

3 次方程式の根の公式 (Cardano の公式)

$f(X) = X^3 + pX + q = 0$ の根は、

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

(但し、3乗根は掛けて $-\frac{p}{3}$ となるように取る)

3乗根の1組を u, v とすると、($\omega^2 + \omega + 1 = 0$)

$$X = u + v, \omega u + \omega^2 v, \omega^2 u + \omega v$$

判別式

$$f(X) = X^3 + pX + q = \prod_{i=1}^3 (X - x_i)$$

$$\begin{aligned} D(f) &:= \prod_{1 \leq i < j \leq 3} (x_i - x_j)^2 \\ &= (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 \\ &\quad : f \text{ の判別式 (discriminant)} \end{aligned}$$

- x_1, x_2, x_3 の対称式
 → 係数 (基本対称式) で書ける
- $f(X)$ が重根を持つ $\iff D(f) = 0$

判別式

$$f(X) = X^3 + pX + q = \prod_{i=1}^3 (X - x_i)$$

$$\begin{cases} s_1 = x_1 + x_2 + x_3 = 0 \\ s_2 = x_1x_2 + x_1x_3 + x_2x_3 = p \\ s_3 = x_1x_2x_3 = -q \end{cases}$$

$$\begin{aligned} D(f) &= s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2 \\ &= -4p^3 - 27q^2 \end{aligned}$$

(\longrightarrow Maple による実演)

判別式

判別式を用いると、**Cardano** の公式は次の形:

$$X = \sqrt[3]{-\frac{q}{2} + \frac{\sqrt{D}}{6(\omega - \omega^2)}} + \sqrt[3]{-\frac{q}{2} + \frac{\sqrt{D}}{6(\omega^2 - \omega)}} \\ (D = -4p^3 - 27q^2)$$

(2 次方程式と同様に、根に \sqrt{D} が現れる!!)

4 次方程式の解法の発見 (16 世紀前半, Ferrari)

3 次方程式の解法から間もなく

- 難しさの違いが少ない？
- 時代が熟していた？
(考察の蓄積・記号法の発達など)

(以下、暫く板書で)

4 次方程式の Ferrari の解法

$$f(X) = X^4 + pX^2 + qX + r = 0$$

補助変数 t を導入して、

$$(X^2 + t)^2 = (2t - p)X^2 - qX + (t^2 - r)$$

の右辺が完全平方になる



$$q^2 - 4(2t - p)(t^2 - r) = 0$$

これは t の 3 次方程式

→ この t を用いて解く

分解式

$$g(t) = q^2 - 4(2t - p)(t^2 - r)$$

: 3 次分解式 (解核多項式, **resolvent**)

$T := 2t$ において、

$$\begin{aligned} R(T) &:= -g\left(\frac{T}{2}\right) \\ &= T^3 - pT^2 - 4rT - (q^2 - 4pr) \end{aligned}$$

5 次以上の方程式の解法への模索

有力な方法の一つ: **Tschirnhaus** 変換

$$X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n = 0$$

$Y = X^{n-1} + b_1X^{n-2} + \cdots + b_{n-2}X + b_{n-1}$
の形の変換で、

解ける方程式 ($Y^n = c$ など) にならないか

5 次以上の方程式の解法への模索

しかし、次の進展は、

3 次・4 次方程式の解法の発見から、
200 年以上も待たねばならなかった

→ 200 年後 (18 世紀後半): **Lagrange** の考察

今まで何故うまく行ったかを詳細に分析
(群論の萌芽・**Galois** 理論への一歩)

実は、4 次以下と 5 次以上とでは、
問題の難しさが本質的に違った
のだった

5 次以上の方程式の解法への模索

しかし、次の進展は、

3 次・4 次方程式の解法の発見から、
200 年以上も待たねばならなかった

→ 200 年後 (18 世紀後半): **Lagrange** の考察

今まで何故うまく行ったかを詳細に分析
(群論の萌芽・**Galois** 理論への一歩)

実は、4 次以下と 5 次以上とでは、
問題の難しさが本質的に違った
のだった

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

3 次方程式

$$f(X) = X^3 + pX + q = 0$$

の 3 根 x_1, x_2, x_3 に対し、

$$u = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3),$$

$$v = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$$

を考えよ

(ω は 1 の原始 3 乗根、 $\omega^2 + \omega + 1 = 0$)

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

$$u = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3), v = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$$

根の置換

$$\sigma = (1\ 2\ 3) : x_1 \mapsto x_2 \mapsto x_3 \mapsto x_1$$

$$\tau = (2\ 3) : x_1 \mapsto x_1, x_2 \mapsto x_3 \mapsto x_2$$

に対して、

$$\sigma : \begin{cases} u \mapsto \omega^2 u \mapsto \omega u \mapsto u \\ v \mapsto \omega v \mapsto \omega^2 v \mapsto v, \end{cases} \quad \tau : u \mapsto v \mapsto u$$

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

u^3 は、根のあらゆる置換で動かしても、
出てくるのは u^3, v^3 のみ (軌道, orbit)



$$(T - u^3)(T - v^3) = T^2 - (u^3 + v^3)T + u^3v^3$$

の係数は、根のあらゆる置換で不変 (対称式)



元の方程式の係数 (基本対称式) で書ける筈!!

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

u^3 は、根のあらゆる置換で動かしても、
出てくるのは u^3, v^3 のみ (軌道, orbit)



$$(T - u^3)(T - v^3) = T^2 - (u^3 + v^3)T + u^3v^3$$

の係数は、根のあらゆる置換で不変 (対称式)



元の方程式の係数 (基本対称式) で書ける筈!!

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

u^3 は、根のあらゆる置換で動かしても、
出てくるのは u^3, v^3 のみ (軌道, orbit)



$$(T - u^3)(T - v^3) = T^2 - (u^3 + v^3)T + u^3v^3$$

の係数は、根のあらゆる置換で不変 (対称式)



元の方程式の係数 (基本対称式) で書ける筈!!

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

ところで、

$$u = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3),$$
$$v = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$$

は何処から来たのか？

更に遡って、

2 次方程式の解法を Lagrange 風に見てみよう

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

ところで、

$$u = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3),$$

$$v = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$$

は何処から来たのか？

更に遡って、

2 次方程式の解法を Lagrange 風に見てみよう

2 次方程式の解法 (Lagrange 風)

$X^2 + aX + b = 0$ の 2 根を α, β とする:

$$\begin{cases} \alpha + \beta = -a \\ \alpha\beta = b \end{cases} \quad (\text{基本対称式})$$

これを直接解こうとしても、
元の方程式に戻るだけ

$\alpha - \beta$ は対称式ではないが、
 α, β を入換えると (-1) 倍

→ $(\alpha - \beta)^2$ は対称式 → a, b で表せる!!

2 次方程式の解法 (Lagrange 風)

$X^2 + aX + b = 0$ の 2 根を α, β とする:

$$\begin{cases} \alpha + \beta = -a \\ \alpha\beta = b \end{cases} \quad (\text{基本対称式})$$

これを直接解こうとしても、
元の方程式に戻るだけ

$\alpha - \beta$ は対称式ではないが、
 α, β を入換えると (-1) 倍

→ $(\alpha - \beta)^2$ は対称式 → a, b で表せる!!

2 次方程式の解法 (Lagrange 風)

$$\begin{aligned}(\alpha - \beta)^2 &= (\alpha + \beta)^2 - 4\alpha\beta \\ &= a^2 - 4b : \text{判別式}\end{aligned}$$

$$\begin{cases} \alpha + \beta = -a \\ \alpha - \beta = \pm\sqrt{a^2 - 4b} \end{cases}$$

$$\longrightarrow \alpha, \beta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

3 次方程式に戻って、

$$u = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3), v = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$$

は、

$\sigma = (1\ 2\ 3) : x_1 \mapsto x_2 \mapsto x_3 \mapsto x_1$ で ω^2 倍
→ 固有値 ω^2 の固有ベクトル

始めから探すには、固有値問題を解けば良い
(対称群の線型表現)

3 次方程式の解法 (Cardano の公式) への Lagrange の考察 (18 世紀後半)

うまくいった理由の要点:

u^3 は、根のあらゆる置換で動かしても、
出てくるのは u^3, v^3 のみ (軌道, orbit)

u^3, v^3 が “程々に” 対称的
→ 方程式を解く途中の手掛かりとなった

4 次方程式の Ferrari の解法 (再掲)

$$f(X) = X^4 + pX^2 + qX + r = 0$$

補助変数 t を導入して、

$$(X^2 + t)^2 = (2t - p)X^2 - qX + (t^2 - r)$$

の右辺が完全平方になる



$$q^2 - 4(2t - p)(t^2 - r) = 0$$

これは t の 3 次方程式

→ この t を用いて解く

分解式 (再掲)

$$g(t) = q^2 - 4(2t - p)(t^2 - r)$$

: 3 次分解式 (解核多項式, **resolvent**)

$T := 2t$ において、

$$\begin{aligned} R(T) &:= -g\left(\frac{T}{2}\right) \\ &= T^3 - pT^2 - 4rT - (q^2 - 4pr) \end{aligned}$$

分解式 (再掲)

$$f(X) = X^4 + pX^2 + qX + r$$

$$R(T) = T^3 - pT^2 - 4rT - (q^2 - 4pr)$$

$R(T)$ が因数分解できる

$\iff f(X)$ が 3 乗根を用いずに
(平方根だけで) 解ける

このような、方程式の“解け方”を統制する群
… (方程式・多項式の) Galois 群

分解式 (再掲)

$$f(X) = X^4 + pX^2 + qX + r$$

$$R(T) = T^3 - pT^2 - 4rT - (q^2 - 4pr)$$

$R(T)$ が因数分解できる

$\iff f(X)$ が 3 乗根を用いずに
(平方根だけで) 解ける

このような、方程式の“解け方”を統制する群
… (方程式・多項式の) **Galois 群**