# ガロアの大発見

BV21019 千葉朱寧

令和3年11月4日

# 目 次

# 研究背景

研究の題材を探すため図書館で数学関連の本棚を眺めていたところ,「ガロア」という文字がいくつか目に入り，興味がわいた．それについての知識がない状態からある程度の理解にこぎつけたいと思った.

## 1　はじめに

4 次以下の方程式には，代数的な解の公式が存在することが証明されている．これらは，方程式の係数から代数的な操作を繰り返すことで解を求めることができるものである．代数的な操作とは,

- 数同士の四則演算 (足し算，引き算，掛け算，割り算)
- ある数の n 乗根をとる

という操作を意味する．5 次以上の方程式でも同様に解の公式が作れると思われたが，1824 年，ノルウェーの数学者アーベルによって 5 次以上の方程式には代数的な解の公式は存在しないということが証明された．解の公式が存在するということは，すなわちその次数では全ての方程式が代数的に解けるということである．では，5 次以上の方程式に代数的に解けるものがないのかというと，そうでもない．以下に 1 つ例を挙げる．$x$ の 5 次方程式

$$x^5 - 15x^4 + 85x^3 - 225x^2 + 274x - 120 = 0$$

を考える．これの左辺は因数分解でき,

$$x^5 - 15x^4 + 85x^3 - 225x^2 + 274x - 120 = (x-1)(x-2)(x-3)(x-4)(x-5)$$

と変形することができる．この方程式は $x = 1, 2, 3, 4, 5$ を解に持つことがわかる．これらの解は全て有理数であり，有理数は方程式の係数から四則演算で計算される．よって，この方程式は代数的に解ける 5 次方程式である．5 次以上の方程式には，全てではないが代数的に解けるものが存在するとわかった．なぜ代数的に解けるのか．それを明らかにしたのが，19 世紀前半のフランスの数学者，ガロアである．以降，ガロアがどのように解明していったのか説明する．

## 2　4 次以下の方程式を代数的に解く

5 次以上の方程式を考える前に，4 次以下の方程式の解の公式がどのようにして成り立っているのか，代数的に解くために何が鍵となっているのかをとらえる必要がある．ここでは，各次数ごとに解の公式の成り立ちについて触れる．

### 2.1　1 次方程式

まず，1 次方程式の解の公式を考える．$a$, $b$ を実数, $a \neq 0$ とすると，一般に次のようになる．

$$ax + b = 0$$

$$ax = -b$$
$$x = -\frac{b}{a} \tag{1}$$

この式 (1) が，1 次方程式の解の公式である．

### 2.2　2 次方程式

次に，2 次方程式で考える．$a$, $b$, $c$ を実数, $a \neq 0$ とすると，一般に次のようになる．

$$ax^2 + bx + c = 0$$

$$ax^2 + bx = -c$$
$$x^2 + \frac{b}{a}x = -\frac{c}{a}$$
$$x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 = -\frac{c}{a} + \left(\frac{b}{2a}\right)^2$$
$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{2}$$

この式 (2) が，2 次方程式の解の公式である．

### 2.3　3 次方程式

続いて，3 次方程式の解の公式を考える．$a$, $b$, $c$, $d$ を実数, $a \neq 0$ とすると，一般に次のようになる．

$$ax^3 + bx^2 + cx + d = 0$$
$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0$$

ここで, $y = x + \dfrac{b}{3a}$とおき，これより $x = y - \dfrac{b}{3a}$を代入して整理すると,

$$y^3 + \left\{ -\frac{1}{3}\left(\frac{b}{a}\right)^2 + \frac{c}{a} \right\} y + \frac{2}{27}\left(\frac{b}{a}\right)^3 - \frac{bc}{3a^2} + \frac{d}{a} = 0$$

となる．そして新たに,

$$\begin{aligned} p &= -\frac{1}{3}\left(\frac{b}{a}\right)^2 + \frac{c}{a} \\ q &= \frac{2}{27}\left(\frac{b}{a}\right)^3 - \frac{bc}{3a^2} + \frac{d}{a} \end{aligned}$$

とおいて方程式を書き直すと,

$$y^3 + py + q = 0 \tag{3}$$

となる．ここで，$y = s + t$ を代入すると,

$$(s+t)^3 + p(s+t) + q = 0$$

となり，変形して

$$(s^3 + t^3 + q) + (s+t)(3st + p) = 0 \tag{4}$$

となる．もし,

$$\begin{cases} s^3 + t^3 + q = 0 \\ 3st + p = 0 \end{cases}$$

を満たす $s$, $t$があれば, 方程式 (3), (4) も満たす．第 2 式より $t = -\dfrac{p}{3s}$と表すことができ, これを第 1 式に代入すると,

$$s^3 - \left(\frac{p}{3s}\right)^3 + q = 0$$

となる．

$$s^6 + qs^3 - \left(\frac{p}{3}\right)^3 = 0$$

6 次方程式が出てきたように見えるが，$s^3$を $u$ とおくと,

$$u^2 + qu - \left(\frac{p}{3}\right)^3 = 0$$

となるため，これは $u$ に関する 2 次方程式である．よって，2 次方程式の解の公式を用いると

$$u = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

となる．これと先程の連立方程式の第 1 式 $s^3 + t^3 + q = 0$，$u = s^3$，$y = s + t$ から，次の式が導かれる．

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} \tag{5}$$

この式 (5) が，3 次方程式の解の公式である．

## 2.4　4 次方程式

4 次方程式では，変数変換をすることで 3 次方程式を解くことに帰着される．そのため，ここでは公式の成り立ちの過程は省略する．

# 3　置換に関する定義

ガロアが方程式の代数的な解法を研究する上で,「解の置換」との関係に着目した．ここでは，置換の性質や定義を説明する．

## 3.1　解の置換

2 つの解が $a, b$ である 2 次方程式を

$$x^2 + px + q = 0$$

とすると，これは

$$(x - a)(x - b) = 0$$

$$x^2 - (a + b)x + ab = 0$$

と書き換えられる．式を見比べると，

$$a + b = -p, \qquad ab = q$$

が成り立つとわかる．これを**解と係数の関係**という．これを利用して，方程式の係数 $p, q$ から四則演算のみを使って $a, b$ の置き換えを考えることが**解の置換**である．例として，

$$(a - b)^2 = (a + b)^2 - 4ab = p^2 - 4q$$

が挙げられる．

## 3.2　置換の表し方

次に,「置換」という操作を考える．$a, b, c$ をそれぞれ異なる任意の数とし，横一列に並べた後，並べ方を変える．例えば，$a$ があった場所に $b$, $b$ があった場所に $c$, $c$ があった場所に $a$ を並べる状況を次のように表す．

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

**注意**　置換において $a, b, c$ の並ぶ順序は関係なく，$a$ があった場所に次に何がくるか, $b$ があった場所に次に何がくるか, $c$ があった場所に次に何がくるか のみを表す．これより，次の 6 つの置換は全て異なる置換を意味する．

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

この 6 個の置換は **3 次対称群**と呼ばれ，$S_3$ と書かれる．

## 3.3 置換の積

2 回置換することを考える．1 回目で $a$ が $b$ に, $b$ が $c$ に, $c$ が $a$ に 置き換わったとすると,

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

と表される．2 回目で $b$ はそのまま, $a$ と $c$ が 置き換わったとすると,

$$\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

と表される．このように 2 回の置き換えを合わせた置換を，1 回目の置き換えを表す置換と 2 回目の置き換えを表す**置換の積**と呼び，次のように表す．

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}\begin{pmatrix} b & c & a \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

また，3 回置換するとき，各回の状況の変化を表す置換を $A, B, C$ とすると次の式が成り立つ．

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

よって，置換同士の積は結合法則が成り立つが,

$$A \cdot B = B \cdot A$$

は必ずしも成り立たないため，**非可換な積**と呼ばれる．

## 3.4 恒等置換

ある置換 $A$ について,

$$(A \cdot A) \cdot A = A^3 = I$$

と表される $I$ を**恒等置換**という．ここで，恒等置換 $I$ の性質をまとめる．

- ある置換の後で恒等置換 $I$ を行っても，結果は最初の置換の結果と変わらない．
- 恒等置換 $I$ の後で何かの置換を行っても，結果は後の置換の結果と変わらない．すなわち，$A \cdot I = I \cdot A = A$ がどのような $A$ についても成り立つ．

ここで，$I, A, A^2$ の組を $\{I, A, A^2\}$ とすると，この 3 個の置換のうちどの 2 個の積の結果も 3 個の置換のうちどれかになるとき，$\{I, A, A^2\}$ は**積について閉じている**という．このように置換の積について閉じている集まりは**置換群**と呼ばれる．置換群に含まれる置換の個数は**位数**と呼ばれ，$\{I, A, A^2\}$ の位数は 3 となる．また，$\{I, A, A^2\}$ は全ての元が $A$ の累乗になっており，このような群は**巡回群**と呼ばれる．そして群に含まれる元同士の積が順番によらない群は**可換群 (アーベル群)** と呼ばれる．これは方程式が代数的に解けるかを知る鍵となる．

# 4　対称式

## 4.1　基本対称式

以下が 1〜4 変数の**基本対称式**である．

| | |
|---|---|
| 1 変数 (a) | a |
| 2 変数 (a, b) | a+b, ab |
| 3 変数 (a, b, c) | a+b+c, ab+bc+ca, abc |
| 4 変数 (a, b, c, d) | a+b+c+d, ab+ac+ad+bc+bd+cd, abc+abd+acd+bcd, abcd |

これらの式は，どんな置換を作用して文字を置き換えても変化しない．例として，**3.2** の 6 個の置換と $a+b+c$ で考える．このうち 1 個の置換で置き換えを式で表すと，

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}(a+b+c) = b+c+a = a+b+c$$

となる．他の 5 個の置換でも同様に $a+b+c$ となり，変化しない．ここで，次のことが言える．

一般に，置換 $A, B, C$ と文字式 $f$ があり $C = AB$ であるとき，

$$Cf = (AB)f = B(Af)$$

が成り立つ．そしてこれらの基本対称式は，それぞれの次数の方程式の解と係数の関係である．

## 4.2　方程式の解の性質

方程式の解の対称式の値は，方程式の係数から四則演算で計算できる．これは有理式においても次のことが成り立つ．

> 方程式の解の有理式 $R$ に全ての解の置換を作用させても変化しないならば，方程式の解の有理式 $R$ の値は，方程式の係数から四則演算で計算できる．しかし，逆は必ずしも成り立つとは限らない．

## 4.3　交代式と差積

2 個の文字だけを入れ替える置換を**互換**という．ある置換を互換の積で表すことを考える．

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix} = (34)(12)(14)(35)(24)$$

これは，5 個の置換の積である．このように奇数個の互換の積で表せる置換は**奇置換**といい，偶数個の互換の積で表せる置換は**偶置換**という．

方程式が代数的に解けるか調べるために役立つものとして，対称式の他に**交代式**がある．これは，全ての互換に対して，作用させると式の符号が変化する式である．ここで，次のことがいえる．

> 交代式に奇置換を作用させると，符号だけ変化する．
> 交代式に偶置換を作用させると，式は変化しない．

これらの性質から，交代式は対称式の平方根だとわかる．

以下が 1〜4 変数の**差積**である．

| | |
|---|---|
| 1 変数 (a) | なし |
| 2 変数 (a, b) | (a-b)　あるいは-(a-b)　(=(b-a)) |
| 3 変数 (a, b, c) | (a-b)(a-c)(b-c)　あるいは　-(a-b)(a-c)(b-c) |
| 4 変数 (a, b, c, d) | (a-b)(a-c)(a-d)(b-c)(b-d)(c-d)　あるいは　-(a-b)(a-c)(a-d)(b-c)(b-d)(c-d) |

そして，全ての交代式は，差積と対称式の積で表せるのだ．

## 4.4　方程式の判別式

差積の 2 乗を**判別式**という．差積は方程式の解の差の積を意味するので，判別式の値が 0 になるかならないかで重解を持つか持たないかを判別できる．これより，次のことがいえる．

> 判別式の値は，方程式の係数から四則演算で計算される．
> 差積の値は，方程式の係数から四則演算で計算される数の平方根である．

## 4.5　解の公式と解の置換

今まで述べたことと解の公式の関係を説明する．3 次方程式

$$y^3 + py + q = 0$$

で考える．これの解の公式は

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

であった．このとき，解を次のように表せる．

$$a = \frac{(a+b+c)+\left(a+\omega b+\omega^2 c\right)+\left(a+\omega^2 b+\omega c\right)}{3} \tag{6}$$

$$b = \frac{(a+b+c)+\omega^2\left(a+\omega b+\omega^2 c\right)+\omega\left(a+\omega^2 b+\omega c\right)}{3} \tag{7}$$

$$c = \frac{(a+b+c)+\omega\left(a+\omega b+\omega^2 c\right)+\omega^2\left(a+\omega^2 b+\omega c\right)}{3} \tag{8}$$

$\omega$は 1 の 3 乗根のうち 1 じゃないもの，すなわち$\dfrac{-1\pm\sqrt{3}i}{2}$である．式 (6) の分子の項に注目する．第 1 項の $(a+b+c)$ は，$a,b,c$ の基本対称式である．第 2 項と第 3 項は，$a,b,c$ の対称式ではないが，方程式の係数と解の差積との四則演算で表せる数の 3 乗根となる．差積は $a,b,c$ の対称式である判別式の平方根である．

これより，分子の項は全て方程式の係数の四則演算で表すことができることがわかる．つまり，この方程式が代数的に解けることを示しているのだ．このことは 2 次方程式や 4 次方程式でも同様にして示された．5 次以上の方程式でも，(6)，(7)，(8) にあたる式がヴァンデルモンドによって作られた．しかし，分子の項の $\left(a+\omega b+\omega^2 c\right)$ や $\left(a+\omega^2 b+\omega c\right)$ にあたるものの満たす方程式の次数が上がってしまいべき根が発見できず，ルフィニやアーベルによって 5 次方程式の代数的な解の公式は作れないと証明された．

# 5　ガロア群

では，ガロアはどのように 5 次以上の方程式で代数的に解けるものを導き出したのか．そこで考え出されたガロア群の考え方を説明する．

## 5.1　解の有理式

**4.2** で述べたことから，方程式のガロア群は次の性質をもつものと定義される．

Ⅰ 置換の積について閉じている．
Ⅱ 有理数を係数とする解の有理式の値について，ガロア群に入る全ての解の置換を作用させても式の値が変化しないことと，その式の値が有理数であることは同値である．

これより，解の式で値が有理数になるものをすべて知るには方程式のガロア群を知ればよいとわかる．1 次方程式から順にガロア群を調べる．

**1 次方程式**

1 次方程式

$$x+p=0$$

を考える．解は 1 つしかないので，置き換えは自分自身しか存在しない．よって，1 次方程式のガロア群は恒等置換 $I$ のみからなる．

**2 次方程式**

- 判別式が有理数の 2 乗ではない場合

$$\begin{pmatrix} a & b \\ a & b \end{pmatrix}、\begin{pmatrix} a & b \\ b & a \end{pmatrix} \text{の両方}$$

- 判別式が有理数の 2 乗の場合

$$\begin{pmatrix} a & b \\ a & b \end{pmatrix} \text{のみ}$$

となる．差積が有理数でないときは，作用させると式の値が変化するような置換が存在しなくてはならないからである．

**3 次方程式**

- 解が 3 個とも有理数の場合

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \text{のみ}$$

- 解の 1 つだけが有理数の場合

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}、\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}、\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

後者の場合では，**3.2** の 6 つの置換のうち差積が変化しない，かつ置換の積について閉じているものがこの 3 つとなる．

これらのことを踏まえて，次のことがわかる．

方程式のガロア群が恒等式 $I$ のみからなる方程式は，全ての解が有理数である．
逆も成り立つ．

## 5.2 ガロア群

3 次方程式で解の 1 つだけが有理数の場合の 3 つのガロア群を，次のように表す．

$$\begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix}$$

これの各行をそれぞれの行に作用させたとき，どの順でも同じ 3 つの順列となる．今までの置換もこのように表すと次のようになる．

**1 次方程式**

$$\begin{bmatrix} a \end{bmatrix}$$

**2 次方程式**

- 判別式が有理数の 2 乗ではない場合

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix}$$

- 判別式が有理数の 2 乗の場合

$$\begin{bmatrix} a & b \end{bmatrix}$$

ここで，次の性質をもつものを**群**と呼ぶ．

1 つの順列からそれぞれの順列に移る置換の集まりが，どの順列から始めても同じになる．

## 5.3 ガロアによるガロア群の作り方

2 次方程式を考える．ガロアは，次の手順でガロア群を作った．

1. 方程式の解 $a, b$ を表せる有理式 $V(a, b)$ で表せる式を見つける．
2. V の値を代入すると値が 0 となる多項式のうち，次数が最も小さいものを探す．
3. ($V$ の最小多項式)=0 の解をすべて求める．
4. 1 で求めた式に解を代入する．

これにより，**5.2** で求めたものと同じものが得られる．そして，ガロア群が以下のことを満たすことを示した．

Ⅰ　各行は方程式の解の順列になっている．
Ⅱ 行の間の置換の集まりが群の性質を持つ．
Ⅲ 行の間の置換の集まりが，**5.1** のⅡ の性質を持つ．

# 6　正規部分群

## 6.1　まずガロア群を求める

3 次方程式 $x^3-2=0$ を考える．これの差積は有理数ではないので，ガロア群には式の値を変化させて積で閉じている置換が含まれる．しかし，差積の値を変化させる置換から見つけると，この場合うまくいかない．よって，はじめに積で閉じているものから調べる．すると，次の 6 個が挙げられる．それぞれを $A$〜$F$ とする．

$$
\begin{aligned}
A &= \textbf{3.2} \text{ の 6 つの置換全部} \\
B &= \left\{ I, \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \right\} \\
C &= \left\{ I, \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \right\} \\
D &= \left\{ I, \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \right\} \\
E &= \left\{ I, \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \right\} \\
F &= \{I\}
\end{aligned}
$$

ガロア群には式の値を変化させて積で閉じている置換が含まれるので，$B$ と $F$ ではない．$C, D, E$ が含まれると仮定すると，これに含まれるどの置換に式 $(a+b)$ を作用させても変化しないので，$(a+b)$ は有理式である．しかし，解と係数の関係から $a+b=-c$ だが，$c$ は有理数ではないので矛盾する．これより，$A$ のみが残るのでこれがガロア群となる．

## 6.2　部分群

次の性質をもつものを**部分群**という．

Ⅰ　分かれたそれぞれの組が群になっている．
Ⅱ 各組の順列の置換の集まりが，分かれた全ての組で共通になる．

$A$ と $F$ のような，全体と恒等置換 $I$ からなる部分群は**自明な部分群**という．それに対し，$B$〜$E$ は**自明でない部分群**という．

**6.1** より，$x^3-2=0$ のガロア群は次のように表せる．

$$
\begin{bmatrix}
a & b & c \\
b & c & a \\
c & a & b \\
a & c & b \\
c & b & a \\
b & a & c
\end{bmatrix}
$$

ここで部分群 $B$ を例に挙げると，次のように書き換えられる．

$$\begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix}$$

$$\begin{bmatrix} a & c & b \\ c & b & a \\ b & a & c \end{bmatrix}$$

先程述べた性質から，これが部分群だとわかる．上の組の第 1 行目を下の組の第 1 行目に移す置換は $b$ と $c$ の置換なので $(bc)$ となる．そして第 2 行目，第 3 行目でも置換は $(bc)$ となる．これが**正規**という性質である．次のようにまとめる．

ある 1 つの組のそれぞれの順列に，同じ置換を作用させることで別の各組のすべての順列が得られるとき，これを**正規部分群**という．

なお，2 つの組に分ける部分群を表す分割は，必ず正規部分群になる．

# 7　代数的解法への正規部分群の利用

## 7.1　正規部分群でべき根を作る

**4.5** から，方程式の係数の四則演算で表されるべき根を用いることで方程式が代数的に求められることを示した．ここで，正規部分群でべき根を作ることを考える．

**6.2** の部分群における置換 $(bc)$ にあたるものを M とする．また，正規部分群で共通の各組の順列の置換の集まり $\{I, (abc), (acb)\}$ を N とする．ここで，次のようなべき根を考える．

Ⅰ 方程式の係数の四則演算で表される数のべき根 $\theta$ を作る．
Ⅱ 方程式の係数とこのべき根 $\theta$ を合わせて考えると，方程式のガロア群が，元のガロア群の正規部分群の順列の組の 1 つに変化する．

正規部分群の M を作用させると値が変化し，正規部分群の N を作用させても値が変化しないものを $\alpha$ とする．そして，$\alpha$ に置換 $(bc)$ を作用させて $-\alpha$ となるものを $\beta$ とする．

ここで，$\theta$ を次のように表す．

$$\theta = \alpha + (-1)\beta$$

この (-1) は 1 の $n$ 乗根のうち 1 でないもので，$n$ は位数を意味する．ここでは 2 であり，$M$ を 2 回続けて作用させると恒等置換になる．

## 7.2　ガロア群の再定義

**5.1** で有理数として考えたものを厳密に定義し直す．ガロア群を考えるうえで決めた数の全体を**使ってよい数**とし，次のように分類する．

使ってよい数 0　＝　方程式の係数の四則演算で計算される数

使ってよい数 1 ＝ 方程式の係数と$\theta$の四則演算で計算される数

$\omega$や$\alpha, \beta$ は使ってよい数 2 である．これより，ガロア群は次のように言い換えられる．

Ⅰ 置換の積について閉じている．
Ⅱ 使ってよい数を係数とする解の有理式の値について，ガロア群に入る全ての解の置換を作用させても式の値が変化しないことと，その式の値が使ってよい数であることは同値である．

使ってよい数が増えると，差積の符号を変える置換 $(ab), (bc), (ca)$ は定義からガロア群には入らなくなる．ガロア群に入る置換は $(abc), (acb)$, 恒等置換 $I$ となる． よって，**6.2** のガロア群は

$$\begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix}$$

となる．これの正規部分群は次のようになる．

$$\begin{bmatrix} a & b & c \end{bmatrix}$$

$$\begin{bmatrix} b & c & a \end{bmatrix}$$

$$\begin{bmatrix} c & a & b \end{bmatrix}$$

このように，使ってよい数を増やすことでガロア群を縮めることができる．これを最終的に恒等置換 $I$ のみにして解を代数的に表すには，この操作を繰り返せばよい．

## 7.3 正規部分群の順列の組を 1 つにする

ここで，$\theta$ と同様に新たな数を作る．これを

$$\tau = a + \omega b + \omega^2 c$$

と表す．この式で使われている文字を説明する．

- $a \cdots$ 方程式の係数の解の四則演算で計算される数で，正規部分群の M を作用させると値が変化し，正規部分群の N を作用させても値が変化しないもの．
- $b \cdots a$ に作用させると変化する M を，$a$ に 1 回作用させたもの．
- $c \cdots a$ に作用させると変化する M を，$a$ に 2 回作用させたもの．
- $\omega \cdots 1$ の $n$ 乗根で 1 でないもの．ただし，$n$ は $a$ に作用させると変化する M の位数．
- $\omega^2 \cdots 1$ の $n$ 乗根で 1 でないものの 2 乗．ただし，$n$ は $a$ に作用させると変化する M の位数．

これは，M(ここでは置換 $(abc)$) の 3 乗が恒等置換であることと，$\omega$ が 1 の 3 乗根であることを組み合わせて利用したものである．そして新たに，

使ってよい数 2 = 方程式の係数と $\theta, \tau$ の四則演算で計算される数

と定める．この方程式の 3 つの解は，使ってよい数 2 になる．以上の操作から，**6.2** ガロア群は

$$\begin{bmatrix} a & b & c \end{bmatrix}$$

となり，方程式は代数的に解けた．

### 7.4　代数的解法の一般化

一般の方程式の場合も，これまでのようにべき根を作ることができる．これを $\rho$ とすると，以下のことが成り立つ．

正規部分群が素数 $p$ 個の組に分かれるならば，$\rho$ の $p$ 乗がその段階の使ってよい数になる．

素数ではない $p$ も，素因数分解して素数乗根を繰り返し添加すればよい．代数方程式の，使ってよい数 $k$ に対するガロア群を $G_k$ とすると，以下の 3 つの性質を持つ解の順列の組の列

$$G_0, G_1, \cdots, G_{n-1}, G_n$$

を常に作れる．

Ⅰ $G_0 = G$
Ⅱ $k = 1, 2, \cdots, n$ に対して，$G_k$は，$G_{k-1}$の正規部分群である．
Ⅲ $G_n$ は 1 つだけの順列からなる．

そして，このような列を方程式の**ガロア群の正規列**という．よって，正規列が以下の性質 P をもつとき，その方程式は代数的に解ける．

$i = 1, 2, \cdots, r$ に対して，$G_i$ に含まれる置換の個数は，$G_{i-1}$ に含まれる順列の個数の，素数分の 1 であり，逆も成り立つ．

## 8　おわりに

解の公式の成り立ちに立ち返ることで，方程式が代数的に解ける仕組みを理解できる．また，置き換えや群の考えを使うことで，次数が上がることによってべき根を見つけにくくなることを回避できるのは画期的だ．今後は，これを応用した作図やその後の数学に与えた影響についても理解を深めたい．

# 参考文献

[1] 中村亨著，ガロアの群論，講談社，2010 年