2016 年度秋期

代数学 III（ガロア理論）

（情報理工学科）

（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

授業概要

今までの代数系科目（代数学基礎・代数学 I（群論）・代数学 II（環と加群））を踏まえて、体論およびガロア理論について講義する。
体論の基礎事項として、体の構成・代数拡大・超越拡大・代数閉体・拡大次数・共役・正規拡大・分離拡大などの概念を導入した後、
ガロア理論の基本定理を紹介し、基本的な例として有限体・円分体・クンマー拡大などに触れる。
併せて古典的な問題意識として方程式の解法理論や作図問題との関連にも時間があれば触れたい。

（シラバスより）

本講義の概要・予定

- 古典的な方程式論（3 次・4 次方程式の根の公式）
- 環（特に有理整数環・多項式環）と体
- 体の構成（分数化・剰余環）
- 体論の基礎事項
  （代数拡大・拡大次数・共役・正規拡大
  ・標数・有限体・分離拡大）
- 体拡大の自己同型群・ガロア拡大・ガロア群
- ガロア理論の基本定理・ガロア対応・計算例
- 円分体・有限体のガロア理論・巡回クンマー拡大
- 方程式のべき根による解法・古典的作図問題など

さて、初めに $\cdots$

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**

$\longrightarrow$ **まず今までに習った数学（算数）を振り返ろう**
（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**
- **簡単な連立方程式**
- 3 **次以上は因数分解出来れば解ける**

ところで $\cdots$

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
- 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 $\longrightarrow$（一般には高次の）1 変数方程式へ（変数消去）

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 !! 今と同じ平方完成の方法）

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**

2 次方程式の根の公式

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。

文化的背景が数学の問題意識に影響？

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**
- **立方完成が第一歩、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（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、**($\omega^2 + \omega + 1 = 0$)

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

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

- 時代が熟していた？
  （考察の蓄積・記号法の発達など）

- 難しさの違いが少ない？
  $\longrightarrow$ “難しさ” ってどう計る？

（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

$$\Updownarrow$$

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

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**