

高校生のためのガロア理論

県立流山北高等学校 増田 史朗

あらすじ

2 次方程式の解の公式が中学校の学習内容から高等学校に移行されたいぶ歳月が過ぎた。数学 I で 2 次方程式の解の公式* を学ぶ生徒に、高次方程式の解の公式をどのくらい話題にできるかわからない。ともあれ、若き天才ガロア (Galois, 1811~1832) が 10 代に作り出した理論に対して、興味・関心がある高校生も多いことだろう。数学のすばらしさを知ってもらうためにも、方程式のガロア理論についてこれからも語り続けたい。

1 3 次方程式の解の公式

(1) 2 次方程式の解の公式の確認

最初に 2 次方程式について確認しよう。

$$ax^2 + bx + c = 0; \quad (a, b, c \text{ 実数 } a \neq 0)$$

の 2 つの解 x_1, x_2 は次のように因数分解

$$\begin{aligned} ax^2 + bx + c &= a \left\{ x^2 + \left(\frac{b}{a} \right) x + \frac{c}{a} \right\} \\ &= a \left\{ \left(x + \frac{b}{2a} \right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} \right\} \\ &= a \left\{ \left(x + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right\} \\ &= a \left(x - \frac{-b + \sqrt{b^2 - 4ac}}{2a} \right) \left(x - \frac{-b - \sqrt{b^2 - 4ac}}{2a} \right) \end{aligned}$$

できる。したがって、解の公式は

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \dots\dots\dots \textcircled{1}$$

*実数解の範囲までとされている。

となる。根号の中の式 $b^2 - 4ac$ を判別式 D (discriminant) とすれば、 D の符号によって解の性質が変わる。

もし $D > 0$ なら、 x_1 と x_2 はともに異なる実数の解である。

$D = 0$ なら、 $x_1 = x_2 = -\frac{b}{2a}$ (重複解)。 2次方程式の解

$D < 0$ なら、 x_1 と x_2 はともに異なる複素数の解である。

と係数の関係も解の公式から次のように求まる。

$$x_1 + x_2 = -\frac{b}{a}, \quad x_1 x_2 = \frac{c}{a} \quad \dots\dots\dots ②$$

(2) 3次方程式の解の公式

2次方程式の解法は紀元前 2000 年頃の古代バビロニアに始まる。3次方程式の解法については、中世(9世紀以後)のインドやアラビアで発展し、アラビアからヨーロッパ(イタリア)へ伝わった。

最終的に、一般の3次方程式の解法と呼ばれるものはカルダノ(Cardano 1501～1576)によって1539年に発見⁽¹⁾されたという。

カルダノの方法により、これから3次方程式の解 x_1, x_2, x_3 を求めてみよう。

$$ax^3 + bx^2 + cx + d = 0, \quad (a \neq 0), \quad \dots\dots\dots ③$$

において、 $x = y - \frac{b}{3a}$ と置き、 y について整理すると、

$$y^3 + py + q = 0, \quad \dots\dots\dots ④$$

のような y の3次方程式に変形することができる。ただし、 p, q は、

$$p = -\frac{b^2 - 3ac}{3a^2}, \quad q = \frac{2b^3 - 9abc + 27a^2d}{27a^3} \quad \dots\dots\dots ⑤$$

である。

次の公式が求まれば、一般の3次方程式の解を求めることができる。

3次方程式の解の公式(カルダノ)

$$y^3 + py + q = 0 \text{ の解は, } y_1 = u + v, \quad y_2 = \omega u + \omega^2 v, \quad y_3 = \omega^2 u + \omega v$$

$$\text{ここで, } u = \left(-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}} \right)^{\frac{1}{3}}, \quad v = \left(-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}} \right)^{\frac{1}{3}}$$

ただし、 $\omega = \frac{-1 + \sqrt{3}i}{2}$ (1の虚数3乗根) とする。

⁽¹⁾実際に公式を発見したのは、ニコラ・フォンタナ(通称タルターリア)というイタリア人の数学者と言われている。

理由はともかく、 $y = u + v$ と置き、3 次方程式 $y^3 + py + q = 0$ に代入して整理すれば、

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0 \quad \dots\dots\dots ⑥$$

となることがわかる。この式において、

$$u^3 + v^3 = -q, \quad uv = -\frac{p}{3} \quad \dots\dots\dots ⑦$$

となるような u, v があれば都合がよい。実際、 $u^3 v^3 = -\frac{p^3}{27}$ であるから、 u^3 と v^3 が t の 2 次方程式

$$t^2 + qt - \frac{p^3}{27} = 0 \quad \dots\dots\dots ⑧$$

の解であることがわかる。したがって、2 次方程式の解の公式を使って、

$$u^3 = -\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}} \quad \dots\dots\dots ⑨$$

となる。さらに、それぞれの 3 乗根⁽²⁾を求めて u, v の値

$$u, v = \left(-\frac{q}{2} \pm \sqrt{\frac{p^3}{27} + \frac{q^2}{4}} \right)^{\frac{1}{3}} \quad \dots\dots\dots ⑩$$

が求まる。3 次方程式 $y^3 + py + q = 0$ の解 y_1, y_2, y_3 は、

$$y_1 = u + v, \quad y_2 = \omega u + \omega^2 v, \quad y_3 = \omega^2 u + \omega v \quad \dots\dots\dots ⑪$$

となるから、元の 3 次方程式の解 x_1, x_2, x_3 は、

$$x_1 = y_1 + \frac{b}{3a}, \quad x_2 = y_2 + \frac{b}{3a}, \quad x_3 = y_3 + \frac{b}{3a} \quad \dots\dots\dots ⑫$$

で求められる。

2 方程式の解と置換群

(1) 2 次方程式の解と置換群

16 世紀中頃にフェ拉里 (Ferrari, 1522～約 1560) が 4 次方程式の解の公式を発見した。

⁽²⁾ u^3 の 3 乗根は $u, \omega u, \omega^2 u$ の 3 個あり、 v^3 も同様。

その後、5 次方程式の解法の発見が目標として浮上した。しかし、200 年以上の空白期間が続き、一般の 5 次方程式の代数的解法⁽³⁾の存在自体を疑う数学者も現れた。

18 世紀の終わり頃、ラグランジュ(Lagrange,1736~1813)を始めとする数学者は、方程式の解を相互に交換したり、移し換える「操作」の集合、いわゆる解の置換群に注目して解法を研究した。

群(ぐん)とは、「この範囲では自由に演算(掛けたり割ったり等)の計算ができる」という集合を表す抽象的な概念である。一般の群の定義を次に示す。

群の定義

積 $a \circ b$ が定義された集合 G で、以下の 3 つの条件を満たすならば G は群である。

- (1) 積 $\circ$ に関する結合法則が成立する;
 $(a \circ b) \circ c = a \circ (b \circ c) \quad (\text{for all } a, b, c \in G)$
- (2) 単位元 e が存在する;
 $a \circ e = e \circ a = a \quad (\text{for all } a \in G)$
- (3) G の任意の元 a に対しその逆元 a^{-1} が存在する;
 $a \circ a^{-1} = a^{-1} \circ a = e$

群 G の元の数のことを位数という。位数を $\|G\|$ という記号で表す。

群 G の部分集合 H が G の積に関して閉じていて、 H のどの元にも逆元が H の中に存在するとき、この部分集合 H を G の部分群⁽⁴⁾という。部分群 N の元 f が群 G の任意の元 g に対して $g \circ f \circ g^{-1} \in N$ を満たすとき、 N を正規部分群という。

G が群であれば、 G および単位群 $E = \{e\}$ (単位元のみからなる群) は必ず G の部分群になる。これらを自明な部分群といい、それ以外の部分群は、真の部分群と呼ぶ。

2 次方程式

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

の 2 つの解を x_1, x_2 とする。 x_1 を x_2 に、 x_2 を x_1 に入れ換える置換を T_{21} とし、これを記号

$$T_{21}[x_1, x_2] = [x_2, x_1]$$

のように表す。

また、実際には移したことになるが、便宜上、 T_{12} を x_1 を x_1 に、 x_2 を x_2 に移し換える置換とする。これを記号

$$T_{12}[x_1, x_2] = [x_1, x_2]$$

⁽³⁾係数の間の四則演算と冪根(べきこん)、この場合 5 乗根までを有限回用いて求めること。

⁽⁴⁾ H の任意の元 a, b に対して $a \circ b^{-1} \in H$ が成り立つことである。

で表す。以上をまとめて一覧表にすれば,

	T_{12}	T_{21}
x_1	x_1	x_2
x_2	x_2	x_1

である。集合 $S_2 = \{T_{12}, T_{21}\}$ の積 $T_{12} \circ T_{21}$ を

$$\begin{aligned}
 T_{12} \circ T_{21}([x_1, x_2]) &= T_{12}(T_{21}([x_1, x_2])) \\
 &= T_{12}([x_2, x_1]) \\
 &= [x_2, x_1] \\
 &= T_{21}([x_1, x_2])
 \end{aligned}$$

より, $T_{12} \circ T_{21} = T_{21}$ と定める。同様に, $T_{21} \circ T_{12}, T_{21} \circ T_{21}$ も定めると, 単位元 e は T_{12} , 置換 T_{21} の逆元 $(T_{21})^{-1}$ は T_{21} 自身であることがわかる。

したがって, 集合 S_2 は 2 次方程式の解の置換群である。

(2) 3 次方程式の解と置換群

一般の 3 次方程式

$$ax^3 + bx^2 + cx + d = 0$$

の解を x_1, x_2, x_3 とし, 解の置換群 S_3 について説明する。

たとえば, T_{231} を解 x_1, x_2, x_3 をそれぞれ, x_2, x_3, x_1 に移し換える置換とする。これを記号

$$T_{231}([x_1, x_2, x_3]) = [x_2, x_3, x_1]$$

で表す。 S_3 の各要素で, 解 x_1, x_2, x_3 が移されるようすを一覧表にすると,

	T_{123}	T_{132}	T_{213}	T_{231}	T_{312}	T_{321}
x_1	x_1	x_1	x_2	x_2	x_3	x_3
x_2	x_2	x_3	x_1	x_3	x_1	x_2
x_3	x_3	x_2	x_3	x_1	x_2	x_1

である。積 $T_{213} \circ T_{132}$ は,

$$\begin{aligned}
 T_{213} \circ T_{132}([x_1, x_2, x_3]) &= T_{213}([x_1, x_3, x_2]) \\
 &= [x_2, x_3, x_1] \\
 &= T_{231}([x_1, x_2, x_3])
 \end{aligned}$$

だから, $T_{213} \circ T_{132} = T_{231}$ と定める。

また, T_{231} の逆元 $(T_{231})^{-1}$ が T_{312} であることは,

$$\begin{aligned} T_{312} \circ T_{231}([x_1, x_2, x_3]) &= T_{312}([x_2, x_3, x_1]) \\ &= [x_1, x_2, x_3] \\ &= T_{123}([x_1, x_2, x_3]) \end{aligned}$$

からわかる。このとき 単位元 e は T_{123} である。

置換群 S_3 の部分集合 $A_3 = \{T_{123}, T_{231}, T_{312}\}$ とする。 A_3 の要素によって解 x_1, x_2, x_3 は次の表のように,

	T_{123}	T_{231}	T_{312}
x_1	x_1	x_2	x_3
x_2	x_2	x_3	x_1
x_3	x_3	x_1	x_2

移される。

ところで,

$$\begin{aligned} (T_{231})^2 &= T_{231} \circ T_{231}, \\ (T_{231})^3 &= T_{231} \circ T_{231} \circ T_{231} \end{aligned}$$

のように, 記号 $(T_{231})^2, (T_{231})^3$ を定め, これらを計算すると,

$$(T_{231})^2 = T_{312}, \quad (T_{231})^3 = T_{123} = e \quad (\text{単位元})$$

であるから, $A_3 = \{e, T_{231}, (T_{231})^2\}$ と表せる。

このことから, A_3 は置換群 S_3 の部分群⁽⁵⁾であることがわかる。置換群 S_3 の部分群はそれ自身も含めて 5 個ある。部分群をすべてあげると,

$$\begin{array}{ll} S_3 &= \{e, T_{132}, T_{213}, T_{231}, T_{312}, T_{321}\}, & \|S_3\| &= 6 \\ A_3 &= \{e, T_{231}, (T_{231})^2\}, & \|A_3\| &= 3 \\ W &= \{e, T_{132}\}, & \|W\| &= 2 \\ V &= \{e, T_{213}\}, & \|V\| &= 2 \\ E &= \{e\}, & \|E\| &= 1 \end{array}$$

のようになる。

⁽⁵⁾さらに, 正規部分群になっている。

3 方程式のガロア理論

(1) 2 次方程式のガロア理論

2 次方程式

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

の 2 つの解を x_1, x_2 とし, $u = x_1 + x_2, v = x_1 - x_2$ として解の置換を考える。たとえば, $T_{21}(u)$ は

$$\begin{aligned} T_{21}(u) &= T_{21}(x_1 + x_2) \\ &= x_2 + x_1 \\ &= u \end{aligned}$$

である。 u, v を置換群 S_2 の要素で移す一覧表は,

	T_{12}	T_{21}
u	u	u
v	v	$-v$

となる。この表から, u^2, v^2 はすべての置換に対して不変であることがわかる。

解 x_1, x_2 があらゆる置換で不変な式のことを対称式と呼ぶ。対称式は, 基本対称式 $x_1 + x_2$ と $x_1 x_2$ を含んだ式で表せることが知られている。実際, $v^2 = (x_1 - x_2)^2$ が基本対称式の式で

$$\begin{aligned} (x_1 - x_2)^2 &= x_1^2 - 2x_1 x_2 + x_2^2 \\ &= (x_1 + x_2)^2 - 4x_1 x_2 \end{aligned}$$

と表せる。また, 2 次方程式の解と係数の関係から, 基本対称式が係数 a, b, c の分数式で

$$x_1 + x_2 = -\frac{b}{a}, \quad x_1 x_2 = \frac{c}{a}$$

のように表せる。よって $v^2 = (x_1 + x_2)^2 - 4x_1 x_2$ は

$$\begin{aligned} v^2 &= \left(-\frac{b}{a}\right)^2 - 4 \cdot \frac{c}{a} \\ &= \frac{b^2 - 4ac}{a^2} \end{aligned}$$

であるから, u, v を 2 次方程式の係数 a, b, c だけを使って

$$u = -\frac{b}{a}, v = \frac{\sqrt{b^2 - 4ac}}{a}$$

のように表せる。また, $x_1 = \frac{u+v}{2}, x_2 = \frac{u-v}{2}$ であるから,

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

となり, 2 次方程式の解の公式を得る。紙数の都合により, 3 次方程式, 4 次方程式については割愛する。

(2) 5 次方程式の解の公式について

これまで, 2 次方程式, 3 次方程式の解の公式についてガロア理論の視点から考えてきた。

これらに共通する考え方は, 解の置換に対して不変な式 (対称式) を発見し, 基本対称式の式で表すことであった。この手法は, 複雑さを増すが 4 次方程式の解の公式についても有効である。

ところが, 5 次方程式の解の公式についてはルジャンドル (Legendre, 1752~1833) の後, 若きアーベル (Abel, 1802~1829) によって否定的に解決された。その定理とは,

——— 定理 (Abel, 1826) ———

5 次以上の方程式は一般に, それを冪根を用いて解くことは不可能である。

というものである。

5 次方程式の解が必ず存在することは, 1779 年にガウス (Gauss, 1777~1855) が証明している⁽⁶⁾。Abel の定理の意味は, その存在する解が, 5 次以上の方程式に対して, 四則演算と冪根 (平方根, 立方根, 4 乗根など) のよって一般に表せないということである。

方程式の解の公式をめぐる長い歴史は, この定理をもって一応の幕を閉じた。その後, アーベルよりも更に若いガロアが最終的な定理

——— 定理 (Galois, 1832) ———

方程式が冪乗根を用いて解ける条件は, その方程式のガロア群が可解群である。

を得た。これは, 代数方程式が解の公式を持つことはどうして可能なのか, 不可能であるのはなぜかに答えるものである。

⁽⁶⁾ガウスの学位論文で, 代数学の基本定理と呼ばれている。

概略を3次方程式において、誤解を恐れず説明する。

3次の置換群 S_3 , その部分群 A_3 の, 単位群 E を考える。それぞれの群の位数は

$$\|S_3\| = 6, \quad \|A_3\| = 3, \quad \|E\| = 1$$

で, すべて正規部分群である。そして次の包含関係

$$S_3 \supset A_3 \supset E$$

を満たしている。

このとき, S_3 と A_3 の位数の商 $[S_3 : A_3] = 2$, A_3 と E の位数の商 $[A_3 : E] = 3$ で, どちらも素数である。3次方程式の解の公式を考えると群の商が深く関連している。一般の方程式の解の有無も, 正規部分群の間の包含関係とその位数の商の性質から判定できる。

ガロア理論は数学の基礎のひとつとして, 抽象的な群そのものを研究する群論 (とくに有限群論), ある数学的対象に変換として働くときの群 (位相群, リー群など) の研究, 抽象群を変換群として実現する研究 (表現論) など現代数学に重要な位置をしめている。

参考文献

- [1] 草場 公邦, ガロワと方程式, 朝倉書店, 1989
- [2] 数学セミナー, 1992, 7月号, 日本評論社