2008 年度後期

代数特論 II

(教育学部理学科数学専修)

(担当: 角皆)

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 理論

“正問題”

多項式 $\longrightarrow$

・ **Galois 群**

体拡大 $\longleftarrow$

“逆問題”

“Inverse Galois Problem”

Galois 理論

“正問題”

多項式 $\longrightarrow$

・ Galois 群

体拡大 $\longleftarrow$

“逆問題”

“Inverse Galois Problem”

与えられた有限群 G に対し、

- G を Galois 群に持つ体拡大の存在／非存在
- 存在するならその具体的な構成
  (多項式の最小分解体として構成)
  $\longrightarrow$ Galois 群の構成問題
- パラメタ付の多項式による G-拡大の族の構成
- 全ての G-拡大を与える多項式の構成
  (生成的多項式,generic polynomial)

「構成的 Galois 理論」

与えられた有限群 G に対し、

- G を Galois 群に持つ体拡大の存在／非存在
- 存在するならその具体的な構成
(多項式の最小分解体として構成)
$\longrightarrow$ Galois 群の構成問題
- パラメタ付の多項式による G-拡大の族の構成
- 全ての G-拡大を与える多項式の構成
(生成的多項式,generic polynomial)

「構成的 Galois 理論」

一般的な理論に乗る部分もあるが、

実際には

扱う体や有限群の個性が強く影響し、

一筋縄でいかない所がある。

特に実例を多く扱うことで

「計算する数学」

の面白さを思い出してもらいたい。

(シラバスより)

- 古典的な方程式論
  (3 次・4 次方程式の根の公式)
- Galois 理論の復習
- Galois 群の計算例
- Galois の逆問題 (構成問題) について
- Galois 群の構成の幾つかの方法の紹介
  - $\star$ Hilbert の既約性定理とその応用
  - $\star$ Noether の問題とその応用
  - $\star$ Galois 剛性の利用

ところで $\cdots$

3 次方程式・4 次方程式の一般解法
(解の公式)

って知ってますか？

$\longrightarrow$ 方程式の解法探求の歴史

ところで $\cdots$

3 次方程式・4 次方程式の一般解法 (解の公式)

って知ってますか？

$\longrightarrow$ 方程式の解法探求の歴史

今までに習った数学 (算数) を

振り返ってみよう。

(人間と数学の歴史を振り返る)

小学校:

- 自然数 (正の整数) の＋×
- −は出来ない時がある
- ÷は商と余りとを求める (整除)
- 分数を用いた÷ (正の有理数)
- 小数 (近似値・正の実数)

中学・高校:

- 正負の数の四則 (＋－×÷)
- 文字式 (多項式) の＋－×
- ÷は分数式 (有理式) として
- 1 変数の整除 (商と余り)
- 数の－÷ $\longrightarrow$ 1 次方程式
- 2 次方程式の根の公式
  (知らなくても困らない？)
- 簡単な連立方程式
- 3 次以上は因数分解出来れば解ける

大学で数学を習って

新しく出来るようになったことって

ある？

中学・高校:

- 正負の数の四則 (＋－×÷)
- 文字式 (多項式) の＋－×
- ÷は分数式 (有理式) として
- 1 変数の整除 (商と余り)
- 数の－÷ $\longrightarrow$ 1 次方程式
- 2 次方程式の根の公式
  (知らなくても困らない？)
- 簡単な連立方程式
- 3 次以上は因数分解出来れば解ける

多変数多項式の割り算 (余りを求める)

$\Downarrow$

Gröbner 基底

(広中-Buchberger の algorithm)

多変数多項式環の ideal の標準的な生成系を組織的に与えるアルゴリズム

連立方程式 $\longrightarrow$ 1 変数方程式へ (変数消去)

本講義の中で行なう計算にも不可欠!!

ここでは、

3 次以上の方程式の根の公式

を考えよう !!

2 次方程式の根の公式

古代バビロニアで既に知られていた
(紀元前 2000 年頃!! 平方完成の方法)

但し、

- 問題も解法も言葉で表された
- 係数は正の数のみ (非整数も OK)
- (正数の範囲の) 引き算は OK
- 解も正の数のみ

考えている「数」は正の数のみ

$\longrightarrow$ **以下は別個に扱われた。($a > 0, b > 0$)**

- $X^2 + aX = b$
- $X^2 = aX + b$
- $X^2 + b = aX$

しかし、分数・平方根の概念はあった。

($\longrightarrow$ 負の数は人間にとって考え難い?!)

考えている「数」は正の数のみ

$\longrightarrow$ **以下は別個に扱われた。(** $a > 0, b > 0$ **)**

- $X^2 + aX = b$
- $X^2 = aX + b$
- $X^2 + b = aX$

しかし、分数・平方根の概念はあった。

($\longrightarrow$ **負の数は人間にとって考え難い?!)**

考えている「数」は正の数のみ

$\longrightarrow$ **以下は別個に扱われた。(**$a > 0, b > 0$**)**

- $X^2 + aX = b$
- $X^2 = aX + b$
- $X^2 + b = aX$

しかし、分数・平方根の概念はあった。

($\longrightarrow$ **負の数は人間にとって考え難い?!)**

3 次方程式の解法 (根の公式) は？

「**根の公式**」とは:

係数に

- 四則と冪根とを
- 有限回だけ

施して解を表す。

参考:

- 作図問題: 定規とコンパス
- 中国: 解の近似計算 (小数)

3 次方程式の解法 (根の公式) は？

「**根の公式**」とは:
係数に

- 四則と冪根とを
- 有限回だけ

施して解を表す。

参考:

- 作図問題: 定規とコンパス
- 中国: 解の近似計算 (小数)

3 次方程式の解法 (根の公式) は？

「根の公式」とは:
係数に

- 四則と冪根とを
- 有限回だけ

施して解を表す。

参考:

- 作図問題: 定規とコンパス
- 中国: 解の近似計算 (小数)

2 次方程式の解法から遥か 3500 年の後、
遂に 3 次方程式の根の公式が発見された!!

16 世紀前半
(del Ferro, Fontana, Cardano)

- 代数の記号法が進歩しつつある時期
  (但し、まだ略記法に近い)
- 負の数はまだ半人前
- 立方完成して、さあそれからどうする

では、

この解法を現代の記号法で見ていこう。

(以下、暫く板書で)

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、($\omega^2 + \omega + 1 = 0$)

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

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

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

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

: 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** $\iff D(f) = 0$

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

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

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)