パラメーター付き多項式の同型問題について*

陸名 雄一 (早稲田大学)

1 動機とアイデア

1.1 多項式の同型問題

体 K 上の一変数多項式 $f(X) \in K[X]$ の K 上最小分解体を $\mathrm{Spl}_K(f(X))$ で表す. 2 つの多項式 $f(X),\ g(X) \in K[X]$ に対して $\mathrm{Spl}_K(f(X)) = \mathrm{Spl}_K(g(X))$ が成り立つとき, 「$f(X)$ と $g(X)$ は K 上同型である」といい,

$$f(X) \sim_K g(X)$$

と書き表す. また, 拡大 $\mathrm{Spl}_K(f(X))/K$ のガロア群を $\mathrm{Gal}(f(X)/K)$ と書く.

体 k 上の n 変数有理函数体 $k(s_1, \ldots, s_n)$ を係数体に持つ一変数多項式

$$F(s_1, \ldots, s_n; X) \in k(s_1, \ldots, s_n)[X]$$

に対して, $(s_1, \ldots, s_n)$ をパラメーターと見做す. 次の問題は体論に於ける最も基本的な問題の一つである.

問題 (同型判定問題). パラメーター $(s_1, \ldots, s_n)$ の 2 通りの特殊化 $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in k^n$ に対して, $F(a_1, \ldots, a_n; X)$ と $F(b_1, \ldots, b_n; X)$ が k 上同型か否か判定せよ.

この問題は, $F(b_1, \ldots, b_n; X) \in k[X]$ が $\mathrm{Spl}_k(F(a_1, \ldots, a_n; X))$ 上で一次式の積に分解するか否か, と言い換えることができる. 従って, 多項式環 $k[X]$ での因数分解アルゴリズムが確立していればこの問題を解くことができる. 基礎体 k が有限次代数体の場合は, 例えば [Co, Chapter 3] に詳論されており, 種々の代数計算ソフトウェアに実装されている.

この様に具体的に与えられた多項式が同型か否かを “判定” することは (技術的な困難を考慮しなければ) 比較的容易であるが, 次の問題になると格段に難しくなる.

問題 (構成問題). パラメーターの特殊化 $(a_1, \ldots, a_n) \in k^n$ を一つ固定するとき, $F(a_1, \ldots, a_n; X)$ と $F(b_1, \ldots, b_n; X)$ が k 上同型となるような特殊化 $(b_1, \ldots, b_n) \in k^n$ を求めよ.

この問題が完全に解けている様なパラメーター付き多項式は極めて少ないのが現状である.

1.2 多項式の標準化

講演では, 多項式の「標準化」を用いた同型問題へのアプローチについて述べた. これによって “パラメトリック多項式” についての同型問題は, 理論的には, 解決する.

*2007 年 8 月 29 日, 第 2 回福岡数論研究集会

定義 1.1 (パラメトリック多項式). G を有限群とする. 多項式 $F(s_1,\ldots,s_n;X)\in k(s_1,\ldots,s_n)[X]$ は, 以下の条件を満たすとき「パラメトリック (G/k-) 多項式」と呼ばれる:

1. $\mathrm{Gal}(F(s_1,\ldots,s_n;X)/k(s_1,\ldots,s_n))\cong G$.
2. G の任意の部分群 H と 任意の H-ガロア拡大体 K/k に対して, $K=\mathrm{Spl}_k(F(a_1,\ldots,a_n;X))$ となる様なパラメーターの特殊化 $(a_1,\ldots,a_n)\in k^n$ が存在する.

定義 1.2 (多項式の標準化). 体 k 上の G-多項式 $g(X)\in k[X]$ とパラメトリック G/k-多項式 $F(s_1,\ldots,s_n;X)$ に対して,

$$g(X)\sim_k F(a_1,\ldots,a_n;X)$$

となる様な $F(a_1,\ldots,a_n;X)\in k[X]$ を与えることを「g(X) の $F(s_1,\ldots,s_n;X)$ への標準化」と呼ぶ.

以下, $k(s_1,\ldots,s_n)$ 上既約な m 次パラメトリック G/k-多項式 $F(s_1,\ldots,s_n;X)\in k(s_1,\ldots,s_n;X)$ と, $F(s_1,\ldots,s_n;X)$ への標準化を一つ固定する. ここで

$$f(X):=F(a_1,\ldots,a_n;X)\in k[X]$$

が G-多項式になる様な特殊化 $(a_1,\ldots,a_n)\in k^n$ を固定すると, これに対する「構成問題」は以下の様に解決できる.

m 個の不定元 $p_0,\ldots,p_{m-1}$ を新たに導入し, 文字 Y に関する終結式

$$\tilde{f}(p_0,\ldots,p_{m-1};X):=\mathrm{Resultant}_Y\left(f(Y),\ X-\sum_{i=0}^{m-1}p_iY^i\right)$$

を考える. これは $\displaystyle\sum_{i=0}^{m-1}p_iX^i$ による $f(X)$ のチルンハウス変換であり, $p_0,\ldots,p_{m-1}$ を k の元に特殊化することによって $f(X)$ と k 上同型となる m 次多項式を全て得ることができる. この $\tilde{f}(p_0,\ldots,p_{m-1};X)$ の標準化を

$$F(b_1,\ldots,b_n;X)\in k(p_0,\ldots,p_{m-1})[X]$$

とすると $b_1,\ldots,b_n$ は $p_0,\ldots,p_{m-1}$ の k 上の有理函数であり, $p_0,\ldots,p_{m-1}$ を k へ特殊化することによって $F(a_1,\ldots,a_n;X)$ に関する「構成問題」の全ての解を与えることができるのである.

1.3 例: X^3+sX+s

有理数体 $\mathbb{Q}$ 上の 3 次拡大体の定義多項式は

$$F(s;X):=X^3+sX+s\in\mathbb{Q}(s)[X]$$

によってパラメトライズされる. つまり, $F(s;X)$ はパラメトリック $\mathfrak{S}_3/\mathbb{Q}$-多項式である. ($\mathfrak{S}_3$ は 3 次対称群.) 3 次式 $X^3-AX^2+BX-C\in\mathbb{Q}(A,B,C)[X]$ の $F(s;X)$ への標準化として

$$F\left(-\frac{(A^2-3B)^3}{D};X\right)$$

($D := A^2B^2 - 4A^3C - 4B^3 + 18ABC - 27C^2$ は $X^3 - AX^2 + BX - C$ の判別式.) を選ぶことができる (例えば [陸] 参照.)

そこで

$$\begin{aligned}
&\mathrm{Resultant}_Y\left(Y^3 + sY + s,\ X - (p_0 + p_1Y + p_2Y^2)\right)\\
&= X^3 + (2p_2s - 3p_0)X^2\\
&\quad + (p_2^2s^2 + (p_1^2 - 4p_0p_2 + 3p_1p_2)s + 3p_0^2)X\\
&\quad - (p_2^2(p_0 - p_1 + p_2)s^2 - (p_1^3 - p_0p_1^2 + 2p_0^2p_2 - 3p_0p_1p_2)s + p_0^3)
\end{aligned}$$

に上の標準化を施すと

$$F\left(\frac{s(p_2^2s - 3p_1(p_1 + 3p_2))^3}{(4s + 27)(p_2^2(p_1 + p_2)s + p_1^3)^2}; X\right)$$

となる[1]. この p_1, p_2 を $\mathbb{Q}$ へ特殊化することによって $F(a; X) \in \mathbb{Q}[X]$ と $\mathbb{Q}$ 上同型となるような $F(b; X) \in \mathbb{Q}[X]$ を全て得ることができる. 上式は p_1, p_2 について同次であるから, $p = \dfrac{p_1}{p_2}$ として

$$F\left(\frac{s(s - 3p(p + 3))^3}{(4s + 27)((p + 1)s + p^3)^2}; X\right)$$

と書ける. これは $F(s; X)$ の

$$-\frac{s - 3p(p + 3)}{(4s + 27)((p + 1)s + p^3)}(3(2p + 3)X^2 + (2s - 9p)X + 2s(2p + 3))$$

によるチルンハウス変換であることが計算できる.

1.4 多項式の再標準化と同型問題

各パラメトリック多項式に対して上記の計算を実行できればよいのだが, 現実問題として, その計算にはかなりの技術的困難が伴う. そこで構成問題の解を “全て” 求める代わりに “沢山 (できれば無限個)” 求めることへと目標を弱めて[2], 以下の (チルンハウス変換を経由しない) アプローチを考える.

定義 1.3 (多項式の再標準化[3]). パラメトリック G/k-多項式 $F(s_1, \ldots, s_n; X) \in k(s_1, \ldots, s_n)[X]$ への標準化 Φ を一つ固定する. $F(s_1, \ldots, s_n; X)$ 自身に標準化 Φ を施したものを

$$\Phi(F(s_1, \ldots, s_n; X)) = F\left(\Phi(s_1), \ldots, \Phi(s_n); X\right) \in k(s_1, \ldots, s_n)[X]$$

と書いて「Φ による再標準化」と呼ぶことにする.

我々のアプローチは, 一つの特殊化 $F(a_1, \ldots, a_n; X) \in k[X]$ から出発して

$$\Phi(F(a_1, \ldots, a_n; X)), \quad \Phi^2(F(a_1, \ldots, a_n; X)), \quad \Phi^3(F(a_1, \ldots, a_n; X)), \quad \ldots$$

と Φ を繰返していけば構成問題の解の列が得られるのではないか, という素朴なアイデアに基づくものである.

[1] $4s + 27 = 0$ のとき, $F(s; X)$ は $\mathbb{Q}$ 上可約.

[2] 一般に, 構成問題の解は一つ求めるだけでも困難である.

[3] $F(s_1, \ldots, s_n; X)$ の形を得るのが標準化だからこの様に名付けたのだが, もっと良い言い方があるかもしれない.

先に例示したパラメトリック $\mathfrak{S}_3/\mathbb{Q}$-多項式

$$F(s;X) = X^3 + sX + s \in \mathbb{Q}(s)[X]$$

への標準化

$$X^3 - AX^2 + BX - C \longmapsto F\left(-\frac{(A^2-3B)^3}{A^2B^2 - 4A^3C - 4B^3 + 18ABC - 27C^2}; X\right)$$

を Φ とすると, $F(s;X)$ の Φ による再標準化として

$$\Phi(F(s;X)) = F\left(-\frac{27s}{4s+27}; X\right)$$

を得る. 従って

$$\phi:\ s \longmapsto -\frac{27s}{4s+27}$$

とすると, 各 $a \in \mathbb{Q} \setminus \{-27/4\}$ に対して

$$F(\phi(a);X), \quad F(\phi^2(a);X), \quad F(\phi^3(a);X), \quad \ldots$$

は $F(a;X)$ に対する構成問題の解の一部を与えている. しかし $\phi^2(s) = s$ であるから, 実は, この方法は構成問題の解を一つしか与えていない.

この例だけを看ると上の方法の効力は疑わしいのであるが, 講演では Brumer の 5 次多項式について非自明な解の列を発見する経緯を示して "再標準化の手法" の有用性を示した.

2 $\mathcal{D}_5$-多項式の再 Brumer 化

$\mathcal{D}_5$ を位数 10 の二面体群とする. 「Brumer 多項式」

$$\mathrm{Bru}(s,t;X) := X^5 + (s-3)X^4 - (s-t-3)X^3 + (s^2-s-2t-1)X^2 + tX + s \in \mathbb{Q}(s,t)[X]$$

はパラメトリック $\mathcal{D}_5/\mathbb{Q}$-多項式である. 従って $\mathbb{Q}$ 上の任意の $\mathcal{D}_5$ 多項式を $\mathrm{Bru}(s,t;X)$ へ標準化することができる. これを「Brumer 化」と呼ぶことにする. 具体的な Brumer 化を得る方法は, Brumer 多項式がパラメトリックであることの "構成的証明" (例えば [JLY, §2.3] 参照) を辿れば得ることができる. しかしこの方法は極めて複雑な $\mathcal{D}_5$-不変式の計算を経由しており, 汎用的な "アルゴリズム" は知られていなかったが, [陸, HR] によって具体的な方法が提示された. この方法は "シンボリック" に実行できるので Brumer 化の「公式」と見做すことができる.

この Brumer 化 Φ によって $\mathrm{Bru}(s,t;X)$ を "再 Brumer 化" すると次の様になる:

$$\Phi(\mathrm{Bru}(s,t;X)) = \mathrm{Bru}(s,\varphi(s,t);X),$$

$$\varphi(s,t) := \frac{\begin{pmatrix} t^4 + s(3s+1)(4s-7)t^2 - 2s(4s^4 - 4s^3 - 40s^2 + 91s - 4)t \\ \qquad + s(s^6 + 5s^5 - 81s^4 + 352s^3 - 634s^2 - 65s - 1) \end{pmatrix}}{4t^3 - (s^2 - 30s + 1)t^2 - 2s(3s+1)(4s-7)t + s(4s^4 - 4s^3 - 40s^2 + 91s - 4)}.$$

Φ が s を動かさないことに注意しておく.

この結果から

$$\mathrm{Bru}(s,\varphi(s,t);X),\quad \mathrm{Bru}(s,\varphi^2(s,t);X),\quad \mathrm{Bru}(s,\varphi^3(s,t);X),\quad \dots$$

が Brumer 多項式 $\mathrm{Bru}(s,t;X)$ と同型な多項式を与えることがわかる. 例えば,

$$\mathrm{Bru}(1,0;X),\quad \mathrm{Bru}\left(1,-\frac{293}{47};X\right),\quad \mathrm{Bru}\left(1,-\frac{2382701963376597}{52653150779963};X\right),\quad \dots$$

は $\mathbb{Q}$ 上同型である.

3 再 Brumer 化 $(s,t)\longmapsto(s,\varphi(s,t))$ の意味

講演の主眼は前章の再 Brumer 化

$$\Phi:\ \mathrm{Bru}(s,t;X)\longmapsto \mathrm{Bru}(s,\varphi(s,t);X)$$

の持つ意味の解明にあった. これを述べる為に, 拡大 $\mathrm{Spl}_{\mathbb{Q}(s,t)}(\mathrm{Bru}(s,t;X))/\mathbb{Q}(s,t)$ が含む 2 次中間体に着目する.

多項式 $\mathrm{Bru}(s,t;X)$ の判別式は

$$s^2(-4t^3+(s^2-30s+1)t^2+2s(3s+1)(4s-7)t-s(4s^4-4s^3-40s^2+91s-4))^2$$

であり,

$$\Delta(s,t):=-4t^3+(s^2-30s+1)t^2+2s(3s+1)(4s-7)t-s(4s^4-4s^3-40s^2+91s-4)$$

とすると $\mathcal{D}_5$-拡大 $\mathrm{Spl}_{\mathbb{Q}(s,t)}(\mathrm{Bru}(s,t;X))/\mathbb{Q}(s,t)$ が含む唯一の 2 次中間体は

$$\mathbb{Q}(\sqrt{\Delta(s,t)})$$

であることが知られている ($\varphi(s,t)$ の分母が $-\Delta(s,t)$ になっている). 従って, $(a,b),(z,x)\in\mathbb{Q}^2$ に対して

$$\begin{aligned}\mathrm{Bru}(a,b;X)\sim_{\mathbb{Q}}\mathrm{Bru}(z,x;X)&\Longrightarrow \mathbb{Q}(\sqrt{\Delta(a,b)})=\mathbb{Q}(\sqrt{\Delta(z,x)})\\&\Longleftrightarrow \Delta(a,b)y^2=\Delta(z,x)\qquad(\exists y\in\mathbb{Q}^\times)\\&\Longleftrightarrow (x,y,z)\text{ は代数曲面 }S_{a,b}:\ \Delta(a,b)Y^2=\Delta(X,Z)\text{ の}\\&\qquad\mathbb{Q}\text{-有理点 }(y\neq 0)\end{aligned}$$

が成立する. 再 Brumer 化 Φ が s を動かさないことを鑑み, 上の議論を $z=a$ と特殊化すると次の様になる.

$$\begin{aligned}\mathrm{Bru}(a,b;X)\sim_{\mathbb{Q}}\mathrm{Bru}(a,x;X)&\Longrightarrow \mathbb{Q}(\sqrt{\Delta(a,b)})=\mathbb{Q}(\sqrt{\Delta(a,x)})\\&\Longleftrightarrow \Delta(a,b)y^2=\Delta(a,x)\qquad(\exists y\in\mathbb{Q}^\times)\\&\Longleftrightarrow (x,y)\text{ は楕円曲線 }E_{a,b}:\ \Delta(a,b)Y^2=\Delta(X,a)\text{ の}\\&\qquad\mathbb{Q}\text{-有理点 }(y\neq 0).\end{aligned}$$

講演での主結果は次の定理である.

定理 3.1. Brumer 化 Φ が導く写像 $x \longmapsto \varphi(a,x)$ は楕円曲線 $E_{a,b}$ の 2 倍写像である.

注意すべき点の第一は, Brumer 化 Φ は純粋に $\mathcal{D}_5$-不変式の計算によるものであり, 楕円曲線 $E_{a,b}$ とは全く無関係に構成されているということである. この事実は, Φ を実際に構成した講演者にとって驚きであった.

第二の注意点は上の結果が, モーデル＝ヴェイユ群 $E_{a,b}(\mathbb{Q})$ が「"最小分解体が $\mathbb{Q}(\sqrt{\Delta(a,b)})$ を含む様な $\mathrm{Bru}(a,x;X)$ の同型類" の統制」に寄与しているであろう, という示唆を与えていることである. 以下に示す [KRY] の結果はこの示唆に強い根拠を与えている.

定理 3.2 (Kida-Renault-Yokoyama). $(x,y) \in E_{1,0}(\mathbb{Q})$ とする. $\mathrm{Bru}(1,x;X) \in \mathbb{Q}[X]$ が $\mathbb{Q}$ 上既約ならば常に

$$\mathrm{Bru}(1,x;X) \sim_{\mathbb{Q}} \mathrm{Bru}(1,0;X)$$

が成り立つ. また, この様な $(x,y) \in E_{1,0}(\mathbb{Q})$ は無限個存在する.

また, 木田雅成氏 (電気通信大) によって次の実験結果が得られ, 後に共同研究 [KRS] によって証明が与えられた. 楕円曲線

$$E_{2,2}:\ 296Y^2 = 4X^3 + 55X^2 - 28X + 100$$

のモーデル＝ヴェイユ群 $E_{2,2}(\mathbb{Q})$ は $\mathbb{Z}^{\oplus 3}$ と同型であり,

$$P_1 := (26,19), \qquad P_2 := \left(-\frac{29}{4}, \frac{19}{8}\right), \qquad P_3 := \left(-\frac{1}{8}, -\frac{19}{32}\right)$$

によって生成される.

$$H := \langle P_1 + 4P_2 + 2P_3,\ 5P_2,\ 5P_3 \rangle$$

とすると $E_{2,2}(\mathbb{Q})/H$ の位数は 25 であり, 位数 5 の部分群を 6 個持つ. この 6 個の部分群 $H_1, \ldots, H_6$ の代表元は以下の通り.

部分群	H_1	H_2	H_3	H_4	H_5	H_6
代表元	$Q_1 := P_2$	$Q_2 := P_3$	$Q_3 := P_2 + P_3$	$Q_4 := P_2 + 2P_3$	$Q_5 := P_2 - 2P_3$	$Q_6 := P_2 - P_3$
x 座標	$-\frac{29}{4}$	$-\frac{1}{8}$	$\frac{233}{36}$	$\frac{15619}{2500}$	$\frac{40091}{676}$	$-\frac{7}{4}$

点 $(2,2) \in E_{2,2}(\mathbb{Q})$ は H_6 に属する.

定理 3.3 (Kida-Rikuna-Sato). $P = (x,y) \in E_{2,2}(\mathbb{Q})$ に対し $\mathrm{Bru}(2,x;X)$ を単に $\mathrm{Bru}(P;X)$ と記すことにすると, 以下が成立する:

1. $P \in H$ ならば $\mathrm{Bru}(P;X)$ は $\mathbb{Q}$ 上可約.
2. $\mathrm{Bru}(Q_i;X)$ $(i = 1, \ldots, 6)$ は互いに $\mathbb{Q}$ 上同型ではない.
3. $P \notin H$ が H_i に属するならば $\mathrm{Bru}(P;X)$ と $\mathrm{Bru}(Q_i;X)$ は $\mathbb{Q}$ 上同型である.

同様の現象が一般の a,b に対しても起きていることが [KRS] によって, 楕円曲線のクンマー理論を用いて証明されている. この結果によって, 「s と中間の 2 次体を固定した場合の $\mathrm{Bru}(s,t;X)$ の同型問題」は完全に解決されたことになる.

参考文献

[Co] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138, Springer, 1996.

[HR] A. Hoshi and Y. Rikuna, *On a transformation from dihedral quintic polynomials into Brumer's form*, in preparation.

[JLY] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials, Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications 45, Cambridge University Press, 2002.

[KRS] M. Kida, Y. Rikuna, and A. Sato, *Classifing Brumer's quintic polynomials by a weak Mordell-Weil group*, preprint.

[KRY] M. Kida, G. Renault, and K. Yokoyama, *Quintic polynomials of hashimoto-tsunogai, brumer, and kummer*, preprint.

[陸] 陸名雄一, 生成的多項式の変換問題について, 第 1–2 回室蘭数論研究集会報告集, 2007.