の意を強くする．ただ，ガロアも高木先生もすでに古典の域に入るものであり，私自身が古色然とした嫌いは何とも拭いがたい．

2016年11月13日

福沢正男

【初版のあとがき】

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

【参考文献】

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「大学教科 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
○ 「岩波数学辞典」第２版
株式会社 岩波書店 1975年4月15日第２版8刷発行
○ 「数学小辞典」矢野健太郎 他編著
共立出版株式会社 昭和49年10月20日初版19刷発行

文献筆頭に掲げた淡中忠郎 著「大学教科 代数学新講」の裏表紙見開きには「147番 数学科 鵜飼勇夫」のサインがある．鵜飼氏は私の中学時代の同級生で，数学好きの私に大切な大学の教科書を貸してくださったのを，私が返却することなしに五十年借りっぱなしにしているのである．この本には若き日の私の鉛筆の書き込みで真っ黒なページもあり，今更お返しすることもできない代物になってしまったが，この小論を鵜飼勇夫氏に捧げることで長年の非礼と感謝の意を表したい．　　2016年11月14日　福沢正男