Galois 理論

- 方程式の解け方の様子
- 体拡大の様子

を Galois 群によって計る

3 次方程式の根の公式（Fontana-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、(**$\omega^2 + \omega + 1 = 0$**)**

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

3 次多項式の判別式

$$f(X) = X^3 + pX + q = \prod_{i=1}^{3}(X - x_i) \qquad \text{に対し、}$$

$$D(f) := \prod_{1 \le i < j \le 3} (x_i - x_j)^2$$

$$= (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$$

：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**
- $f(X)$ **が重根を持つ** $\Longleftrightarrow D(f) = 0$

3 次多項式の判別式

根と係数との関係を用いて判別式を求めると、

$f(X) = X^3 + pX + q$ **の判別式は**

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

Fontana-Cardano の公式は次の形

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

（2 次方程式と同様に、根に $\sqrt{D}$ が現れる !! ）

3 次方程式の “不還元の場合”

実は、3 実根を持つ 3 次方程式を
Fontana-Cardano の方法で解くと、

$$\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2 = -\frac{D}{108} < 0$$

となり、負数の平方根を経由する（不可避）
$\cdots$ “不還元の場合 (Casus irreducibilis)”

歴史上で、負数の平方根が扱われた最初

“存在しない” 数を形式的に扱うと、
“存在する” 実根が計算できる

$\longrightarrow$ 数式の形式的な操作の有用性

3 次方程式の “不還元の場合”

実は、3 実根を持つ 3 次方程式を
Fontana-Cardano の方法で解くと、

$$\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2 = -\frac{D}{108} < 0$$

となり、負数の平方根を経由する（不可避）
$\cdots$ “不還元の場合 (Casus irreducibilis)”

歴史上で、負数の平方根が扱われた最初

“存在しない” 数を形式的に扱うと、
“存在する” 実根が計算できる

$\longrightarrow$ 数式の形式的な操作の有用性

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

（Fontana-Cardano の公式で解ける !! ）

$\longrightarrow$ この t を用いて解く

4 次多項式の 3 次分解式

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

：3 次**分解式（解核多項式, resolvent）**

$T := 2t$ **とおいて、**

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

$R(T)$ **が因数分解できる**
$\Longleftrightarrow$ $f(X)$ **の根が** 3 **乗根を用いずに表せる**

4 次多項式の 3 次分解式

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

：3 次**分解式**（**解核多項式**, **resolvent**）

$T := 2t$ **とおいて、**

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

$R(T)$ **が因数分解できる**

$\Longleftrightarrow$ $f(X)$ **の根が** 3 **乗根を用いずに表せる**

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

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

に対し、

$$Y = X^{n-1} + b_1X^{n-2} + \cdots + b_{n-2}X + b_{n-1}$$

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

$\longrightarrow$ 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

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

$\longrightarrow$ 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

体拡大の Galois 理論

- 方程式の解け方の様子
- 体拡大の様子

を Galois 群によって計る

Galois の理論は元々は方程式論であったが、
現代では体拡大の理論として扱うことが多い

その前にちょっとお話から

「数」とは何だろうか？
（というか、
我々が普通「数」だと思っているものは、
どのようなものだっただろうか？）

体拡大の Galois 理論

- 方程式の解け方の様子
- 体拡大の様子

を Galois 群によって計る

Galois の理論は元々は方程式論であったが、
現代では体拡大の理論として扱うことが多い

その前にちょっとお話から

「数」とは何だろうか？

（というか、
我々が普通「数」だと思っているものは、
どのようなものだっただろうか？）

「数」体系の拡張

$\mathbb{N}$：**自然数全体**

$\cap$

$\mathbb{Z}$：**整数全体（整数環）**

$\cap$

$\mathbb{Q}$：**有理数全体（有理数体）**

$\cap$

$\mathbb{R}$：**実数全体（実数体）**

$\cap$

$\mathbb{C}$：**複素数全体（複素数体）**

「数」体系の拡張

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

我々がこれを

「数」体系の拡張

と思ってきたのは、

新たに付け加わったもの達も

「数」

だと思ってきたということである

ところが . . .

「数」体系の拡張

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

我々がこれを

「数」体系の拡張

と思ってきたのは、

新たに付け加わったもの達も

「数」

だと思ってきたということである

ところが . . .

「数」？の例 1：剰余類の成す体の拡大

合同式 ($a \equiv b \pmod{m}$) は有用であった
（現代風に言えば、剰余環 $\mathbb{Z}/m\mathbb{Z}$ を考えた）

一方、$\mathbb{R}$ 内では $X^2 + 1 = 0$ に解がなかったが、

この “解” を仮想すると便利なので、

$i = \sqrt{-1}$ を「数」だと認識して、
「数」体系を $\mathbb{C}$ まで拡張した

「数」？の例 1：剰余類の成す体の拡大

さて、例えば、

$\mathbb{Z}/3\mathbb{Z}$ **内には、やはり** $X^2+1=0$ **の解がない**

X	$X^2+1 \bmod 3$
0	**1**
1	**2**
2	**2**

では、ここに “$\sqrt{-1}$” を付け加えて
「数」を拡張することが出来るのか？
（この “$\sqrt{-1}$” は「数」なのか？）

「数」？の例 1：剰余類の成す体の拡大

さて、例えば、

$\mathbb{Z}/3\mathbb{Z}$ 内には、やはり $X^2+1=0$ の解がない

X	$X^2+1 \bmod 3$
0	1
1	2
2	2

では、ここに “$\sqrt{-1}$” を付け加えて

「数」を拡張することが出来るのか？

（この “$\sqrt{-1}$” は「数」なのか？）

「数」？の例 2：p 進数

実数は、

有理数（特に十進有限小数）の極限

として定式化された

$$\pi = 3.14159265358979323846264338327 9\cdots$$
$$= 3 \times 10^{0} + 1 \times 10^{-1} + 4 \times 10^{-2} + \cdots$$

計算は、適当な精度で途中で打ち切って行なう

「数」？の例 2：p 進数

一方、20 世紀初頭に Hensel は、
次のような “極限” を考えることを提唱した

素数 p に対し、

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

$\cdots$ p 進数 (p-adic numbers)

任意の N に対し、$\bmod\ p^N$ での計算は、
その “精度” で途中で打ち切って出来る

「数」？の例 2：p 進数

$X^2 = -1$ を $\mathrm{mod}\ 5^N$ で解こう

$$-1 \equiv (2 \cdot 5^0)^2 \mod 5^1$$

$$-1 \equiv (2 \cdot 5^0 + 1 \cdot 5^1)^2 \mod 5^2$$

$$-1 \equiv (2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2)^2 \mod 5^3$$

$$\cdots$$

$$-1 = (2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2 + \cdots)^2$$

この最後の式の右辺の括弧の中の

$$2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2 + \cdots$$

は「数」なのか？

「数」？の例 2：p 進数

$X^2 = -1$ を $\bmod 5^N$ で解こう

$$-1 \equiv (2 \cdot 5^0)^2 \mod 5^1$$

$$-1 \equiv (2 \cdot 5^0 + 1 \cdot 5^1)^2 \mod 5^2$$

$$-1 \equiv (2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2)^2 \mod 5^3$$

$$\cdots$$

$$-1 = (2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2 + \cdots)^2$$

この最後の式の右辺の括弧の中の

$$2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2 + \cdots$$

は「数」なのか？

「数」？の例 2：p 進数

$X^2 = -1$ を $\bmod 5^N$ で解こう

$$-1 \equiv (2 \cdot 5^0)^2 \mod 5^1$$

$$-1 \equiv (2 \cdot 5^0 + 1 \cdot 5^1)^2 \mod 5^2$$

$$-1 \equiv (2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2)^2 \mod 5^3$$

$$\cdots$$

$$-1 = (2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2 + \cdots)^2$$

この最後の式の右辺の括弧の中の

$$2 \cdot 5^0 + 1 \cdot 5^1 + 2 \cdot 5^2 + \cdots$$

は「数」なのか？

我々はどんなものを「数」と思ってきたか？

“「数」の範囲”の満たすべき性質は？

$\longrightarrow$ 不自由なく計算（四則演算）が行える

$\longrightarrow$ 公理化（公理的な「体論」の誕生）

体：Körpar（独），corps（仏），field（英）

我々はどんなものを「数」と思ってきたか？

“「数」の範囲”の満たすべき性質は？

$\longrightarrow$ 不自由なく計算（四則演算）が行える

$\longrightarrow$ 公理化（公理的な「体論」の誕生）

体：Körpar（独），corps（仏），field（英）

我々はどんなものを「数」と思ってきたか？

“「数」の範囲”の満たすべき性質は？

$\longrightarrow$ 不自由なく計算（四則演算）が行える

$\longrightarrow$ 公理化（公理的な「体論」の誕生）

体：Körpar（独），corps（仏），field（英）

では、現代的な代数の言葉による
「体論」「Galois 理論」の授業を始めよう

本授業では専ら、体とその有限次代数拡大を扱う

まずは、「環」と「体」の話から

（以下、板書で）