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 $-\dfrac{p}{3}$ となるように取る)

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

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

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

$$\begin{aligned} D(f) :&= \prod_{1 \le i < j \le 3} (x_i - x_j)^2 \\ &= (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 \end{aligned}$$

: f の**判別式 (discriminant)**

- x_1, x_2, x_3 の対称式

  $\longrightarrow$ 係数 (基本対称式) で書ける

$$D(f) = -4p^3 - 27q^2$$

- $f(X)$ が重根を持つ $\iff D(f) = 0$

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!!**

$\longrightarrow$ **理由は Galois 理論で説明される**

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

$$\Updownarrow$$

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

これは t の 3 次方程式

$\longrightarrow$ **この t を用いて解く。**

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

$: 3$ **次分解式 (解核多項式,resolvent)**

$T := 2t$ **とおいて、**

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

演習 2:

(1) “二重根号をはずす公式”

$\sqrt{(a+b) \pm 2\sqrt{ab}} = \sqrt{a} \pm \sqrt{b}$ を確かめよ

(2) $x = \sqrt{5 + 2\sqrt{6}}$ について、

(a) 二重根号をはずせ

(b) x が満たす有理数係数の方程式は？

(c) その方程式を Ferrari の方法で解いてみよ

(3) $x = \sqrt{10 + 2\sqrt{17}}$ について、

(a) 無理やり二重根号をはずそうとすると？

(b) x が満たす有理数係数の方程式は？

(c) その方程式を Ferrari の方法で解いてみよ

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

$$X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = 0$$

$$Y = X^{n-1} + b_1 X^{n-2} + \cdots + b_{n-2} X + b_{n-1}$$

の形の変換で、

解ける方程式 ($Y^n = c$ など) にならないか。

$$\begin{cases} X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = 0 \\ X^{n-1} + b_1 X^{n-2} + \cdots + b_{n-2} X + b_{n-1} = Y \end{cases}$$

の解 (x, y) **を考える**

$Y = y$ **に対し、**

$$\exists x : (x, y) \text{ が解}$$

$$\Updownarrow$$

$$\begin{cases} X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = 0 \\ X^{n-1} + b_1 X^{n-2} + \cdots + b_{n-2} X + (b_{n-1} - y) = 0 \end{cases}$$

が共通根を持つ

$$
\begin{cases}
f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \\
\qquad\;\; = \displaystyle\prod_{i=1}^{n} (X - \alpha_i) \\
g(X) = X^m + b_1 X^{m-1} + \cdots + b_{m-1} X + b_m \\
\qquad\;\; = \displaystyle\prod_{j=1}^{m} (X - \beta_j)
\end{cases}
$$

が共通根を持つ

$$
\iff \qquad R(f,g) := \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) = 0
$$

$R(f,g)$ **: 終結式 (resultant)**

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n = \prod_{i=1}^{n} (X - \alpha_i)$$

$$g(X) = X^m + b_1 X^{m-1} + \cdots + b_m = \prod_{j=1}^{m} (X - \beta_j)$$

$$R(f, g) := \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) \qquad : \textbf{終結式}$$

- α_i **達・**β_j **達 それぞれについて対称式**
  $\longrightarrow a_i, b_j$ **達の多項式で書ける**
- f, g **から** X **を消去した多項式**

さて、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。

$\longrightarrow$ 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 $\cdots$ "Lagrange resolvent"

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

$$u = (x_1 + \omega x_2 + \omega^2 x_3)/3$$
$$v = (x_1 + \omega^2 x_2 + \omega x_3)/3$$

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、

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

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)

$$\Downarrow$$

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

の係数は、根のあらゆる置換で不変 (対称式)

$$\Downarrow$$

元の方程式の係数 (基本対称式) で書ける筈!!

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。**

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。

$$\begin{cases} \alpha + \beta = -a \\ \alpha\beta = b \end{cases}$$

(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

$\longrightarrow (\alpha - \beta)^2$ は対称式 $\longrightarrow a, b$ 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。

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

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

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

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

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

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

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

$\longrightarrow$ 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)

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**

$\longrightarrow$ **方程式を解く途中の手掛かりとなった。**

では、4 次方程式

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

の Ferrari の解法がうまくいった理由は？

- **3 次分解式**

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

  の根の正体は？

- **"程々に対称的" な根の組合せは？**

では、4 次方程式

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

の Ferrari の解法がうまくいった理由は？

- **3 次分解式**

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

  の根の正体は？

- **"程々に対称的" な根の組合せは？**

Lagrange の定理(の元々の形)

n 次多項式の根から作った有理式 u に対し、

全ての根の置換 $n!$ 個のうち
u を不変にする置換が m 個ならば、

$$m \mid n!$$

であり、u は根の置換により
$d := \dfrac{n!}{m}$ 個の異なる値を取る。

更にこのとき、
u は係数から作られる d 次多項式の根である。