

# 5 次多項式の同型問題について

陸名雄一（早稲田大学）

ガロア理論とその周辺 徳島 2008

## Mestre-Brumer の $\mathcal{D}_5$ -多項式の定義

- $\mathcal{D}_5 = \langle \sigma, \tau \mid \sigma^5 = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$  : 5 次二面体群 (位数 10)
- $K$  : 基礎体
- $K(u, v)$  :  $K$  上の 2 変数有理函数体

### Mestre-Brumer の多項式

$\text{Bru}(u, v; X) :=$

$$X^5 + (u - 3)X^4 + (v - u + 3)X^3 + (u^2 - u - 2v - 1)X^2 + vX + u$$

- $K(u, v)$  上の  $\mathcal{D}_5$ -多項式
- 任意の  $\mathcal{D}_5$ -拡大  $L/K$  に対して,  $L = \text{Spl}_K(\text{Bru}(\alpha, \beta; X))$  を満たす  $\alpha, \beta \in K$  が存在する
- つまり,  $\text{Bru}(u, v; X)$  は  $K$  上の全ての  $\mathcal{D}_5$ -拡大を実現できる

## Brumer 多項式の同型問題 — 判定問題

対応  $K^2 \ni (\alpha, \beta) \mapsto \text{Spl}_K(\text{Bru}(\alpha, \beta; X))$  は (一般には) 1 対 1 ではない.

### 問題

予め与えられた  $\alpha, \beta, \alpha', \beta' \in K$  に対して,

「 $\text{Spl}_K(\text{Bru}(\alpha, \beta; X)) = \text{Spl}_K(\text{Bru}(\alpha', \beta'; X))$  となるか否か」

を判定せよ

### 解

$\text{Bru}(\alpha', \beta'; X)$  が  $\text{Spl}_K(\text{Bru}(\alpha, \beta; X))$  上で一次因子の積に分解するか否かを調べればよい

— 分解体の計算. (横山氏の講演を参照)

## Brumer 多項式の同型問題 — 分類問題

### 問題

$\alpha, \beta \in K$  の動く範囲に制限を課したとき, どのような  $D_5$  拡大体  $/K$  が現れるか

### 定理 (Kida-Sato-R)

- $\alpha \in K$  と “中間の二次体” を固定して  $\beta \in K$  を動かすと, 現れる分解体  $\text{Spl}_K(\text{Bru}(\alpha, \beta; X))$  の種類は有限個
  - これらの類別は, 上の条件から定まる楕円曲線 (弱 Mordell-Weil 群) を用いて記述できる □
- (木田氏の講演, 及び arXiv:0802.0054v1 を参照)

## Brumer 多項式の同型問題 — 構成問題

### 問題

$(\alpha, \beta) \in K^2$  を一つ固定するとき,  
 $\text{Spl}_K(\text{Bru}(\alpha, \beta; X)) = \text{Spl}_K(\text{Bru}(\alpha', \beta'; X))$  となる様な  $(\alpha', \beta') \in K^2$   
を見つけよ

単に“サーチ”して見つけていくのではなくて、以下の様なことができれば理想的

- 解を全て見つける
- 解を“たくさん”見つける
- 解をパラメーター付きで表示する
- 或る解から別の解を“システマティック”に求める（アルゴリズムを発見する）

## システムティックな構成

- Kida-Sato-R の定理より, 与えられた  $(\alpha, \beta) \in K^2$  に対して,  
 $\text{Spl}_K(\text{Bru}(\alpha, \beta; X)) = \text{Spl}_K(\text{Bru}(\alpha, \beta'; X))$  となる様な  $\beta' \in K$  の全てを, 先程の楕円曲線の加法を用いてシステムティックに求める (計算する) ことができる.
- 一般  $D_5$ -多項式の “Brumer 化” を用いる方法
  - $D_5$ -多項式は必ず  $\text{Bru}(\alpha, \beta; X)$  の形にチルンハウス変換できる. これを “Brumer 化” と呼ぶ.
  - $\text{Bru}(\alpha, \beta; X)$  自身に Brumer 化を施すとどうなるか

## $\mathcal{D}_5$ -多項式の Brumer 化

定理 (Brumer 多項式の genericity)

$L$  を  $K$  上の任意の  $\mathcal{D}_5$ -拡大体とし,  $\text{Gal}(L/K)$  を  $\langle \sigma, \tau \rangle$   
( $\sigma^5 = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1}$ ) と表示すると,

$$L = K(\theta), \quad \tau(\theta) = \theta, \quad \sigma^2(\theta) = \frac{1 - \sigma(\theta)}{\theta} \quad (*)$$

を満たす  $\theta \in L$  が存在する. □

この  $\theta$  の  $\langle \sigma, \tau \rangle$ -orbit は

$$R_\theta := \left\{ \theta, \sigma(\theta), \frac{1 - \sigma(\theta)}{\theta}, \frac{\theta + \sigma(\theta) - 1}{\theta\sigma(\theta)}, \frac{1 - \theta}{\sigma(\theta)} \right\}$$

であり,  $\theta$  の  $K$  上最小多項式は  $\text{Bru}(-\text{sym}_5(R_\theta), \text{sym}_4(R_\theta); X)$  となっている.

## $L$ の Brumer 元

- 条件 (\*) を満たす  $\theta \in L$  を “ $L$  の Brumer 元” と呼ぶ
- $L$  の Brumer 元が求まる毎に  $L = \text{Spl}_K(\text{Bru}(\alpha, \beta; X))$  となる  $(\alpha, \beta) \in K^2$  が求まる.

従って, Brumer 元を計算するシステムティックな方法を考えればよい

定理 (Jensen-Ledet-Yui)

任意の  $x \in L^{\langle \tau \rangle} \setminus K$  に対して, 複比

$$\phi(x) := \frac{(\sigma(x) - \sigma^4(x))(\sigma^2(x) - \sigma^3(x))}{(\sigma(x) - \sigma^3(x))(\sigma^2(x) - \sigma^4(x))}$$

は  $L$  の Brumer 元である. □

(注) この様な  $\{x, \sigma(x), \dots, \sigma^4(x)\}$  の複比は本質的に 1 種類しかない

## Brumer 化の方法

- $f(X) = X^5 - aX^4 + bX^3 - cX^2 + dX - e \in K[X]$  :  $K$  上の 5 次  $D_5$ -多項式
- $\alpha_1, \dots, \alpha_5$  :  $f(X)$  の根
- $G := \text{Gal}(f(X)/K) = \langle \sigma, \tau \rangle$  を  $\sigma = (12345), \tau = (25)(34)$  と表現しておく, つまり  $\tau(\alpha_1) = \alpha_1$  なる様に根のラベリングを定めておく
- $\phi(\alpha_1) = \frac{(\alpha_2 - \alpha_5)(\alpha_3 - \alpha_4)}{(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_5)} =: A$  は  $\text{Spl}_K(f(X))$  の Brumer 元
- $u := -\text{Sym}_5(\text{Orb}_G(A)), v := \text{Sym}_4(\text{Orb}_G(A))$  を計算する

不変式論を使って symbolic に計算したい.

$\alpha_i$  を不定元  $x_i$  で置き換えると,  $u, v$  は 10 次の  $D_5$ -不変式

$p, q, r, \Delta := \prod_{i < j} (x_i - x_j)$  を用いて

$$u = -\frac{p(x_1, \dots, x_5)}{\Delta}, \quad v = \frac{q(x_1, \dots, x_5)}{r(x_1, \dots, x_5)} \text{ と表される.}$$

## 不変式の計算 1

- $D_5$  は  $\mathfrak{A}_5$  に含まれるので,  $\Delta$  は  $f(X)$  の判別式の平方根として計算できる
- $p$  は  $D_5$ -不変式なので,  $\mathfrak{S}_5$ -orbit を根とする 12 次式を作ると, その各係数は  $x_1, \dots, x_5$  の基本対称式になるので, これを因数分解して一次因子の根をとればよい
- この様にして  $p, q, r$  を計算できる筈だが, 5 変数 120 次式の処理が必要であり, この多項式を計算できなかった.
- そこで  $\mathfrak{S}_5$ -orbit ではなく,  $\mathfrak{A}_5$ -orbit から 6 次式を作る
- それでも 次数は 60 であり, 実行できなかった. できたとしても, その後の因数分解は困難だと予想できる.

## 不変式の計算 2

(この部分は星氏との共同研究)

- そこで方針を転換し,  $p, q, r$  を, orbit を使わずに, 直接計算する
- 不変式環  $K[x_1, \dots, x_5]^{\mathcal{D}_5}$  は,  $K$  上 9 個の元

$$\text{Sym}_1(x_1), \dots, \text{Sym}_5(x_1)$$

$$\text{Orb}_{\langle \sigma \rangle}(x_1 x_2), \text{Orb}_{\langle \sigma \rangle}(x_1 x_2 x_3), \text{Orb}_{\langle \sigma, \tau \rangle}(x_1^3 x_2), \text{Orb}_{\langle \sigma, \tau \rangle}(x_1^4 x_2)$$

で生成される.

- $p, q, r$  を, これらの生成元で表示することは, 次数が 10 なので容易にできる.
- 後は, 上の生成元に  $\alpha_1, \dots, \alpha_5$  を代入した結果 ( $\in K$ ) を求めればよいが, 次数が高々 30 程度なので, この計算は前ページの方法で可能である

これで  $f(X)$  の Brumer 化 (の一つ) が完全に計算できたことになる.

## 再 Brumer 化

以上の Brumer 化の方法を  $\text{Bru}(u, v; X) \in K(u, v)[X]$  自身に適用することによって, 以下の結果を得る

定理 (Hoshi-R)

$$\begin{aligned} p(u, v) &:= u^7 + 5u^6 - 8vu^5 - 81u^5 + 8vu^4 + 352u^4 + 12v^2u^3 + 80vu^3 \\ &\quad - 634u^3 - 17v^2u^2 - 182vu^2 + 65u^2 - 7v^2u + 8vu - u + v^4 \\ q(u, v) &:= 4u^5 - 4u^4 - 24vu^3 - 40u^3 - v^2u^2 + 34vu^2 + 91u^2 \\ &\quad + 30v^2u + 14vu - 4u + 4v^3 - v^2 \end{aligned}$$

とすると,  $\text{Bru}(u, v; X)$  と  $\text{Bru}\left(u, \frac{p(u, v)}{q(u, v)}; X\right)$  は  $K(u, v)$  上同じ最小分解体を持つ □

実は, この変換  $(u, v) \mapsto (u, p/q)$  は Kida-Sato-R に於ける楕円曲線の 2 倍写像に相当している!!

## Brumer 化の族 (new result)

- $D_5$ -多項式  $f(X)$  の Brumer 化を一つ計算することができたが,  $f(X)$  にチルンハウス変換  $X \mapsto c_0 + c_1X + c_2X^2 + c_3X^3 + c_4X^4$  を施した後に Brumer 化を施すことによって “Brumer 化の族” をパラメータ一付きで得ることができる
- 判別式の因数分解すら困難. 計算すべき不変式の次数は 4 倍, つまり 120 次程度になっている
- チルンハウス変換による「ずれ」をうまく処理することによって計算することができた
- $\text{Bru}(u, v; X)$  にこの Brumer 化を施して得られる  $u, v$  はテキストファイルで 100 KB ~ 1 MB のオーダー

### 今後の問題

こうして得られた 4 パラメータ一付きの「Brumer 化の族」が, 全ての Brumer 化を尽くしているか? No であれば, “方程式  $\sigma^2(\theta) = \frac{1 - \sigma(\theta)}{\theta}$ ” の複比以外の解を探さなければならない.