ガロアの大発見

千葉朱寧

芝浦工業大学 数理科学研究会

November 4, 2021

はじめに

4 次以下の方程式は，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．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)
- とある数の n 乗根をとる

である．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．しかし，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．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．

解が代数的に解けるとは

解が a, b, c の 3 次方程式を考えると，解 a は次のように表される．

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

同様に，

- $b \cdots$ 分子の第 2 項目に ω^2 をかけて第 3 項目に ω をかけたもの
- $c \cdots$ 分子の第 2 項目に ω をかけて第 3 項目に ω^2 をかけたもの

ω は 1 の 3 乗根のうち 1 じゃないもの，すなわち $\frac{-1\pm\sqrt{3}i}{2}$．そして，この分子の項は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．
これらの項の次数が上がっていくにつれ，べき根を発見するのが困難になった．

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のがガロア群である．まず，「置換」というものを説明する．

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

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

以上が 3 次方程式の全ての置換である．これらは，上の行の並びを下の行の並びに移すことを意味する．
また，例えばこの 3 個目の置換と 5 個目の置換は

$$(bc), (abc)$$

とも表せる

任意の置換 A で

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

と表される I を「恒等置換」という．
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．

これを踏まえて，方程式のガロア群を次の性質をもつものと定義する．

- 置換の積について閉じている．
- 「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」は後ほど説明するが，今は有理数とする．

例として，$x^3 - 2 = 0$ のガロア群は次のように表せる．

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

これを上下半分に分けると，上の組の第 1 行目から下の組の第 1 行目に移す置換は (bc) で，2，3 行目でも共通である．
このようなものを「正規部分群」という．

- M$\cdots$ この正規部分群で共通の置換 (bc)
- N$\cdots$ 共通の各組の順列の置換の集まり $\{I, (abc), (acb)\}$
- $\alpha\cdots$ 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
- $\beta\cdots\alpha$ に置換 (bc) を作用させて $-\alpha$ となるもの

以上のように定めると，前述したべき根 θ は

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

と表される．
ここで使ってよい数とは， 方程式の係数と θ の四則演算で計算される数と方程式の係数と θ の四則演算で計算される数である．

これで改めてガロア群を考えると，

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

となる．これを恒等置換のみになるまで繰り返す．この場合は，

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

を θ と同様に作る．

ここ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．

これにより，使ってよい数に方程式の係数と θ, τ の四則演算で計算される数が追加され，ガロア群は

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

となり，恒等置換のみになる．

代数的解法の一般化

- 一般の方程式のべき根を ρ とすると，正規部分群が素数 p 個の組に分かれるならば，ρ 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．
- ここで，1 つの順列からなるガロア群 G_n において，$G_0 = G$ であり $k = 1, 2, \cdots, n$ に対して G_k が G_{k-1} の正規部分群であるとき，これを「ガロア群の正規列」という．

今までのことから，次の性質をもつ方程式は代数的に解けるといえる．

$i = 1, 2, \cdots, r$ 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

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．

 中村亨著，ガロアの群論，講談社，2010 年.