代数方程式の根の公式とガロア理論入門　（その 1）

2025.12.29　　鈴木　実

1　はじめに

2 次方程式の根の公式は良く知られている．3 次方程式の根の公式はカルダノの公式として，4 次方程式の根の公式はフェラーリの公式として知られている．5 次以上の方程式の場合は，楕円関数のような特殊関数を用いた公式を除き，四則演算と冪根のみを用いた根の公式はない．このことは，最初アーベルによって証明され，すぐ後にガロアによって群という概念を用いることにより必要十分条件という形で体系的にかつ簡潔に証明された．ところが，簡潔にとはいうものの，実際にガロア理論を理解するのはそれほど簡単ではない．それは，ガロアによって導入された群という概念が代数学で重要な分野を築いたということにも関係がある．そのため，各種の書籍を読もうとしても，まるまる一冊の本を読む必要があり，しかも関連する内容が体系的かつ網羅的に記述されている場合がほとんどであり，十分理解するのはかなり大変である．初心者を対象とした本もあるが，群や体の概念の理解なしに，その本の範囲で本当に理解できると考えるのはかなり無理がある．ガロアの理論を理解する上で，群と体の概念は必須な前提といえる．そこで，この解説文では，代数方程式の四則演算と冪根による解法とガロア理論の関係がどのようなものであるのかということを，一般の解説書と同様に群と体の概念の上に立ちつつ，網羅的であることをなるべく避けて，できるだけ直線的にかつ直接的具体的に述べたい．

ガロア理論の面白さを理解するためには,「群」と「体」の概念，および「体の拡大」という概念を理解することは不可欠であると筆者は考えている．そこで，本文では代数学の基礎知識を前提としていないので，最初に，群と体および体の拡大の基礎知識に関する項目を設けている．ただし，それは読み進めるために必要な基礎的な部分のみにとどめ，それ以上に必要な内容については，随時説明を補うことにした．また，各種の定理などの証明は長くなる場合が多く，直線的な記述から逸脱する場合には，脚注や付録にまとめて記すことにした．

次節では，ガロア理論による代数方程式の解法とその考え方の筋道を述べる．第 3 節から第 6 節では，その筋道に沿って，数学の定義に基づき，代数方程式の解法に密接な関係を有する二項拡大体までを述べる．第 7 節では，二項拡大体のガロア群について，前節まで述べられたことを踏まえて，可解の概念に密接に関係する剰余群および巡回群について述べる．

本文章は主にポストニコフ「ガロアの理論」[1] に則っているが，アルティン「ガロア理論入門」[2]，彌永昌吉「ガロアの時代　ガロアの数学　第二部　数学篇」[3] 中島匠一「代数方程式とガロア理論」[4] も参考にした．

2　ガロア理論における解法の筋道

2.1　方程式が代数的に解けるということ，根の公式とは

2.1.1　2 次方程式の場合

有理数を係数とする 2 次方程式を考えよう．2 次方程式の根の公式はまとめてしまうと，有理数の 2 乗根とそれに対する有理数の加算として得られる．ここで出てくる各有理数は，それぞれ方程式の係数の四則演算結果である．このことを以下のように考える．

有理数のみの集合の中には因数分解ができない 2 次方程式の根は含まれない．これに上の有理数の 2 乗根を加え，かつ，この 2 乗根と有理数の間のあらゆる四則演算の結果をすべて含めた集合に拡大すれば，この集合にはこの 2 次方程式の根が含まれることになる．このことは，有理数とある有理数の 2 乗根の四則演算により 2 次方程式の根が得られることを意味する．すなわち，その四則演算と 2 乗根の操作を式に表せば，2 次方程式の根の公式が得られるということである．

2.1.2 3 次方程式の場合

3 次方程式の根は次のカルダノの公式

$$x = \omega \sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \omega^2 \sqrt[3]{-\frac{q}{2} \mp \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} \tag{1}$$

で与えられる．2 次方程式の場合と同じように，以下のように有理数の集合を拡大した集合の中に根が含まれることを示すことができる．まず式 (1) において，根 x は，有理数のみの集合に有理数 $(q/2)^2 + (p/3)^3$ の 2 乗根を加えて上の意味で拡大し，さらにその 2 乗根にある有理数 $-q/2$ を加えて得られる数の 3 乗根を加えてさらに拡大し，これに $x^2 + x + 1 = 0$ の複素根 $\omega = (-1 \pm \sqrt{3}\mathrm{i})/2$(i は虚数単位) を加えて拡大した集合を作る．次に，同じように $-q/2$ から上の 2 乗根を差し引いた数はすでに拡大した集合にあるので，この数の 3 乗根を加えて拡大した集合を作り，その中の要素とその前に得られた集合の要素から 3 次方程式の根を四則演算で得られることがわかる．ここまでの過程で，もとの有理数の集合を 4 回拡大していることになる．この操作の結果得られた集合に 3 次方程式の根が含まれるということは，有理数の集合を 4 回拡大することによって，3 次方程式の根を含む集合が得られることを意味する．つまり，3 次方程式の根の公式が四則演算と冪根によって得られることを意味する．

2.1.3 根の公式が存在するということ

上の 2 つの場合から次のことがわかる．有理数の集合に，その中の 1 つの数の冪根を加え，その冪根を含むあらゆる四則演算結果を含めた集合を作るという操作，すなわち，最初の有理数の集合を拡大するという操作をひとつの単位として，これを有限回繰り返して方程式の根をその集合の中に取り込んでいることがわかる．この操作は，2 次方程式の場合は 1 回，3 次方程式の場合は 4 回行ったことになる．一般に，n 次方程式の場合，この操作を有限回繰り返して，その結果拡大された集合にその方程式の根が含まれていれば，n 次方程式の根を冪根と四則演算で表すことができる．すなわち，n 次方程式の根の公式が存在することを意味する．このとき，$m \leq n$ として，m 乗根による拡大の操作は，繰り返してもよく，さらに操作の順番は m の大小に関わらず任意であっても構わない．これが，代数方程式の根の公式が存在するか否かという問題を数学的に取り扱うためにより具体的に表現したことになり，根の公式が存在するか否かという問題は，冪根と四則演算で拡大した集合の中に根が含まれるか否かという問題と等価であるということである．

2.2 なぜ群や体が必要なのか，可解とは，ガロア理論との関係

2.2.1 体および体の拡大とは

上で使われた有理数の集合において，任意の 2 つの数の間の四則演算の結果はまた有理数の集合の中に入る．このような集合を四則演算に閉じているという．四則演算に閉じている数の集合を「体」という．たとえば，上述の有理数の集合は体である．この体という数の集合に，その中には含まれていない冪根を加えること

で元の体に含まれる数との四則演算により新しい数が増え，集合の元が増えて，それがもっと大きな体を作ることになる．これを「体の拡大」という．代数方程式を代数的に解くということは，この体の拡大を有限回数続けることによって得られた体の中にその代数方程式の根が含まれているということである．したがって，体の拡大という考えが n 次方程式を代数的に解くということと密接に関係していることがわかる．

2.2.2 可解とは

では，代数方程式の根が拡大された体の中に含まれているか否かを明らかにするにはどのようにこれを解析すればよいのか，という問題が残る．これを明らかにしたのがガロアである．ガロアの理論はこのような体の拡大という考えを出発点にしている．上で述べたような，冪根を加えることによって拡大された体が根を含んでいるとき，このような体を，解くことができるという意味で,「可解」であるという．二項方程式 $x^n - a = 0$ のような場合，上の例と同じように有理数の冪根で拡大された体は根を含むので可解である．

2.2.3 なぜ群が必要か

しかし，それ以外の場合，根を含む拡大された体があったとしても，それが冪根を加えて連続的に拡大された体であるか，あるいはそういう体を含むか，ということをそのままの状態で知ることができない．ガロアは，これを知るために，体を拡大するという操作の結果と拡大する前の体の間の関係において，ある種の写像に着目し，その写像を元とする群を考えたのである．すなわち，ガロアは，体を拡大したときに，もとの体の元を含まない，新しく生成された体の元のみの間の一種の置換（後で自己同型写像としてあらためて定義する）を考え，その置換の集合が群を形成する場合を考えたのである．この群の構造を解析することにより，その群が作られた元の体の拡大の性質についても，知ることができることになり，拡大された体が可解が否かが知られるのである．これはガロアの主定理あるいはガロアの基本定理と呼ばれ，本解説の後半で具体的に述べる．このような群はガロア群と呼ばれ，ガロア理論の中核をなしている．したがって，方程式が代数的に解けるかという問題において，群や体を扱うことは必須のことなのである．

2.2.4 ガロア群の意味

ガロア群およびその定義については後で述べる．体を次々に拡大したときに，その一連の拡大の一つ一つに対応してガロア群が定義され，一連のガロア群が生成される．一連の体の拡大が冪根による拡大の場合に，その体の系列は可解であるということだった．そのとき，対応する一連のガロア群も特別な性質をもつことになる．この特別な性質とは，後で述べる巡回群という性質であるが，それが備わっているとき，そのガロア群は可解といわれる．すなわち，体を拡大したときに，そのガロア群が可解であれば，方程式は代数的に解くことができて，根の公式が存在するということになるのである．したがって，根の公式が存在するか否かという問題は，ガロア群を調べることに尽きるのである．

代数方程式の解がわからない状態で，その解を含む体の拡大は定義できるが，具体的にどのような体であるのかはそれ以上明らかにすることはできない．ところが，その拡大のガロア群は同様に定義できるだけではなく，ガロア群が具体的に定まり，その分析ができるのである．そのため，そのガロア群が可解という性質をもつか否かがその分析によって明らかになる．これがガロア群を導入することの意味である．ガロアが導入した群がこのように使われるということがガロア群の面白いところである．

2.2.5　その他の難解なところ

以上のような筋道に沿って，ガロア理論を追っていくと，難しいところが何箇所か出てくる．例えば，代数方程式の根が体を有限回拡大しても本当に含まれているかという問題がある．これについては，代数学の基本定理により，n 次方程式には複素数解，重複解も含めて n 個の解が存在するということがわかっている．複素数体でない場合は複雑になるのでこの解説ではそこまでは述べない．また，根が重複する場合の問題もあるが，これも実数体を係数とする既約多項式の場合はすべての根が分離的になるので，この問題についてもそれ以外の場合は述べない．また，代数方程式には因数分解できるものも含まれるので，そのような場合も含めて一般に方程式が解けないと証明するのは無理がある．したがって，代数方程式の係数が特別な代数的関係を持たないということが必要になるが，そのような一般性を保持するために，係数を変数にするという処理が用いられる．ガロア理論を適用するために，そのような代数的な基盤が用意されていないといけない．これについても後に触れる．

以下では，このようなあらすじに沿って体の拡大とガロア群および可解という性質を具体的に順を追って述べることにする．

3　群および体

体の拡大について具体的に述べる前に，群および体の定義をしておく．また，正規部分群や剰余群など，必要な基礎知識についても述べる．

3.1　群

3.1.1　群の定義

集合とは数学的に定義されたものの集まりで，その要素を元という．群とは集合の一つで，元の間に演算が定義され，その演算のもとで，単位元，逆元をもち，結合則を満たすものをいう．演算記号を，数変数の乗法のように，ここでは省略する．演算といっても，数の乗法でもよいし，単なる置換の連続でも演算とみなすことができることに注意する必要がある．ただし，演算が加法のときには $+$ を用いる場合がある．群を G とすると，上のことは以下のように表される．

(1) G は演算に対して閉じている．すなわち，G の任意の元を a および b とすると，a および b に対し，G の中にある元 c が存在して，

$$ab = c \tag{2}$$

が成り立つ．

(2) 単位元が存在する．すなわち，e を G の単位元とすると，G の任意の元 a に関して，

$$ae = ea = a \tag{3}$$

が成り立つ．

(3) 逆元が存在する．a を G の任意の元とする．a の逆元を a^{-1} と表すとき，

$$a^{-1}a = aa^{-1} = e \tag{4}$$

が成り立つ.

(4) 結合則が成り立つ．すなわち，a, b, c を G の任意の元とすると，

$$(ab)c = a(bc) \tag{5}$$

が成り立つ.

3.1.2 可換群

a, b を G の任意の元とする．そのとき，演算において，

$$ab = ba \tag{6}$$

が成り立てば，G の演算が可換であるという．一般に，群の演算は可換ではない．可換な群を可換群という．アーベル群ともいう.

3.1.3 位数

群の元の数を位数という．元に対して用いる位数，すなわち元の位数は意味が異なり別に定義があるので，区別しなければならない．したがって，群の位数あるいは G の位数というように明示する必要がある.

3.1.4 部分群と単純群

群 G の中の部分集合 H が上述の群が満たす要件 (1)〜(4) を満足していれば，H は群 G の部分群という．明らかに，部分群と元の群の単位元は共通である.

単位元と G 自身は部分群である．この 2 つの部分群を自明な部分群という．単位元と G 自身以外に部分群をもたない群を単純群という.

部分群 H の位数は G の位数の約数である．これはラグランジュの定理とよばれる.

3.1.5 正規部分群

H を群 G の部分群とする．a を G の任意の元，b を H の任意の元とする．そのとき，aba^{-1} が H に属すれば H を正規部分群という.

単位元と G 自身は正規部分群である.

正規部分群は，体の拡大の系列があり，一方で対応する群の系列があるときに，ガロア群となるための条件を示すときに現れる.

3.1.6 剰余類と剰余群

剰余群は，体の拡大の系列があって，それに対応する群の系列があるときに，その群の系列間において用いられる性質である．これは，群が可解である条件において重要な役割を果たす．具体的な定義は以下の通りである.

H を群 G の部分群とする．h を H の任意の元，g を G のある元とする．このとき，hg のすべての元からなる集合を H の剰余類という．もし，g が H に属するならこの剰余類は H 自身である．

異なる剰余類は共通部分をもたない．群 G の位数を n，部分群 H の位数を m，剰余類の数 k とすると，$n = mk$ である．k を部分群 H の指数という．

H が正規部分群の場合を考える．H と G の元 g_1 で作られる剰余類を Hg_1 と表すことにする．Hg_2 も同様である．剰余類 Hg_1 および Hg_2 について，H の任意の元を h_1 および h_2 とすると，$h_1g_1h_2g_2$ は剰余類 Hg_1Hg_2 に属する（証明は後述）．これから，剰余類 Hg_1 と Hg_2 の積 Hg_1Hg_2 を定義することができる．その結果，剰余類が群を形成する．これを群 G の正規部分群 H に関する剰余群といい，G/H と表す．

3.2 体

3.2.1 体の定義

体とは，任意の 2 つの元の間に乗法と加法に相当する演算が定義され，かつその演算に閉じた集合で，それぞれの演算において，単位元および，乗法の 0 を除いて逆元が存在し，結合則と分配則が成り立つものをいう．すなわち，体では以下の (1)〜(4) が満たされる．

(1)a および b を体 P の任意の元とすると，積 ab および和 $a + b$ は P に属する．

(2)P は乗法の単位元 1 と加法単位元 0 を含む．

(3) a を P の任意の元とすると，P は，乗法の逆元 a^{-1} $(a \neq 0)$ および加法の逆元 $-a$ を含む．

(4) P の任意の元 a, b, c について，

$$a(bc) = (ab)c, \qquad a(b + c) = ab + ac \tag{7}$$

が成り立つ．

実数の集合 $\mathbb{R}$，有理数の集合 $\mathbb{Q}$, 複素数の集合 $\mathbb{C}$ は体である．

3.2.2 標数

法 n による演算を考えると，この数の集合は $0, 1, \cdots, n-1$ に限られる．このような集合でも体を形成する．有限な体においては，単位元を e とすると，$ne = 1$ である．一般に，$ne = 1$ が成り立つ n で最小の数 p を標数という．$p > 0$ なら，その体は有限である．

$ne = 1$ が成り立つ n が存在しない体の標数は 0 とされる．実数や複素数などの標数は 0 である．本文では標数 0 の体のみを扱う．

4 体の拡大

すでに第 2 節で述べたように，体 P に新しい元を 1 個または複数個加え，その元を含む任意の元の間の四則演算によって得られるすべての数を P に加えることによって新たに体を生成することを体の拡大といい，得られた体を拡大体という．この拡大体を K としよう．P に追加される数 α が P の元を係数とする n 次多項式の根であるとき，n 次の拡大といい，拡大体という．そのとき，$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ が基底となり，K の任意の

元はこれらの基底の 1 次結合として表される．なお，上において，α^n 以上の高次の項は n 次多項式を用いて α^{n-1} 以下の低次の項に変換される．

体の拡大という概念はガロアの理論において重要な概念である．特に，ガロア拡大と呼ばれる拡大においては，正規拡大と分離拡大という 2 つの概念が重要である．

4.1 部分体と拡大体, および中間体

体 P が体 K に含まれる場合，すなわち $P \subset K$ なら，P は K の部分体といい，K は P の拡大体といい，この拡大を K/P と表す．$P \subset M \subset K$ となる体 M を中間体という．

4.2 体の拡大と基礎体

一定の体の上の拡大を扱うときに，このもとの体を基礎体という．同じように，複数の拡大体を作るときに基準となる体，あるいは，いくつかの拡大体が共通にもつ体を基礎体という．本文では，基礎体として主に P を用いる．

4.3 拡大体の種類

ここでは拡大の次元を有限とする．

拡大体の生成の仕方やその具体的な定義に従い，以下のような拡大体の種類がある．拡大体の種類がこの後ですべて利用されるわけではないが，拡大体の多様性と柔軟性ならびに関係性を示すために述べることにする．

4.3.1 代数的拡大体

体 K を体 P の拡大体とする．K の元が P の元を係数とする多項式の根として表されるとき，この元を代数的であるという．このような拡大体を代数的拡大体という．

以下の 4.3.2 節から 4.3.5 節の拡大体は代数的拡大体であり，かつ，すべて等価である．

4.3.2 有限拡大体

体 K を体 P の拡大体とする．K の任意の元 β が，K の元 $\alpha_1, \cdots, \alpha_n$ と P の元 $b_1, \cdots, b_n$ を用いて，

$$\beta = b_1\alpha_1 + \cdots + b_n\alpha_n \tag{8}$$

のような形に一意的に表されるとき，K は P の有限拡大体という．$\alpha_1, \cdots, \alpha_n$ を基底という．

このとき，K は P の上の線形空間とみなすことができる．その場合，n は線型空間の次元であり，これを P の上の拡大体 K の次数といい，$[K : P]$ と表す．すなわち

$$n = [K : P] \tag{9}$$

である．

有限拡大体は代数的拡大体である．K の次元を n とする．K の任意の元を β とする．そのとき，$\beta^0, \beta^1, \beta^2, \cdots, \beta^n$ の $n+1$ 項は 1 次従属である．したがって，P のある元の組み合わせ $b_0, b_1, b_2, \cdots, b_n$ を用いて，

$$b_0\beta^0 + b_1\beta^1 + b_2\beta^2 + \cdots + b_n\beta^n = 0 \tag{10}$$

とすることができる．これは β が P の元を係数とする x の多項式

$$b_0 + b_1x + b_2x^2 + \cdots + b_nx^n \tag{11}$$

の根であることを意味するから，結局，有限拡大体は代数的拡大体であるを示している．

体 P も P の拡大体とみなすことができる．そのときの拡大次数は 1 である．

最小多項式

式 (11) が P の元を係数とする多項式で因数分解できない場合，すなわち規約である場合，このような式を K の元 β の最小多項式という．

4.3.3 代数的単純拡大体

体 P に含まれない代数的な数 α と P の元のあらゆる組み合わせによる四則演算によって得られる数を追加して得られる体を代数的単純拡大体という．これを $P(\alpha)$ と記す．

α は代数的な数であるから，α を根とする多項式が存在する．そのうちの最小多項式を $f(x)$，その次数を n とする．すべての K の元はある多項式の根であるから，その多項式を $f(x)$ で割った剰余は次数が $n-1$ 以下の多項式である．つまり，その元は α の $n-1$ 次以下の多項式で表される．すなわち，すべての元は P の元を係数として，$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ の 1 次式で表すことができる．これは，K の基底が $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ であることを意味する．これから，代数的単純拡大体の次数 $[P(\alpha) : P]$ は n である．

代数的単純拡大を簡単に単拡大という場合もある．

4.3.4 代数的生成拡大体

体 P の上に，P に含まれない数 $\alpha_1, \cdots, \alpha_n$ と P の元のすべての組み合わせの四則演算によって得られた数を加えて得られる最小の体を P の代数的生成拡大体といい，$P(\alpha_1, \cdots, \alpha_n)$ とかく．代数的単純拡大体は代数的生成拡大体の $n = 1$ の場合である．

$P(\alpha_1, \cdots, \alpha_n)$ の基底は一般に $\alpha_1^i\alpha_2^j \cdots \alpha^l$ のような形式の項になる．$i, j, \cdots, l$ などは，それぞれの α_k の最小多項式の次数よりも小さい．

4.3.5 代数的組成拡大体

代数的単純拡大体 $P(\alpha_1)$ を L_1 とする．同様に，L_1 の代数的単純拡大体 $L_1(\alpha_2)$ を L_2 とし，以下同様にして，L_{i-1} の代数的単純拡大体 $L_{i-1}(\alpha_i)$ を L_i とし，L_n の拡大体を定義する．この L_n を $P(\alpha_1)(\alpha_2)\cdots(\alpha)$ とかく場合もある．P の拡大体を K とし，P と K の中間体を L とする．これらの拡大体の次数には次の関係がある．

$$[K : P] = [K : L][L : P] \tag{12}$$

上の代数的組成拡大体の場合は

$$[L_n : L_0] = [L_n : L_{n-1}][L_{n-1} : L_{n-2}] \cdots [L_2 : L_1][L_1 : P] \tag{13}$$

である．

第 2 節で述べた，連続した冪根拡大体はこの代数的組成拡大体に含まれる．

4.4 ガロア拡大

第 2 節で述べたように，連続した冪根拡大体が多項式の根を含む拡大体を含むか否かを知ることが目的である．その，多項式の根をすべて含む拡大体を生成する体の拡大がガロア拡大である．これをもう少し詳しく述べると以下のようになる．

根の公式の有無を考える多項式はここでは最小多項式と考えてよい．そのとき，この最小多項式の根がすべて含まれる体への拡大がガロア拡大である．ただし，最小多項式は重根を含まないとする．

代数的生成拡大体において考えれば，$\alpha_1, \alpha_2, \cdots, \alpha_n$ がすべて異なり，それらの最小多項式が共通でかつ，最小多項式の根をすべて尽くしている場合，この代数的拡大を特にガロア拡大という．

共通の最小多項式を $f(x)$ とすると，$f(x)$ は体 P の上の，すなわち P の元を係数とする，既約な n 次多項式で，その根は，$\alpha_1, \alpha_2, \cdots, \alpha_n$ であり，いずれも重根と異なる．この拡大の次数は $n!$ である．この証明は後述するが，拡大の次数が 4.3.4 節の代数的生成拡大体の場合と異なっている．これは，ガロア拡大の場合には最小多項式が共通であるのに対し，後者では最小多項式が独立であることによる．

ガロア拡大は，正規拡大でかつ分離拡大と定義することができる．それぞれの拡大は以下に定義される通りであるが，以下に示されているように，有理数体や実数体のような標数 0 の体の場合，最小多項式が既約な場合はこれが満たされるので，正規拡大がガロア拡大になる．

正規拡大

α と β が同じ最小多項式の根であるとき，両者を互いに共役であるという．

体 P の拡大 K とする．K の元 α の最小多項式が K において 1 次式の積に分解されるとき，この拡大を正規拡大という．明らかに，正規拡大体は最小多項式の根をすべて含む．同じことであるが，正規拡大体は α と共役な元をすべて含む．

分離拡大

K を P の代数拡大とする．K の元 α の P 上の最小多項式を $f(x)$ とする．$f(x)$ が重根を持たないとき，$f(x)$ を分離的という．そのとき，α を P 上分離的という．K のすべての α が分離的であるとき，K/P を分離拡大という．

重根を持たないことは，$f(x)$ と $f'(x)$ が互いに素であることと同値である．これから，標数 0 の体では，既約な多項式はすべて分離的である（証明は後述）．このような体を完全体という．有理数体 $\mathbb{Q}$，実数体 $\mathbb{R}$，複素数体 $\mathbb{C}$ などは完全体である．$\mathbb{Q}$ の上のガロア拡大は，それだけで分離的であることが満たされているので分離拡大であることを特に示す必要はない．

4.5 分解体

P の元を係数とする多項式を P の上の多項式という．P の上の規約多項式で重根をもたない場合，それを $f(x)$ とすると，$f(x)$ の根をすべて含む P の最小の拡大体を $f(x)$ の分解体という．いまの場合，P として標数 0 の体を考えているから，P の上の既約多項式は重根を持たない．したがって，分解体はガロア拡大である．

5 準同型写像

5.0.1 体の間の写像

いま，体 A と体 B があるとする．体 A から体 B への写像 ϕ とは，A の元 a が体 B の元 b に変換されることである．ϕ によって A の元がすべて B の元のいずれかに変換され，すべての B の元が A のある元 a を用いて $\phi(a)$ と表されるとき，この写像は全射であるという．$\phi(a) = b$ であるとき，b に対して，こうなる a がただ一つしかないときこの写像は単射であるという．全射で，かつ単射の場合は全単射という．ϕ が定義されれば任意の元に対して写像による変換が確定する．

5.0.2 準同型写像の条件

ガロア拡大で生成された拡大体の自分自身の間の全単射写像から構成されるのがガロア群であるが，このガロア群を構成するための条件がある．その中で，最も重要なものが準同型写像という条件である．この条件は制約が大きく，場合によっては，これを満たす写像は恒等写像のみということもあるくらいである．以下では，この準同型写像について述べる．

A と B を体とし，A の元を B の元に結びつける写像で，すなわち A から B への写像 φ において，a と b を A の元とし，次の関係式を満たす写像を準同型写像という．

$$\varphi(a+b) = \varphi(a) + \varphi(b) \tag{14}$$

$$\varphi(ab) = \varphi(a)\varphi(b) \tag{15}$$

この写像では，2 つの体の間で演算の構造が保存されるという意味をもつ．

2 つの環の間のこのような写像を特に環準同型写像，あるいは簡単に準同型という．2 つの体の間の写像であることを特に示すときは体準同型という．

写像が 1 対 1 のときは単射，B のすべての元が A の元の写像であるときを全射，単射かつ全射の場合を全単射といい，その場合の準同型写像を同型写像という．A から A 自身への同型写像を自己同型写像という．この自己同型写像がガロア群のところで重要な役割を担う．

準同型写像は，演算の構造を保存しているために，2 つの集合の間の単なる対応関係では成り立たない．例として，有理数体 $\mathbb{Q}$ に $\sqrt{2}$ を加えて生成された拡大体から自分自身への準同型写像を考えよう．これはすなわち，$\mathbb{Q}(\sqrt{2})$ の間の準同型写像になる．単なる写像として，$\mathbb{Q}(\sqrt{2})$ の元に $\sqrt{2}$ が含まれているときには $\sqrt{2}+1$ と交換し，それ以外は同じままにするという写像 ϕ を考える．そのとき，$a_1 + b_1\sqrt{2}$ と $+\ a_2 + b_2\sqrt{2}$ の積を考えてみよう．一般に，$\phi(a + b\sqrt{2}) = a + 1 + b\sqrt{2}$ となるので，

$$\begin{aligned}\phi((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) &= \phi((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}) \\ &= (a_1a_2 + a_1b_2 + a_2b_1 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\end{aligned} \tag{16}$$

となるのに対し，

$$\begin{aligned}\phi(a_1+b_1\sqrt{2})\phi(a_2+b_2\sqrt{2}) &= (a_1+b_1+b_1\sqrt{2})(a_2+b_2+b_2\sqrt{2}) \\ &= (a_1a_2+a_1b_2+a_2b_1+3b_1b_2)+(a_1b_2+a_2b_1+2b_1b_2)\sqrt{2} \end{aligned} \tag{17}$$

であるから，明らかに式 (??) が満足されない．したがって，この写像は準同型写像にはならない．なお，式 (??) に関してはこの写像でも成り立つ．

上の写像をもっと一般に

$$\phi(\sqrt{2}) = c + d\sqrt{2} \tag{18}$$

と定義すると，$\phi(a+b\sqrt{2}) = a+bc+bd\sqrt{2}$ のように変換される．これから，上と同じような計算により，ϕ が準同型写像になるのは，$c=0$ かつ $d=\pm 1$ のときだけであることがわかる．結局，$\mathbb{Q}(\sqrt{2})$ の間の準同型写像 σ は，$\sigma(\sqrt{2}) = \sqrt{2}$ と $\sigma(\sqrt{2}) = -\sqrt{2}$ の 2 つしかないことがわかる．

同じような例として，有理数体からの拡大体 $\mathbb{Q}(\sqrt{2})$ と $\mathbb{Q}(\sqrt{3})$ の間の準同型写像を考えると，上のような考察をして，結局，準同型写像はないことがわかる．もちろん，恒等写像すら存在しないことがわかる．このような場合もあるほど，準同型写像には制約の大きい条件が付随している．

6 二項拡大体

6.1 二項方程式，二項拡大体

第 2 節で述べたように，代数方程式の根の公式の有無は，四則演算と冪根を用いた拡大体がこの多項式の根を含むか否かということと同値である．したがって，これからはこの拡大体を追求することになる．この体は，1 回の冪根演算に伴う体の拡大を有限回繰り返して得られる．このときの 1 回の拡大で生成されるのが以下に述べる二項拡大体である．したがって，二項拡大体の成り立ち，構造を知ることは重要である．ここでは，この二項拡大体の基本的な特徴を述べる．この特徴から，拡大体が解をふくむこと，すなわち可解性との関係が得られる．この過程でガロア群との関係が密接になってくる．その自然な流れの中でガロア群が導入されるのである．

二項方程式は，

$$x^n - \alpha = 0 \tag{19}$$

と表される．α は基礎体 P の元である．この二項方程式の根を体 P に加える拡大を考える．このとき，この二項方程式は α の最小多項式である．こうして得られる拡大体は二項方程式 (16) の分解体である．この拡大体を二項拡大体という．式 (19) の解は，

$$\theta,\ \theta\gamma,\ \theta\gamma^2,\ \cdots,\ \theta\gamma^{n-1} \tag{20}$$

である．ここで，$\theta = \alpha^{1/n}$ とする．γ は 1 の原始 n 乗根で，$\gamma = \exp(2\pi\mathrm{i}/n)$ である．θ は式 (16) の解の 1 つで，γ は 1 の原始 n 乗根の 1 つとして構わないがここでは上のようにおく．これから，二項拡大体は P に θ と γ および P のあらゆる組み合わせの四則演算を加えて得られる最小の体ということになる．すなわち，代数的生成拡大体 $P(\theta,\gamma)$ である．この拡大体を K と表すことにする．ここで，体 K から K 自身への次のような自己同型写像を考えることにしよう．ここからがガロア理論の中に入るといえる．

6.2 自己同型写像と固定体

6.2.1 固定体

体 K を基礎体 P からの代数的拡大とする．体 K から体 K 自身への写像を考える．この写像では，体 K の元が K 自身の別の元または同じ元へ一対一に変換され，かつ K のすべての元が写像の始集合となり，かつ終集合となるとする．すなわち全単射写像を考える．さらに，ここでは基礎体 P の元はそのまま不変に保ち，それ以外の K の元を別の K の元に変換するような写像を考えることにする．つまり，P に関しては恒等写像であるような全単射を考える．これを，始集合を P に制限したときに恒等写像になる全単射ということもできる．このように，K から K への全単射写像に際して不変に保たれる部分体を固定体とよぶ.

6.2.2 拡大体 K から自分自身 K への写像

上のような P を不変に保つ写像において，個々の元の変換としては，K に拡大したときに P に付加された生成元の間の変換のみを考えればよい．なぜなら，このような写像には，P の元から K の生成元へ変換されたり，K の生成元から P の元に変換されたりする元の変換は含まれないからである．新たに生成された K の元，すなわち P に含まれない K の元は，一般に，K の生成元の多項式で係数が P の元であるものか，あるいはそうした多項式の商となるが，そのとき係数となる P の元は写像に際して変化しない．したがって，P の元を不変に保つ写像の場合は，K への拡大における生成元の間だけの変換のみを考慮すればよいことがわかる．

拡大体が分解体の場合は，生成元となる最小多項式のすべての根について，全部またはそのいくつかの根を互いに交換する変換から構成される写像をすべて考慮すればよいということになる．K のすべての元は上の生成元と P の元のあらゆる四則演算の結果であるから，任意の元の写像先は，このような変換によって一意的に決定されることがわかる．逆写像も同じように一意的に決定される．したがって，こうして得られる写像は全単射であることがわかる．

6.2.3 準同型写像の条件

K から K への自己全単射において，写像に関して何も条件がなければ単なる一対一対応を考えればよく，一般には組み合わせの数だけあるが，ここでは，準同型条件を満たす全単射を考えなければならない．準同型条件を満たすということは，演算の構造を保存するという意味であり，異なる体の間の準同型は，一方の演算構造を他方に埋め込むことから，埋め込みと呼ばれる．いまの場合，同じ体の間の写像であるから，もともと演算構造も同じであり，準同型条件を満たすことはなかば必然といってもよい.

したがって，以上のような全単射が式 (14), (15) の準同型写像の条件を満たすことを示す必要がある．このとき，次の 2 通りの場合がある．1 つは，K の生成元の間に代数的な関係がなく代数的に独立な場合である．このときは，2 つの生成元の和または積はそのままで変わることがなく，変数のように扱ってよいことになる．代数的に独立であることと，そのような独立な係数をもつ多項式を一般多項式として，ガロア群を多項式の根の代数的解法の有無の判定に用いることは後述する.

もう 1 つは，K の生成元の間に代数的な関係が存在し，生成元の間の和または積がそれ以外の生成元になるような場合である．このときは，生成元となる根を具体的に明らかにし，その上に立って準同型写像を構成する必要がある．このような場合に，条件を満足する全単射は単純ではない．ここで述べている二項拡大体がその場合に該当し，その根についてはすでに述べたが，その 2 つの根の積は別の根になる．このような根から構成される準同型写像はこの後で述べる.

生成元が代数的に独立な場合の全単射が準同型条件を満たすことを以下に示す．全単射を ϕ と表す．一般に K の元は，P の元を係数とし，生成元 $\alpha_1, \cdots, \alpha_n$ を多変数とする多項式として表すことができる．この多項式を $f(\alpha_1, \cdots, \alpha_n)$ と表すことにする．これに ϕ を作用させると $g(\alpha_1, \cdots, \alpha_n)$ に変換されることになる．g は f の変数 α_i を α_j に変換した関数である．すなわち，ϕ による K の元 f の写像先 g は，単に変数 $\alpha_1, \cdots, \alpha_n$ 置換であるから，

$$\phi(f(\alpha_1, \cdots, \alpha_n)) = g(\alpha_1, \cdots, \alpha_n) \tag{21}$$

と表される．同様に，K の元 f_1 と $g1$ の写像先をそれぞれ g_1 と g_2 と表すと，

$$\begin{aligned} \phi(f_1(\alpha_1, \cdots, \alpha_n) + f_2(\alpha_1, \cdots, \alpha_n)) &= g_1(\alpha_1, \cdots, \alpha_n) + g_2(\alpha_1, \cdots, \alpha_n) \\ &= \phi(f_1(\alpha_1, \cdots, \alpha_n)) + \phi(f_2(\alpha_1, \cdots, \alpha_n)) \qquad (22) \\ \phi(f_1(\alpha_1, \cdots, \alpha_n) f_2(\alpha_1, \cdots, \alpha_n)) &= g_1(\alpha_1, \cdots, \alpha_n) g_2(\alpha_1, \cdots, \alpha_n) \\ &= \phi(f_1(\alpha_1, \cdots, \alpha_n))\phi(f_2(\alpha_1, \cdots, \alpha_n)) \qquad (23) \end{aligned}$$

となることは明らかであるから，ϕ は準同型条件を満たし，同型写像であることがこれで示される．したがって，上で述べた，P を不変とする K から K への全単射は同型写像であり，かつ自己同型であることが示された．

6.2.4 自己同型群

上で示された P を固定体とする K の自己同型写像の集合は群となる．実際，これは以下のように示される．まず，上のような自己同型の 2 つの写像を ϕ，ψ とすると，それぞれは全単射であるから，ϕ の終集合は ψ の始集合に一致する．したがって，ϕ の写像元を a，ϕ の写像先を b，ψ の写像元を b，ψ の写像先を c とすると，ϕ を作用させた後に ψ を作用させると，写像元 a から写像先 c は一意的に決まる．したがって，これを 2 つの写像の積 $\phi\psi$ の写像元および写像先とすれば，ϕ と ψ の演算を定義することができる．明らかに $\phi\psi$ は K の自己同型となるから，もとの自己同型の集合に含まれる．一方，$\phi\psi$ も全単射であるから，写像元 c から写像先 a への全単射が定義されるから，逆写像が存在する．さらに，明らかに恒等写像も存在するので単位元となる．結局，群の条件が満たされるのである．このような自己同型写像からなる群を自己同型群という．

しかしながら，以上は K の生成元が互いに代数的に独立な場合に成り立ち，生成元の間の積が別の生成元になる場合にはこのように単純には準同型規則は成り立たない．自己同型写像は基本的に最小多項式の根の間の写像で決定されるので，2 つの根の間の積が他の根に変換される場合は十分考えられ，その場合は上のようには準同型規則が成り立たなくなる．その典型的な例が以下で扱う二項拡大体の場合である．

6.3 二項拡大体の準同型と自己同型群

6.3.1 二項拡大体の基底

二項拡大体 $P(\theta, \gamma)$ の基底は生成元 θ と γ から生成される．まず，θ は $x^n - \alpha = 0$ の根であるから，n 次元の基底を作る．すなわち，$1, \theta, \cdots, \theta^{n-1}$ である．次に，γ は $x^n - 1 = 0$ の根であるから，原始 n 乗根である．$x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$ となり可約であるから，最小多項式は $(x^{n-1} + \cdots + x + 1$ となり，γ^i は $n-1$ 次元の基底を作る．それぞれの基底は独立であるから，$P(\theta, \gamma)$ の基底は $\theta^i \gamma^j$ $(i = 0, \cdots, n-1;\ j = 0, 1, \cdots, n-2)$ となる．具体的には，

$$1, \theta, \gamma, \theta\gamma, \theta^2\gamma, \theta^2\gamma^2, \cdots, \theta^{n-1}\gamma^{n-2}$$

のようになる．

6.3.2 二項拡大体の単純な写像

二項拡大体の生成元のもととなる二項方程式の根は式 (20) で示される．これを α_i と表すことにする．すなわち，

$$\alpha_i = \theta\gamma^i \tag{24}$$

とし，$\alpha_0 = \theta$ とする．α_i と α_j の積は

$$\alpha_i\alpha_j = \theta^2\gamma^{(i+j) \mod n} \tag{25}$$

となるここで，φ を自己全単射としてとして α_i から α_{i+2} へ変換する写像を取り上げてみよう．すなわち，

$$\varphi(\alpha_i) = \theta\gamma^{(i+2) \mod n} = \alpha_{i+2 \mod n} \tag{26}$$

である．しかし，この単純な置換の全単射では (14) は成り立たないことがわかる．実際，$\varphi(\alpha_i\alpha_j)$ は，

$$\varphi(\alpha_i\alpha_j) = \theta^2\gamma^{(i+j+2) \mod n} \tag{27}$$

となり，一方，$\varphi(\alpha_i)\varphi(\alpha_j)$ は

$$\varphi(\alpha_i)\varphi(\alpha_j) = \theta\gamma^{(i+2) \mod n}\,\theta\gamma^{(j+2) \mod n} = \theta^2\gamma^{(i+j+4) \mod n} \tag{28}$$

となるので $\varphi(\alpha_i\alpha_j)$ と $\varphi(\alpha_i)\varphi(\alpha_j)$ は等しくならない．二項拡大体の場合はこのような単純な全単射では準同型規則は成り立たないのである．

6.3.3 二項拡大体の 2 重演算子写像

式 (20) は二項方程式の根であり，二項拡大体の基底の一部である．二項拡大体の基底については後述する．この n 個の根の置換を二項拡大体の自己全単射とし，それが準同型の条件を満たすためには，以下のような方法がある [1]．この方法では，写像の変換元を式 (24) の $\theta\gamma^i$ から $\theta^j\gamma^i$ のように一般化し，これに作用することによって 2 つの整数変数 i と j が変化して別の $\theta^{j'}\gamma^{i'}$ に変換される演算子 $\sigma[a]$ および $\tau[b]$ を導入する．すなわち，この全単射では 2 つの演算子による 2 重の演算を考えるのである．a と b は整数のパラメータである．$\sigma[a]$ は γ のみに作用して，他の因子は変わらない変換であり，$\tau[b]$ は θ のみに作用し，それ以外の因子には作用しない．このような全単射は $\sigma[a]\tau[b]$ という演算子の積になる．

具体的には以下のようになる．まず $\sigma[a]$ の変換の定義は次式で表される．

$$\sigma[a](\gamma) = \gamma^a, \tag{29}$$

$$\sigma[a](\gamma^i) = (\sigma[a]\gamma^a)^i = \gamma^{ai} \tag{30}$$

と定義される．ここで，a は 1 から $n-1$ までの整数，i は整数である．つまり，σ により γ は a 乗される．

もう一つの演算子 $\tau[b]$ の変換の定義は

$$\tau[b](\theta) = \tau\gamma^b, \tag{31}$$

$$\tau[b](\theta^j) = (\tau[b](\theta))^j = (\tau\gamma^b)^j = \theta^j\gamma^{bj} \tag{32}$$

である．ここで，b は 0 から $n-1$ までの整数，j は整数である．この変換により，θ は $\theta\gamma^b$ に変わる．別の言い方をすれば，θ は変わらず，θ に因子 γ^b が追加されるとみてもよい．

式 (20) から明らかなように，γ の指数は n を法とする整数演算になる．また，$\theta^n - \alpha = 0$ という関係から θ は $n-1$ 次であるので，$j = 0, \cdots, n-1$ までを考えれば十分である．$a = 0$ の場合は，写像元が異なる i で

も写像先が $ai = 0$ となって等しくなり単射ではなくなるから除かれる．したがって，i, j, b は 0 から $n-1$ までの整数，a は 1 から $n-1$ までの整数である．

$\sigma[a]$ と $\tau[b]$ を同時に $\theta^j\gamma$i に作用させると，

$$\sigma[a]\tau[b](\theta^j\gamma^i) = \tau[b](\theta^j)\sigma[a](\gamma^i) = \theta^j\gamma^{bj}\gamma^{ai} = \theta^j\gamma^{bj+ai} \tag{33}$$

となる．この式から明らかなように，写像元の i，j が異なれば，写像先の $bj + ai$ も異なるから，この写像は単射であることがわかる．簡単のために，

$$\sigma[a]\ \tau[b] \equiv [a, b] \tag{34}$$

と表すことにする．そうすると，上の関係は，

$$[a, b](\theta^j\gamma^i) = \theta^j\gamma^{bj+ai} \tag{35}$$

と表される．σ と τ を単独で表すには，

$$[a, 0](\theta^j\gamma^i) = \theta^j\gamma^{ai} \tag{36}$$

$$[1, b](\theta^j\gamma^i) = \theta^j\gamma^{bj+i} \tag{37}$$

とすればよい．

このように定義した K から K への自己全単射が準同型条件を満たすことは以下にように示すことができる．まず，$p = \theta^i\gamma^j$，$q = \theta^k\gamma^l$ とすると，

$$[a, b](pq) = [a, b](\theta^i\gamma^j\theta^k\gamma^l) = [a, b](\theta^{i+k}\gamma^{j+l}) = \theta^{i+k}\gamma^{b(i+k)}\gamma^{a(j+l)}) = \theta^{i+k}\gamma^{a(j+l)+b(i+k)} \tag{38}$$

である．一方，

$$[a, b](p)[a, b](q) = [a, b](\theta^i\gamma^j)[a, b](\theta^k\gamma^l) = \theta^i\gamma^{bi}\gamma^{aj}\ \theta^k\gamma^{bk}\gamma^{al} = \theta^{(i+k)}\gamma^{a(j+l)+b(i+k)} \tag{39}$$

となり，$[a, b](pq) = [a, b](p)[a, b](q)$ となり，写像 $[a, b]$ に関する準同型規則式 (15) が成り立つのである．式 (14) が成り立つのは明らかである．

以上述べた K の間の写像が全単射になっていることを確認しておこう．上の写像は，二項拡大体の基底の間の置換になっている．この基底は後述するが，二項方程式の根を含んでいる．K の基底以外の元を K の自己全単射の写像元とした場合，これらの元が P の元と基底との間の四則演算で決定し，一方 P の元は不変に保持されるので，基底の変換が決定した段階で写像先は一意的に決定する．したがって，すべての 1 対 1 写像が一意的に決まる．さらに，基底以外の K の元も含めてすべて写像の始集合になっているから全射でもあり，これにより全単射であることが確認できる．

以上から，写像 $[a, b] = \sigma[a]\tau[b]$ は P を固定体として K から K への自己同型であることが示された．この自己同型の特徴は，置換される元の範囲を二項方程式の根から二項拡大体の基底まだ拡張したことである．この自己同型の数は，単なる組み合わせとは異なり，次節で述べるように $n(n-1)$ と制限された数になる．最小方程式の根が代数的に独立な場合には，根の間の置換が組み合わせの数 $n!$ だけ自己同型になるのと比較すると大きな違いがあることがわかる．具体的な内容は次節で述べる．

6.3.4 写像 $[a, b]$ に関して

この写像の一番の特徴は，二項方程式の根の集合から自分自身へ単純な置換による写像ではなく，二項拡大体の基底の集合から自分自身への 1 対 1 準同型写像になっていること，すなわち自己同型になっていることで

ある．具体的にみると，$[a,b]$ により，基底 $\theta^j\gamma^i$ は $\theta\gamma^{bj+ai}$ に写像される．a は 1 から $n-1$ まで，b は 0 から $n-1$ までの値をとるのでこの写像は $n(n-1)$ 種類あることがわかる．

γ は 1 の原始 n 乗根の 1 つで，原始 n 乗根は，$x^n-1=0$ の根のうち 1 を除く $x^{n-1}+x^{n-2}+\cdots+x+1=0$ の $n-1$ 個の根である．これを

$$\gamma_1=\gamma,\gamma_2,\cdots,\gamma^{n-2},\gamma^{n-1}$$

とすると，写像 $[1,b]$ は，γ_i を γ_{i+b} にうつす写像である．すなわち，γ_i を右側に b 個シフトする操作である．なお，添字は n を法とする．このような写像は $b=1$ から $b=n-2$ まで $n-2$ 個ある．恒等変換の $b=0$ も加えると $n-1$ 個である．

一方，$x^n-\alpha=0$ の根で P に含まれないものは，

$$\theta_0=\theta,\ \theta_1=\theta\gamma^1,\ \theta_2=\theta\gamma^2,\ \cdots,\ \theta_i=\theta\gamma^i,\ \cdots,\ \theta_{n-1}=\theta\gamma^{n-1} \tag{40}$$

の n 個である．このとき，写像 $[a,0]$ は θ_i を θ_{ai} に変換する．これは，つまり，$\theta_1,\theta_2,\theta_3,\cdots$ を式 () の添字の増える方向に $a-1$ 個おきに $\theta_a,\theta_{2a},\theta_{3a},\cdots$ に変換する．この変換の種類は $n-1$ 個あることがわかる．恒等変換も加えると n 個である．

以上の 2 個の変換を同時に施す変換が $[a,b]$ であり，その種類は $n(n-1)$ 個である．

体を拡大するため冪根と四則演算を繰り返す中で，二項拡大の中にすでに原始 n 乗根が P に含まれているような場合，すなわち，同じ n 乗根を繰り返す場合もあり得る．このような場合は，根を $\theta\gamma$ とすると，二項拡大は θ による代数拡大をすることになる．そのような場合でも根は，式 () と同じになり，

$$\theta_0=\theta,\ \theta_1=\theta\gamma^1,\ \theta_2=\theta\gamma^2,\ \cdots,\ \theta_i=\theta\gamma^i,\ \cdots,\ \theta_{n-1}=\theta\gamma^{n-1} \tag{41}$$

拡大体の自己同型写像は $[1,b]$ である．異なる写像の数は $n-1$ 個である．

式 (19) で $\alpha=1$ の場合は，二項方程式の根は原始 n 乗根である．したがって，体の拡大は γ の追加によって生成される．P に含まれない二項方程式の根は

$$\gamma_1=\gamma,\gamma_2,\cdots,\gamma^{n-2},\gamma^{n-1}$$

で，これらの根の組から自分自身への写像による自己同型写像は $[a,0]$ である．

代数方程式の根の公式が存在するということは，冪根と四則演算による体の拡大すなわち二項拡大の繰り返しによる体の拡大が方程式の根を含むことになるということである．このとき，使われる二項拡大は上に述べた 3 種類の形に限られる．

7 ガロア群

7.1 ガロア群とは

ある基礎体 P の上のガロア拡大体 K を考えよう．基礎体とはいくつかの体の拡大を考えるときにその出発点となる共通の体である．ガロア拡大とは，P の上のある最小多項式の根をすべてふくむ P の拡大であり，その拡大体はその最小多項式の分解体である．P を固定体とする K の自己同型からなる群をガロア群という．前節で定義された P の拡大体 K の自己同型 $[a,b]$ の集合は群となる．自己同型 $[a,b]$ は拡大体 K の基底のみを変換し P を不変に保つからガロア群である．

ガロア拡大があればそれに付随して必ずガロア群がある．極端な場合，K 自身も K を固定体とするガロア拡大である．そのとき，ガロア群は単位元のみからなる群である．K と P の間に中間体 M があって，M を

固定体とするガロア拡大体があればそのガロア拡大体に対応するガロア群がある．このようなガロア群がどういう意味を持つかというと，この後で説明するように，ガロア拡大体とガロア群が 1 対 1 に対応していて，拡大体の包含関係があれば，それに対応してガロア群にも部分群という包含関係があるということである．もし，体のガロア拡大において冪根による拡大という関係があれば，それがガロア群の包含関係の一定の性質に反映されることになる．拡大体に比べれば，ガロア群の性質の方がより分析しやすいので，ガロア群の系列を考えることによって，拡大体の包含関係を明らかにすることができるという意味を持つのである．つまり，根の代数解と密接な関係がある冪根拡大体の系列の有無をガロア群を調べることにより明らかにできることになる．これがガロア群の大きな意義である．

二項拡大体のガロア群について詳しく述べる前に，一般のガロア群についていくつかの性質を述べる．基礎体 P に，α_1 を加えることによって体 P を拡大する場合を考える．代数的拡大を考えると，α_1 を根とする既約多項式 $f(x)$ が存在する．ここで，$f(x)$ の係数はすべて P に属する．そのとき，$f(x)$ は次のように書くことができる．

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \tag{42}$$

$f(x)$ は既約であるから $\alpha_2, \cdots, \alpha_n$ は P に属さない K の元である．ここで，K にガロア群の 1 つの自己同型 S を体 K に施すと，K 自身は全体として何も変わらない．また，$f(x)$ の係数は P に属するので多項式 $f(x)$ も変わらない．したがって，変換 S を施すことによって，式 (44) は変わらないから，α_1 が変換 S によって行く先は $f(x)$ の根のうちの一つでなければならない．なぜなら，もし根以外の K の元に変換されれれば $f(x)$ の係数が変わることになってしまうからである．したがって，ガロア群の元 S の写像で $f(x)$ の根の写像先は，根の中だけでなければならず，かつ 1 対 1 写像でなければならないということがわかる．他の $f(x)$ の根の場合でも同じことが言える．すなわち，$f(x)$ の根を α_i $(i = 1, \cdots, n)$ とすると，S は $\alpha_1, \cdots, \alpha_n$ の 1 つの置換への写像になるということがわかる．

そのほかの K の元に関しては，それが α_i を 1 個あるいは複数個含むものであれば，その元の自己同型変換先は α_i の置換関係で自動的に決定されてしまう．もし，α_i が含まれなければ，それは基礎体 P の元であるから，変化しない．したがって，K の自己同型は $\alpha_1, \cdots, \alpha_n$ の置換の種類により一意的に決定される．

一方，K のどの自己同型も，α_i に関する部分においては上のことが成り立つので，$\alpha_1, \cdots, \alpha_n$ の置換の 1 つに対応することがわかる．つまり，P の元を係数とする既約多項式 $f(x)$ の根による拡大体 K，すなわち P の上の既約多項式の分解体 K はガロア拡大体になるが，そのガロア群の位数は $\alpha_1, \cdots, \alpha_n$ の置換の数，すなわち $n!$ であることがわかる．

以上述べたガロア拡大体 K は既約多項式の係数が代数的に独立で特別な関係がない場合である．このような多項式は一般多項式と呼ばれる．しかし，既約多項式であっても一般多項式ではない場合もあり，その場合には既約多項式の根が特別な関係をもつようになる．たとえば，二項方程式の 2 つの根の積が別の根になるような関係である．自己同型写像も単純な置換で表すことができなくなる．その例が，今まで述べた二項拡大体で，そのもととなる二項方程式では，最高次と最低次の係数が 0 であるという特別な関係がある．そのようなガロア拡大体のガロア群は，今の場合は二項拡大体のガロア群であるが，次節に示すように自己同型の間の関係を具体的に明らかにする必要がある．

7.2 二項拡大体のガロア群

まず，この自己同型写像 $[a, b]$ の間の演算を定義する．そのため，$[a, b]$ および $[c, d]$ という任意の 2 つの自己同型写像 (以下，自己同型) を取り上げ，$[a, b][c, d](\theta^i \gamma^j)$ を計算しよう．

$$\begin{aligned} [a, b][c, d](\theta^i \gamma^j) &= [a, b]([c, d](\theta^i \gamma^j)]) = [a, b][\theta^i \gamma^{di+cj}] = \theta^i \gamma^{bi+a(di+cj)} = \theta^i \gamma^{(b+ad)i+acj} \\ &= [ac, ad + b](\theta^i \gamma^j) \end{aligned} \tag{43}$$

これから，$[a,b]$ と $[c,d]$ の演算（乗算）を次式で定義することができる．

$$[a,b][c,d] = [ac, ad+b] \tag{44}$$

この式の右辺で，ac や $ad+b$ は n を法として演算されるので，$[ac, ad+b]$ は明らかに，同じ二項拡大体の自己同型である．つまり，自己同型同士の演算はその中で閉じている．

この式から，

$$[a,b][1,0] = [a,b], \tag{45}$$

$$[1,0][c,d] = [c,d] \tag{46}$$

となり，これから単位元 e は

$$e = [1,0] \tag{47}$$

であることがわかる．

最後に，$[a,b]$ の逆元 $[p,q]$ を求めよう．$[p,q]$ を逆元とすると，

$$[a,b][p,q] = [1,0] \tag{48}$$

である．式 (44) から

$$[ap, aq+b] = [1,0] \tag{49}$$

となる．これから，

$$ap = 1 \tag{50}$$

$$aq + b = 0 \tag{51}$$

でなければならない．ここで，a, b, p, q は n を法とする整数である．一般に，a と n は互いに素であるから，

$$ak + nl = 1 \tag{52}$$

となる整数 k と l が必ず存在する．この証明は後で述べる．このような k を $\overline{a}$ と書くと，n を法として，

$$a\overline{a} = 1 \tag{53}$$

となる．これを用いると，式 (50)，(51) は

$$p = \overline{a} \tag{54}$$

$$q = -\overline{a}b \tag{55}$$

となる．これから，$[a,b]$ の逆元 $[a,b]^{-1}$ は

$$[a,b]^{-1} = [\overline{a}, -\overline{a}b] \tag{56}$$

となる．

以上から，自己同型 [a, b] の集合は，式 (44) で表される演算に閉じており，単位元と逆元が存在するから，群を構成することがわかる．この群を G と表す．群 G は，基礎体 P を固定体とするガロア拡大体の自己同型写像が作る群である．これはガロア群である．最小多項式の分解体がガロア拡大であった．いまの場合，二項方程式が最小多項式である．

7.3 ガロア群の部分群

二項拡大体の自己同型 $[a,b]$ の作る群 G において，$[1,b]$ という形の元からなる集合は G の部分群を作る．実際，任意の 2 つの元 $[1,b_1]$ と $[1,b_2]$ の積を考えると，

$$[1,b_1][1,b_2]=[1,b_2+b_1] \tag{57}$$

となり，積も同じ集合の中で閉じている．

一方，$[1,b]$ の逆元は $[1,-b]$ であることが明らかである．したがって，$[1,b]$ の形の自己同型の集合は G の中に部分群を作ることが示された．

7.4 ガロア群の正規部分群

一般に群 G の部分群 H が正規部分群であるとは，H に属する任意の元 g に対し，G の任意の元を h とすると，hgh^{-1} も H に属することである．

二項拡大体のガロア群 G の部分群 H は正規部分群になる．実際，H の任意の元を $[1,b]$，H の任意の元を $[c,d]$ とすると，$[c,d]^{-1}=[\bar{c},-\bar{c}d]$ であるから，

$$[1,b][\bar{c},-\bar{c}d]=[\bar{c},-\bar{c}d+b] \tag{58}$$

$$[c,d][1,b][\bar{c},-\bar{c}d]=[c\bar{c},-c\bar{c}d+cb+d]=[1,cb] \tag{59}$$

となり，H の元であるから，H が正規部分群であることがわかる．

7.5 剰余類

ここから，剰余類，剰余群，巡回群という，群論からみても，やや特殊な項目について述べる．なぜこうした項目が必要かというと，それがガロア群の可解性という重要な性質の存否に関係するからである．それが，二項拡大体のガロア群について，上記の項目を詳細に調べることで明らかになるのである．

まず，剰余類について述べる．群 G の正規部分群を H とする．群 G の元 g と H のすべての元の積を集合を考える．この集合を gH と書く．正規部分群 H が G 自身の場合あるいは単位元の場合，gH は H 自身である．それ以外の場合，gH は H と異なる．gH を H に関する剰余類という．gH の元の数（gH は群ではない）と正規部分群 H の位数は一致する．

gH の任意の元 g' と H の積は gH に等しい．なぜなら，g' は H のある元 h があって $g'=gh$ と表される．h' を H の任意の元とすると，$g'h'=ghh'$ となり hh' は H の元であるから，$g'H$ は gH と等しくなるのである．

gH にも H にも含まれない G の元 f が作る剰余類 fH は H とも gH とも異なる．すなわち，異なる剰余類に共通な元は存在しない．なぜなら，g' を gH の元，f' を fH の元とし，もしそれらが等しいとすると，$gh'=fh$ およびとなるような H の元 h' と h が存在する．この式から $g=f(hh'^{-1})$ となり，hh'^{-1} は H の元であるから，g と f は同じ剰余類の元でなければならない．しかし，これは最初の仮定に矛盾する．したがって，剰余類が重なることはない．

G のすべての元は H に関するいずれかの剰余類に属する．もし剰余類に属しない元があれば H との積を作れば剰余類が作られるが，その剰余類にその元は属することになるので，剰余類に属しない元はない．

以上のことから，群 G は正規部分群 H に関する剰余類に分割され，H_1 に属さない元は必ずいずれかの剰余類に属する．剰余類の元の個数は H の位数に等しい．したがって，G の位数は H の位数の約数である．これは，部分群の位数はもとの群の位数の約数である，というラグランジュの定理である．

7.6 剰余群

剰余類の集合を考える．剰余類をこの集合の元とみなし，以下のように剰余類の間の演算を定義すると，この剰余類の集合は群を構成することがわかる．2 つの異なる剰余類 gH と fH の元 gh と fh' を考える．g と f は G の任意の元，h と を h' は H の任意の元である．gh と fh' の積を以下のように変形する．

$$(gh)(fh') = g(ff^{-1})hfh' = gf(f^{-1}hf)h' = gf(h''h') = gfh_1 \tag{60}$$

ここで，$h'' = f^{-1}hf$ は正規部分群の定義により H の元であり，$h_1 = h''h'$ は同じく H の元である．この式から，gfh_1 は剰余類 gfH の元となり，$(gH)(fH)$ の元の集合は gfH の元の集合と一致することがわかる．実際，上の式は $(gH)(fH)$ の元は gfH に含まれ，gfH の元は $(gH)(fH)$ の形に表されることを示している．具体的には，上の式を直積 $(gH) \times (fH)$ から gfH_1 への写像とすると，その写像は全射であり，核は (gh, fh^{-1}) になる．したがって，剰余類 gH と fH の間の乗法は

$$(gH)(fH) = gfH \tag{61}$$

と定義することができる．この式から，単位元は eH，gH の逆元は $g^{-1}H$ であることがわかる．e は G の単位元である．以上から，剰余類の集合が群を構成することがわかる．この剰余類が作る群を G の H に関する剰余群といい，G/H と表す．G の位数を n，H の位数を m とすると，m は n の約数である．これはラグランジュの定理とよばれる．剰余類の個数は $n/m = k$ であり，剰余群の位数である．剰余群 G/H の位数は剰余類の個数 k であり，これは G に関する部分群 H の指数とよび $(G : H)$ のように表す．ラグランジュの定理では，群 G の位数を $|G|$，部分群 H の位数を $|H|$，部分群 H の指数を $(G : H)$ で表すと，

$$(G : H) = \frac{|G|}{|H|} \tag{62}$$

と表される．

7.7 巡回群

前節で定義された剰余群の具体例を，二項拡大体に対応するガロア群 G とその正規部分群 H について見てみよう．

G の任意の元を $g = [a, b]$，G の正規部分群 H の任意の元を $h = [1, d]$ とする．そうすると，剰余類 gH の元は，

$$gh = [a, b][1, d] = [a, ad + b] \tag{63}$$

となる．b と d は a と独立であり，n を法として 0 から $n-1$ の整数値をとることができるから，$ad+b$ も a とは独立に n を法として 0 から $n-1$ の値をとることができる．したがって，c を n を法とする任意の整数とすれば，$[a, ad + b]$ を $[a, c]$ と表すことができて，$[a, c]$ は a で特定される H に関する剰余類 gH の元である．この剰余類は前節で定義された演算のもとで剰余群を構成する．すなわち，2 つの剰余類 $[a, b]H$ と $[c, d]H$ の積はもう 1 つの剰余類 $[ac, ad + b]H$ となる．この剰余群を G/H と表す．剰余類の元の個数は a のとる整数の範囲から $n-1$ である．正規部分群 H の位数は n である．したがって，G の位数は $n(n-1)$ である．

正規部分群 H と剰余群 G/H は以下に示す巡回群になる．巡回群の定義は以下の通りである．

G を位数 n の乗法群とする．群 G の任意の元が G に含まれる 1 つの元の巾乗で表されるとき，この群を巡回群とよぶ．このような巾乗することによって G の任意の元となる G の元を生成元という．原始根とよばれることもあるが同じものを指す．ここで述べるのは，ある整数を法とする剰余群が巡回群になる場合である．

巡回群の 1 つの生成元を γ とすると，

$$\gamma^n = 1 \tag{64}$$

が成り立つ．ここで，単位元をこの後の表現で便利なように 1 とした．この関係を満たす最小の正の整数を元 γ の位数という．群の元の個数を意味する「群の位数」とは意味が異なるので注意を要する．この関係式は，次のような $n+1$ 個の巾乗の元を考えてみればわかる．

$$\gamma, \gamma^2, \gamma^3, \cdots, \gamma^n, \gamma^{n+1}$$

G の元の個数は n であるから，γ と等しい元が必ずなければならない．そのとき，γ と γ^{n+1} がはじめて等しくなる場合に上の関係式が成り立ち，γ は生成元となる．(γ と γ^m $(m < n)$ が等しくなる場合もあるが，その場合は γ が 1 つの巡回群の部分群を作る．) γ の位数は n である．生成元は単一とは限らない．

G が巡回群であるための必要十分条件の表現はいくつかあるが，その中から 2 つを以下に示す（証明は後述）．

(1) 群 G の位数の任意の約数 d に対し，$x^d = 1$ となる G の元 x の個数が d 以下である．

(2) 位数が n の群 G において，n の約数 d に対し，位数が d の約数となる G の元が d 個存在するなら，位数がちょうど n であるような元が存在する（すなわち，G は巡回群である）．

典型的な巡回群として，ある整数 N を法とする剰余類の乗法群がある．整数環 $\mathbb{Z}$ において，n を法とする剰余類において，そこから零因子を除いた集合 $(\mathbb{Z}/n\mathbb{Z})^\times$ は乗法群を構成し，n が素数のとき，この群は巡回群となる．

では，H が巡回群になることを以下にみてみよう．

H の元は $f = [1, b]$ $(b = 0, 1, \cdots, n-1)$ で n 個ある．f の巾乗を作ると，

$$f^0, f^1, f^2, \cdots, f^{n-1}, f^n$$

となる．その数は $n+1$ で H_1 の位数 n を超えるので，必ず 2 つ以上の同じ項がある．これから $f^m = 1$ という関係が得られる，m は n の約数である．n が素数の場合，$f^n = 1$ となり，f の位数は n になる．

上の式に $f = [1, b]$ を代入した具体的な式は，式 (55) の演算定義を用いると，

$$[1, 0], [1, b], [1, 2b], \cdots, [1, (n-1)b], [1, nb]$$

となる．n を法としているので，最後の項は $[1, 0]$，すなわち単位元である．たとえば，$[1, 1]$ は明らかに生成元となることがわかる．以上のようにして，正規部分群 H は巡回群であることがわかる．

次に，剰余群 G/H が巡回群であることを示そう．そのために，まず剰余群 G/H の性質を調べよう．

正規部分群 H の任意の元を $[1, b]$ $(b = 0, 1, \cdots, n-1)$ と表す．H に関する $[a, c]$ の剰余類は $[a, c]H$ と表される．ここで a は 1 から $n-1$ の整数値を，c は 0 から $n-1$ の整数値をとる．剰余類 $[a, c]H$ の元の個数は，$[a, c]$ と H の元との積がすべて異なるので，H の位数に等しく n である．特に，$a = 1$ のとき剰余類は $[1, c]H = H$ となる．なぜなら，$[1, c]$ は H の元であり，H の元との積は H に含まれ，その個数は n 個でかつすべて異なるからである．これから，$([a, c]H)([1, c]H) = [a, c]HH = [a, c]H$ となり，$[1, c]H$ は剰余群 G/H の単位元であることがわかる．このように，剰余群の元である剰余類 $[a, c]H$ の性質は a のよって決まる．

2 つの剰余類 $[a, c]H$ と $[a', c']H$ の積 $[a, c]H[a', c']H$ は前記定義から $[a, c][a', c'][1, b']H = [aa', ac' + c]H$ である．これから，この剰余群の元の積は aa' の H に関する剰余類であり，a と a' の積で決定されるから，剰余群の 1 つの元 $\gamma = [a, c]H$ の巾乗は $\gamma^i = [a^i, c]H_1$ となる．したがって，G/H が巡回群であることを示すためには，γ が原始根であること，すなわち，$\gamma.\gamma^2, \cdots, \gamma^{n-1}$ がすべて異なることを示せばよい．それは，$a, a^2, \cdots, a^{n-1}$ がすべて異なることであり，a の位数が n であることと等価である．一般に，素数 n を法とする整数の集合 Z において，その乗法群 $(Z/nZ)^\times$ は位数が $n-1$ で巡回群であることが示される（証明は後述）．すなわち，a が巡回群の原始根となる整数が 1 から $n-1$ の中に必ず存在する．したがって，n は素数であることが前提となっているから，G/H は巡回群となるのである．

(つづく)

参考文献

[1] エム・ポストニコフ 「ガロアの理論」 日野寛三訳 (東京図書, 1964).

[2] エミール・アルティン 「ガロア理論入門」寺田文行訳 (ちくま学芸文庫) (筑摩書房, 2010).

[3] 彌永 昌吉 「ガロアの時代　ガロアの数学　第二部 数学篇」(シュプリンガー数学クラブ) (シュプリンガー・フェアラーク, 2002).

[4] 中島 匠一「代数方程式とガロア理論」(共立叢書現代数学の潮流,) (共立出版, 2006).