数理解析研究所講究録
941 巻 1996 年 57-72

9.

A_5 を Galois 群に持つ6次式の族 – 分解体と Galois 群の計算 –

穴井 宏和 (富士通情報研)
近藤 武 (東京女子大学)

9.1 はじめに

まず、本稿の内容は研究集会「代数学と計算」(於 東京都立大) で発表したものを修正加筆したものであることを御断りしておく。

本稿では, ある 6 次式の族に着目し, Galois 理論および代数的整数論の観点から考察する. これらの 6 次式は Galois 群として 5 次交代群 A_5 をもつよい族を与える. この考察において, いくつかの定理が実際に数式処理 (Computer Algebra) の理論とシステムの助けを得て示される. それらの様子を中心に述べ, さらに, その礎となる計算アルゴリズム, 代数拡大体上の因数分解そして分解体の計算法, についても触れることにする.

本稿の内容は, 数式処理の立場から見た場合, 有理関数体上の一変数多項式の Galois 群の決定と分解体の計算の 2 つが中心となるが, その意義は, 代数的算法自体の進展というよりも数式処理研究の純粋数学 (整数論) の研究への貢献という点にある. 本稿中, 数式処理 (Computer Algebra) を利用した計算は, 富士通情報研で開発中の「数式処理システム Risa/Asir」[18] を用いて行なった. 計算に使用した計算機は, RISC NEWS (cpu: R4000(50MHz)) を用いた.

9.2 問題の背景

有理数体 $\mathbf{Q}$ 上の既約な n 次多項式 $f(x)$ の Galois 群は n 次対称群 S_n の可移部分群である. よって, Galois 群を考えると $\mathbf{Q}$ 上の既約な n 次の多項式は S_n の可移部分群により類別できる. しかし, このような分類すなわち "ある S_n の部分群を Galois 群にもつ n 次多項式を求める" という問題 (**Galois 群の逆問題**) は一般には解決されていない. (多項式の Galois 群を決定する問題については, 大きく 3 つのアプローチが提案され, それらの算法は実際にいくつかの数式処理システムにも実装されている ([2] 参照).)

6 次の場合, S_6 の可移部分群は 16 個存在し, それらを Galois 群とするような 6 次式が存在することは知られている. (これら可移部分群を Galois 群にもつ多項式については [1] 参照.) 16 個の可移部分群のうち非原始的なものについては, それを Galois 群とするような 6 次式の満たすべき条件がほとんどの群に対して得られている. それに対し原始群の場合 ($S_6, A_6, S_5(=G_{120}), A_5(=G_{60})$) はいずれの場合もそのような条件を見つかってはいず, 容易ではない. (例えば, 一般に n 次の交代群 A_n を Galois 群とする n 次多項式を捉えることはかなり難しい. ただし A_4 を Galois 群とするような 4 次式の一般的な構成法については [1] に見られる.)

そこで, 例えば, 本稿で対象とする A_5 を Galois 群に持つ 6 次式の族が " $\mathbf{Q}$ 上の A_5-拡大 (特に 2 次体上の不分岐 A_5-拡大を与える) 6 次式のうちどの位をカバーするのか？ " ということを考察する. こうして 原始群を Galois 群に持つ場合の Galois 群の逆問題の答を探っていこうという訳である. この意味で, Galois 群として原始群をもつような多項式の族を考察する意義は大きい.

9.3 6次式の族 $f(x;b,c,d)$

本稿の主役となる 6 次式は以下で与えられる :

$$\begin{aligned} f(x;b,c,d) &= x^6+2cx^5+(c^2+2c+2)x^4+(2c^2+2c+2)x^3+(c^2+4c+5)x^2 \\ &\quad +(2c+6)x+1-bdx^2(x+1)^2+b(x+1)^3-4dx^3 \\ &= x^6+2cx^5+(-db+c^2+2c+2)x^4+((-2d+1)b+2c^2+2c-4d+2)x^3 \\ &\quad +((-d+3)b+c^2+4c+5)x^2+(3b+2c+6)x+b+1. \end{aligned}$$

ここで, b,c,d は有理数あるいは有理数体 $\mathbf{Q}$ 上独立な不定元である. この式は, A.Brumer が種数 2 の代数曲線の族でそのヤコビ多様体の準同型環が $\mathbf{Q}(\sqrt{5})$ を含むようなものとして構成したものらしく, M. Olivier [12] の文献表中に [13] として出典が示されているが, [13] はその後出版された気配がなく未だ見る機会を得ていない. この 6 次式の Galois 群は, 殆どの場合に A_5 (A_6 ではない) で整数論的に大変面白い性質がある. A.Brumer の本来の構成意図とは無関係にこの 6 次式の族を Galois 理論および代数的整数論の観点から考察する.

9.3.1 判別式

$f(x;b,c,d)$ の判別式 $d(b,c,d)$ は次のようになる：

$$d(b,c,d) = \delta(b,c,d)^2$$

ここで,

$$\begin{aligned}\delta(b,c,d) = {} & 16dbc^6 + ((-144d+16)b - 64d)c^5 + ((-48d^2-4d)b^2 + (-16d^2+192d-144)b + 384d - \\ & 64)c^4 + ((288d^2-160d-4)b^2 + (832d^2+1008d+208)b + 64d^2+320d+384)c^3 + ((48d^3 + \\ & 8d^2)b^3 + (32d^3-608d^2+1336d-108)b^2 + (-1280d^2+1184d+896)b - 2304d^2 - 2752d + \\ & 256)c^2 + ((-144d^3+144d^2+36d)b^3 + (-768d^3+528d^2-2880d+1008)b^2 + (-576d^3 - \\ & 1536d^2-10032d+432)b - 4032d^2 - 9408d - 2496)c + (-16d^4-4d^3)b^4 + (-16d^4+416d^3 + \\ & 24d^2+108d+27)b^3 + (2112d^3-1824d^2-264d-2268)b^2 + (3456d^3-6096d^2-1936d - \\ & 7744)b + 1728d^3 - 5184d^2 - 2176d - 6592.\end{aligned}$$

まず注意すべきは, 判別式が平方数であるから次を得る:

命題 1 $f(x;b,c,d)$ の $\mathbf{Q}(b,c,d)$ 上の *Galois* 群は *6* 次交代群 A_6 の部分群である.

この判別式の計算は, 未定係数法によっても求めることができる (2 日ほどかかった) が, Risa/Asir で $f(x;b,c,d)$ とその導関数の終結式として直接計算して 52.580 sec で得られる. またその因数分解は 980 msec で得られる.

9.3.2 主結果

この 6 次式の族について次の 2 つの定理が成り立つ:

定理 2 b,c,d を有理数体 $\mathbf{Q}$ 上独立な不定元とするとき, $f(x;b,c,d)$ の $\mathbf{Q}(b,c,d)$ 上の *Galois* 群は *(6* 次置換群と見て*)* *5* 次交代群 A_5 と同型である.

証明は §3.5 で述べる. この定理より $b,c,d \in \mathbf{Q}$ のとき, $f(x;b,c,d)$ の $\mathbf{Q}(b,c,d)$ 上の Galois 群は一般には A_5 に同型である (Hilbert の既約性定理). しかし, $f(x;b,c,d)$ $b,c,d \in \mathbf{Q}$ が $\mathbf{Q}$ 上既約であっても Galois 群が A_5 とは限らない. 実際,

$$f(x;-2,0,d) = x^6 + (2d+2)x^4 + (2d-1)x^2 - 1$$

の Galois 群は 4 次交代群 A_4 と同型である. なお, $f(x;b,c,d)$ の定数項は $b+1$ であるから $b=-1$ のとき $f(x;b,c,d)$ は可約である. このとき, 5 次式の族 $f(x;-1,c,d)/x$ は Galois 群が位数 10 の正 2 面体群 D_{10} の大変良い族を与えるが, これについては §4 にて述べる.

定理 3 $f(x;b,c,d) \in \mathbf{Z}[x]$ とする *(*$b,c,d \in \mathbf{Q}$ であるが, 有理整数である必要はない*)*. $f(x;b,c,d)$ の *Galois* 群は A_5 とする. さらに

($\star$) $\delta(b,c,d)$ が平方因子を持たない

と仮定する. m を $\delta(b,c,d)|m$ なる平方因子のない有理整数とするとき, 2 次体 $\mathbf{Q}(\sqrt{m})$ 上の $f(x;b,c,d)$ の分解体は不分岐 A_5-拡大である.

証明は [11] 参照.

注意 1 *(1)* 数値を実際に入れて確かめてみればわかるように定理 3 の条件 ($\star$) を満たす b,c,d はたくさん *(恐らく無限に)* 存在する. $\delta(b,c,d)$ が素数である b,c,d ですら無限に存在すると思われるが確認していない. $\delta(b,c,d)$ が素数である $f(x;b,c,d)$ の例は *[11]* に見られる.

(2) ($\star$) のもとで *1* つの $f(x;b,c,d)$ は無限に多くの 2 次体の上の不分岐 A_5-拡大を与える.

(3) $b=4b'+1, c=c'+\frac{1}{2}, d=d'+\frac{1}{4}(b',c',d'\in\mathbf{Z}[x])$ のとき, $f(x;b,c,d)\in\mathbf{Z}[x]$ である.

9.3.3 6 次式の 15 次分解式 (Resolvent)

L を体として多項式環 $L[x]$ の 6 次式 $f(x)$ をとる. $f(x)$ の根を $\theta_1,\theta_2,\cdots,\theta_6$ として

$$\theta_p\theta_q+\theta_r\theta_s+\theta_t\theta_u \quad \{p,q,r,s,t,u\}=\{1,2,3,4,5,6\} \quad (\#)$$

なる形の 15 個の式を考え, これらを根とする 15 次式

$$F_{15}(y;f)=\prod(y-(\theta_p\theta_q+\theta_r\theta_s+\theta_t\theta_u))$$

を $f(x)$ の 15 次分解式という. 明らかに $F_{15}(y;f)\in L[x]$ である.

注意 2 分解式について より一般的な定義を述べておく. $f(x)$ を n 次の多項式としその根を $\theta_1,\cdots,\theta_n$ とする. G を S_n の部分群とする. 群 G がある集合 E に作用しているとき, E の部分集合 A に対して $Stab_G(A)$ で G における A の固定部分群を表すとする. $\Phi\in L[x_1,x_2,\cdots,x_n]$ を $Stab_{S_n}(\Phi)=G$ なる多項式とする. この Φ を G-不変式という. このとき

$$\mathcal{L}(y;f)=\prod_{\sigma\in(S_n//G)}(y-\widetilde{\sigma\Phi})$$

を絶対 G-分解式という. ここで, $(S_n//G)$ は S_n における G の左剰余類の代表系である. また $h\in L[x_1,x_2,\cdots,x_n]$ に対して $\tilde{h}$ は h の f の根による特殊化 $\tilde{h}=h(\theta_1,\cdots,\theta_n)$ を表す. *(位数 48 の S_6 の可移部分群 G_{48} を考えて, $G=G_{48}$, $\Phi=x_1x_2+x_3x_4+x_5x_6$ に対する絶対 G_{48}-分解式がここでいう 15 次分解式 $F_{15}(y;f)$ である.)*

このとき次の補題が成立する :

補題 4 $F_{15}(y;f)$ が $L[x]$ において, *5* 次既約式と *10* 次既約式の積に分解すれば $f(x)$ の L 上の *Galois* 群は *5* 次対称群 S_5 あるいは *5* 次交代群 A_5 に同型である.

(証明) 6 次対称群の可移部分群は (1)(原始群) S_6, A_6, (6 次置換群と見た)S_5, A_5 (2)(非原始群) レス (Wreath) 積 $S_3\int S_2$ (位数 72), $S_2\int S_3$ (位数 48) の部分群である. ここに挙げた 6 つの群のそれぞれを (#) の 15 個の式に作用させて軌道分解するとその軌道の長さは

15 (S_6), 15 (A_6), 5+10 (S_5), 5+10 (A_5), 6+9 ($S_3 \int S_2$), 1+6+8 ($S_2 \int S_3$)

となる. (これは, それぞれの群に対する絶対分解式の既約因子の次数に一致する.) 既約式 $f(x)$ の Galois 群はこれら 6 つの群のうちの一つ (あるいはその部分群) であり, $F_{15}(x;f)$ の $L[x]$ における因子として軌道の長さを次数とするもの (一つの既約式のベキ) が得られる. このことより補題は明らか. Q.E.D.

注意 3 S_n の部分群 G に対する絶対 G-分解式の $\mathbf{Q}$ 上の既約因子の次数と f の *Galois* 群の S_n/G への軌道分解とは *1* 対 *1* に対応する. 絶対 G-分解式の既約因子の次数のパターン *(partition* という*)* は G と S_n の抽象部分群としての f の *Galois* 群 $Gal_{\mathbf{Q}}(f)$ にのみ依存する. *(partition* を $[Gal_{\mathbf{Q}}(f), H]$ と書く.*)* よって一度 S_n の全ての部分群 G, H について, それらの *partition* $[G, H]$ の *(*正方の*)* 表を構成すれば, *(*この次数については*)* *Galois* 群を決めることが可能となる. このような絶対 G-分解式の因数分解を利用した多項式の *Galois* 群の決定の方法はいくつか提案され, 次数に制限はあるものの実際に計算機に実装されている. *([2],[4]~[10], [14], [16],[17]* 参照. *)*

9.3.4 15 次分解式の計算

一般に, 分解式の計算には, (a) Gröbner 基底の計算を利用するものや (b) (基本) 対称式を利用するものなどいくつか挙げられるがここでは $f(x;b,c,d)$ の 15 次分解式 $F_{15}(y;f)$ の場合に対して (a)(b) の方法について簡単に述べる. まず, $f(x;b,c,d)$ の根 $r_1,\cdots,r_6$ を不定元と考えて 15 次分解式

$$F_{15}(y;f) = y^{15} + C_{14}(r_1,\cdots,r_6)y^{14} + \cdots + C_1(r_1,\cdots,r_6)y + C_0(r_1,\cdots,r_6)$$

を構成する (72.120 sec). ここで残された問題は,

(†)「各係数 $C_i(r_1,\cdots,r_6)$ を $f(x;b,c,d)$ の係数で表す, すなわち b,c,d の多項式として表す」

ことである.

(a) さて, $f(x;b,c,d)$ の根 $r_1,r_2,\cdots,r_6$ の基本対称式 (elementary symmetric function) を:

$$\left\{\begin{array}{ll} \sigma_1 = & r_1+r_2+\cdots+r_6, \\ \sigma_2 = & r_1r_2+r_1r_3+\cdots+r_2r_3+\cdots+r_5r_6, \\ & \cdots \\ \sigma_6 = & r_1r_2\cdots r_6 \end{array}\right. \quad \cdots (S)$$

とする. ここで, $f(x;b,c,d)$ の係数より

$$\left\{\begin{array}{ll} \sigma_1 = & -2c, \\ \sigma_2 = & -db+c^2+2c+2, \\ \sigma_3 = & (2d-1)b-2c^2-2c+4d-2, \\ \sigma_4 = & (-d+3)b+c^2+4c+5, \\ \sigma_5 = & -3b-2c-6, \\ \sigma_6 = & b+1 \end{array}\right. \quad \cdots (C)$$

である. 多項式集合 (S) により生成される $Q(b,c,d)[r_1,r_2,\cdots,r_6]$ のイデアルを $\mathcal{J}$ とする. $\mathcal{J}$ の

Gröbner 基底を $\mathcal{G}$ とする. (実際には $\mathcal{G}$ は多項式集合 $S \cup \{f(r_1; b, c, d), \cdots, f(r_6; b, c, d)\}$ の変数順序 (‡) $b \prec c \prec d \prec r_1 \prec r_2 \prec \cdots \prec r_6$ の辞書式順序での Gröbner 基底として 1.092 sec で計算される.) このとき, 各係数 $C_i(r_1, \cdots, r_6)$ $(i = 14, \cdots, 0)$ に対して $\mathcal{G}$ についての正規形 (normal form) を (変数順序 (‡) の辞書式順序で) 計算すれば, $r_1, \cdots, r_6$ が消去できて (†) の目的は達成される. とはいえ, $F_{15}(y; f)$ の低次の係数はかなり大きくなる. 実際以下に示すように次数が小さくなるにつれその次数に対する係数 $C_i(r_1, \cdots, r_6)$ の正規形の計算時間が指数的に増大して全ての係数について計算するのはほとんど不可能である:

次数 i	14	13	12	11	10	9	8	7	6	$\cdots$	0
時間 (sec)	0.02	0.08	0.90	8.77	80.23	577.93	3722.61	15254.3	-	-	-

(b) そこで, 各係数 $C_i(r_1, \cdots, r_6)$ は根の対称式であることに着目する. まず, よく知られた次の定理を思い起こそう [21].

定理 5 *(対称式の基本定理)* n 次の任意の対称式 $\psi(x_1, \cdots, x_n) \in \mathbf{Q}[x_1, \cdots, x_n]$ は基本対称式 $\sigma_1(x_1, \cdots, x_n)$, $\cdots$, $\sigma_n(x_1, \cdots, x_n)$ の多項式として一意に表される:

$$\psi(x_1, \cdots, x_n) = p(\sigma_1, \cdots, \sigma_n).$$

(証明) k 次の対称式 $P(x_1, \cdots, x_n) \in \mathbf{Q}[x_1, \cdots, x_n]$ が与えられたとする. P の各項を全次数辞書式順序 "$\prec$" に従って並べる. この順序では 2 つの単項式 $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, $x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ に対して全次数について $\sum \alpha_i < \sum \beta_i$ であるか, あるいは $\sum \alpha_i = \sum \beta_i$ のときに最初の 0 でない差 $\alpha_i - \beta_i$ が負であるとき, $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \prec x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ である. 任意の多項式 $h \in \mathbf{Q}[x_1, \cdots, x_n]$ の順序 $\prec$ について最大の単項式を頭単項式 (head monomial) と言い $HM(h)$ と表すとする.

$HM(P) = c \cdot x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ とする. P のある単項式 $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ に対して 指数 α_i を置換した指数を持つような全ての単項式が P には現れる. よって $e_1 \geq e_2 \geq \cdots \geq e_n$ である. 次に

$$P' = P - c \cdot \sigma_1^{e_1 - e_2} \sigma_2^{e_2 - e_3} \cdots \sigma_{n-1}^{e_{n-1} - e_n} \sigma_n^{e_n}$$

とする. ここで, 基本対称式の積 $c \cdot \sigma_1^{e_1 - e_2} \sigma_2^{e_2 - e_3} \cdots \sigma_n^{e_n}$ の頭項は $c x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ であり $HM(P)$ に等しい. よって, P' はより次数の小さい対称式になっていることが分かる. P' が定数多項式でなければ, P' を P として以下同様の手順を繰り返す. 最終的には P' は定数多項式となる. (P' の構成よりこの手順の停止性は明らか.) 各ステップにおいて P から引く頭項が P と等しい基本対称式の積の和が P の基本対称式の多項式としての表現を与える. 最終的に各段階での被加数の和をとれば P の基本対称式による表現が得られる. また, こうして得られた P の基本対称式による表現は一意的な表現であるがその証明は割愛する. Q.E.D.

この証明は, 任意の対称式を基本対称式の多項式として表すアルゴリズムを与える. この方法に従って $F_{15}(y; f)$ の全ての係数の基本対称式による表現を求めるてみると 12332.893 sec で計算できた. 後は, 基本対称式にそれぞれ (C) を代入して $F_{15}(y; f)$ の計算が終了するが, これはは数秒で得られる. (結果については §2.5 参照.)

(a) の方法は分解式の係数の持つ対称性を無視した方法といえるのに対し (b) は逆にその対称性を積極的に利用することで計算の劇的な効率化が可能となっている. 数式処理で, 例えば Galois 群の決定のアルゴリズムにおいて, 主として実際に分解式を計算するのに用いられるのは対称式を用いた方法である.

9.3.5 定理 2 の証明

定理 2 は $f(x;b,c,d)$ の 15 次分解式 $F_{15}(y;f)$ が上の補題 4 の条件を満たすことを検証して証明するのであるが, 問題はこの分解式の計算である. 実際に, (a)(b) の手法で分解式を計算してみると, (a) の方法では 3 日かけても結果は得られないが, (b) の方法では 約 3 時間半ほどで計算できる. この分解式を書き下すと A4 の用紙に隙間なくプリントして数ページにも及ぶ大きな式になる. 因数分解した結果は, $F_{15}(y;f) = F_1(y;b,c,d)\cdot F_2(y;b,c,d)$ である. ここで, $deg_y(F_1) = 5$, $deg_y(F_2) = 10$ となる. この因数分解は 6.660sec で得られる. 因数分解した結果を以下に示す:

$$F_1 = y^5 + (db - c^2 - 2c - 2)y^4 + (((-4d+2)c + 2d - 6)b + 4c^3 + 2c^2 + (-8d-4)c - 10)y^3 + ((-2d^2 - 4d - 1)b^2 + ((8d-8)c^2 + (-12d+30)c - 16d^2 - 14d - 20)b - 6c^4 - 4c^3 + (16d+18)c^2 + 48c - 16d^2 - 8d - 32)y^2 + (((4d^2+14d+4)c - 19d^2 - 34d - 9)b^2 + ((-8d+10)c^3 + (30d-38)c^2 + (8d^2 - 8d + 26)c - 64d^2 - 70d + 2)b + 4c^5 + 5c^4 + (-8d-16)c^3 + (16d-62)c^2 + (-24d+52)c - 48d^2 - 16d + 33)y + d^3b^3 + ((-3d^2 - 12d - 4)c^2 + (22d^2+50d+18)c - 52d^2 - 72d - 27)b^2 + ((3d-4)c^4 + (-20d+14)c^3 + (16d-8)c^2 + (48d^2 + 88d + 14)c - 168d^2 - 215d - 72)b - c^6 - 2c^5 + 4c^4 + (-16d+24)c^3 + (24d-21)c^2 - 30c - 144d^2 - 168d - 54.$$

$$F_2 = y^{10} + (2db - 2c^2 - 4c - 4)y^9 + (d^2b^2 + (-2dc^2 + (-12d+4)c - 12)b + c^4 + 12c^3 + 12c^2 - 16dc - 16)y^8 + (((-8d^2+4d)c + 2d^2 - 20d - 2)b^2 + ((16d-4)c^3 + (28d-12)c^2 + (-16d^2 - 12d + 64)c - 32d^2 - 22d + 38)b - 8c^5 - 30c^4 + (16d-36)c^3 + (64d+62)c^2 + (80d+212)c - 32d^2 + 56d + 98)y^7 + ((-2d^3 - 8d^2 - 2d)b^3 + ((30d^2 - 24d + 6)c^2 + (-20d^2 + 150d - 12)c - 32d^3 + 28d^2 - 20d + 31)b^2 + ((-54d+32)c^4 + (-40d-38)c^3 + (128d^2 + 24d - 156)c^2 + (88d^2 + 388d - 218)c - 32d^3 + 184d^2 - 126d + 120)b + 26c^6 + 60c^5 + (-96d + 28)c^4 + (-152d-284)c^3 + (96d^2 - 232d - 694)c^2 + (64d^2 - 176d - 632)c + 112d^2 - 312d + 6)y^6 + (((12d^3 + 58d^2 - 4)c + 10d^3 - 30d^2 + 35d + 12)b^3 + ((-68d^2 + 44d - 48)c^3 + (34d^2 - 436d + 173)c^2 + (152d^3 - 36d^2 + 114d - 232)c + 164d^2 + 188d - 46)b^2 + ((100d-102)c^5 + (94d+178)c^4 + (-368d^2 - 24d + 526)c^3 + (-256d^2 - 1360d + 504)c^2 + (384d^3 - 408d^2 - 168d - 1174)c - 16d^3 + 536d^2 + 80d - 832)b - 44c^7 - 138c^6 + (216d+60)c^5 + (512d+1036)c^4 + (-384d^2 + 248d + 1448)c^3 + (-496d^2 - 1080d + 440)c^2 + (256d^3 - 416d^2 - 488d - 1392)c + 368d^2 - 136d - 1082)y^5 + ((d^4 + 8d^3 + 18d^2 + 8d + 1)b^4 + ((-28d^3 - 172d^2 + 72d + 32)c^2 + (-56d^3 + 220d^2 - 342d - 114)c + 32d^4 + 250d^3 - 106d^2 + 76d + 40)b^3 + ((94d^2 + 150)c^4 + (96d^2 + 616d - 570)c^3 + (-288d^3 - 438d^2 - 68d + 384)c^2 + (-232d^3 - 388d^2 - 1818d + 768)c + 288d^4 + \cdots$$

因に、F_2 を全て記述するには以降本稿のページで 2 ページ分程必要である。

9.4 5次式の族 $f(x;-1,c,d)/x$

$b=-1$ のとき, $g(x;c,d)=f(x;-1,c,d)/x$ とおくと 5 次式 :

$$g(x;c,d)=x^5+2cx^4+(c^2+2c+d+2)x^3+(2c^2+2c-2d+1)x^2$$
$$+(c^2+4c+d+2)x+2c+3$$

が得られる. その判別式 $d(g)$ は §2.1 の結果から直ちに得られて

$$d(g)=\{8dc^5+(-52d+8)c^4+(16d^2-16d-52)c^3+(216d^2+448d-8)c^2$$
$$+(8d^3+496d^2+628d+386)c+12d^3+312d^2+204d+381\}^2$$
$$=(2c+3)^2\cdot\Delta(c,d)^2$$

ここで,

$$\Delta(c,d)=-4d^3+(-8c^2-96c-104)d^2+(-4c^4+32c^3-40c^2-164c-68)d$$
$$-4c^3+32c^2-44c-127$$

となる. このとき, 次の定理が示される:

定理 6 c,d を $\mathbf{Q}$ 上独立な不定元とする. このとき,

(1) $g(x;c,d)=0$ の $\mathbf{Q}(c,d)$ 上の *Galois* 群は位数 *10* の正 *2* 面体群 D_{10} である.

(2) $g(x;c,d)=0$ の $\mathbf{Q}(c,d)$ 上の分解体 K に含まれる *2* 次体は $\mathbf{Q}(c,d,\sqrt{\Delta(c,d)})$ である.

(証明) ここでは証明の指針だけ示す. 実際の証明は §4.1 参照.

(1) 15 次分解式 $F_{15}(y;f)$ の 10 次部分 $F_2(y;b,c,d)$ が, $b=-1$ のとき, すなわち $F_2(y;-1,c,d)$ が 2 つの 5 次式の積に分解することを示せばよい.

(2) $K_0=\mathbf{Q}(c,d,\sqrt{\Delta(c,d)})$ とする. このとき, K_0 が 分解体 K に含まれることがわかれば (1) より位数 2 の部分体は一意に K_0 であることがわかる. よって, K_0 が K に含まれることを示せばよい. そのため $y^2-\Delta(c,d)$ が $g(x;c,d)=0$ の $\mathbf{Q}(c,d)$ 上の分解体 K において 2 つの 1 次因子の積に分解されることを示せばよい.

この定理から次の定理を得る (証明は [11] 参照.):

定理 7 $\Delta(c,d)\in\mathbf{Z}$ *($c,d\in\mathbf{Q}$, c,d は有理整数である必要ではない)* とする. $\Delta(c,d)$ がある *2* 次体の判別式と一致するとき *(多くの c,d に対してこの条件は満たされる)*, $g(x;c,d)=0$ の $\mathbf{Q}(c,d)$ 上の分解体は *2* 次体 $\mathbf{Q}(\sqrt{\Delta(c,d)})$ 上不分岐であり, *2* 次体 $\mathbf{Q}(\sqrt{\Delta(c,d)})$ の類数は *5* で割れる.

5 次式の族 $g(x;c,d)(c,d\in\mathbf{Q})$ から, Galois 群が位数 10 の正 2 面体群の Galois 拡大 (とくに二次体上の不分岐 5 次拡大が) がどのくらい得られるかということは, 整数論的に非常に興味深い問題である. 2 次体 $\mathbf{Q}\sqrt{m}$ の不分岐 5 次拡大は $|m|<1000$ の範囲で

実 2 次体のときは $m=401,439,499,727,817,982$ の 6 個

虚 2 次体のときは $-m=47,79,\cdots,982$ の 114 個

に対して存在する. このうち実 2 次体については全て, 虚 2 次体については数個の例外 (e.g. $-m = 613,769,977$ など) を除いて, 適当な $c, d \in \mathbf{Q}$ に対する $g(x; c, d)$ から得られる. いずれにしても, $g(x; c, d)$ は $\mathbf{Q}$ 上の D_{10}-拡大をかなり広い範囲でカバーしているように思われる.

9.4.1 定理6の証明

定理 6 の証明は以下に見られるように数式処理の応用で証明される:

(1) 実際に $F_2(y; -1, c, d)$ は直ちに求まりこれを因数分解すると:

$$F_2(y; -1, c, d) = H_1(y; c, d) \cdot H_2(y; c, d)$$

である. ここで,

$$\begin{aligned} H_1 = {} & y^5 + (-2c^2 - 2d + 6)y^4 + (c^4 + 4c^3 + (2d - 13)c^2 + (-12d - 16)c + d^2 - 21d + 9)y^3 + (-4c^5 + 6c^4 + (8d + \\ & 30)c^3 + (20d - 18)c^2 + (12d^2 - 34d - 54)c + 14d^2 - 58d - 7)y^2 + (5c^6 - 16c^5 + (-21d - 26)c^4 + (24d + \\ & 66)c^3 + (39d^2 + 152d + 83)c^2 + (104d^2 + 82d)c + d^3 + 66d^2 - 33d - 7)y - 2c^7 + 8c^6 + (2d + 8)c^5 + (-24d - \\ & 47)c^4 + (10d^2 + 16d - 32)c^3 + (104d^2 + 202d + 111)c^2 + (6d^3 + 200d^2 + 224d + 164)c + 8d^3 + 105d^2 + 63d + 67 \end{aligned}$$

$$\begin{aligned} H_2 = {} & y^5 + (-4c - 10)y^4 + (5c^2 + 36c + d + 47)y^3 + (-2c^3 - 38c^2 + (-2d - 138)c - 6d - 127)y^2 + (12c^3 + \\ & 105c^2 + (4d + 262)c + 9d + 193)y - 18c^3 - 108c^2 + (-2d - 210)c - 4d - 131 \end{aligned}$$

である. 確かに次数 5 の 2 つの因子が得られる. この因数分解の計算は Risa/Asir により 42 msec で得られる.

(2) まず, $f(x, -1, c, d)$ の $\mathbf{Q}(c, d)$ 上の分解体 K を求める. (1) より $K/\mathbf{Q}(c, d)$ の Galois 群が D_{10} なので分解体 K は $\mathbf{Q}(c, d)$ に 2 根添加すれば得られる. その 2 根を順に x_1, x_2 とする (x_1 の最小多項式は $g(x_1; c, d)$). K の $\mathbf{Q}(c, d)$ の原始元として $x_2 - x_1$ をとるとその最小多項式 H は

$$\begin{aligned} H = {} & x^{10} + (-4c^2 + 12c + 4d + 18)x^8 + (6c^4 - 36c^3 + (-4d - 2)c^2 + (60d + 180)c + 6d^2 + 74d + 149)x^6 + \\ & (-4c^6 + 36c^5 + (-4d - 50)c^4 + (-72d - 264)c^3 + (4d^2 + 172d + 278)c^2 + (84d^2 + 696d + 1056)c + \\ & 4d^3 + 94d^2 + 478d + 612)x^4 + (c^8 - 12c^7 + (4d + 34)c^6 + (12d + 84)c^5 + (6d^2 - 182d - 363)c^4 + (60d^2 - \\ & 120d - 480)c^3 + (4d^3 + 398d^2 + 1394d + 1228)c^2 + (36d^3 + 756d^2 + 2592d + 2448)c + d^4 + 38d^3 + \\ & 429d^2 + 1292d + 1156)x^2 + 16dc^6 + (-80d + 16)c^5 + (32d^2 - 188d - 80)c^4 + (480d^2 + 848d - 172)c^3 + \\ & (16d^3 + 1640d^2 + 2600d + 748)c^2 + (48d^3 + 2112d^2 + 2292d + 1920)c + 36d^3 + 936d^2 + 612d + 1143 \end{aligned}$$

となる. すなわち,

$$K = \mathbf{Q}(c, d)[x]/Id(H(x))$$

である. ここで, 多項式の集合 A について $Id(A)$ は A によって生成されるイデアルを表す.

2 次拡大 $K_0/\mathbf{Q}(c,d)$ についてであるが, この場合 K_0 が K に含まれることがわかれば位数 2 の部分体は一意に決まる. よって, K_0 が K に含まれることを示せばよい. そのために

$$L(y;c,d) = y^2 - \Delta(c,d)$$

が K 上で一次因子に分解されることを示せば良い. これを示すのに square-free norm を用いた Trager の代数拡大体上の因数分解のアルゴリズム [19] を利用する. このアルゴリズムについては簡単に §5.1 で述べる.

まず, $L(y;c,d)$ の y に $y-x_2$ を代入する: すなわち $L(y-x_2;c,d)$. $L(y-x_2;c,d)$ のノルム $Norm(L(y-x_2;c,d))$ すなわち H と $L(y-x_2;c,d)$ の x_2 についての終結式を計算する. ここで $y-x_2$ を代入する意味は, $Norm(L(y-x_2;c,d))$ が無平方になることにある (§5.1 定理 8 (3) 参照). この終結式の計算は, 時間こそ 16.500 sec で得られるが, 得られた結果は A4 の用紙に隙間なくプリントして数ページにも及ぶほど大きい式になる. 得られた $Norm(L(y-x_2;c,d))$ は y について 20 次の多項式である. Trager の方法に従って $Norm(L(y-x_2;c,d))$ の K 上の因子から $L(y;c,d)$ の K 上の因子を構成できるが, この場合の証明では. Trager の代数拡大体上の因数分解のアルゴリズムの性質より, $Norm(L(y-x_2;c,d))$ が $\mathbf{Q}(c,d)$ 上の因子と $L(y;c,d)$ の K 上の因子は 1 対 1 に対応するので, $Norm(L(y-x_2;c,d))$ が $\mathbf{Q}(c,d)$ 上 2 つの因子に分解されることを見れば良い (定理 8 (2)(3) 参照). 実際に $Norm(L(y-x_2;c,d))$ を因数分解すると 10 次の因子 2 つに分解される. この因数分解は 27.730 sec で得られる.

9.5 代数的算法について

9.5.1 代数的拡大体上での因数分解

Trager により提案された代数的拡大体上の多項式の因数分解 [15] [19] について述べよう. 2 つの体 K, L に対して, $L = K(\alpha)$ であるとする. (α は K 上代数的であるものとする.) α の最小多項式を $m(x)$ とし次数 n であるとする. すなわち, $L = K(\alpha) \equiv K[t]/Id(m(t))$.

K 上の α の共役元は $m(x)$ の他の相違なる元: $\alpha_2, \alpha_3, \cdots, \alpha_n$ である. $g \in L$ が

$$g = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in K(\alpha)$$

と表されるとき ($g(\alpha)$ とかく), g の共役元 $g_2, \cdots, g_n$ は $g_i = a_0 + a_1\alpha_i + \cdots + a_{n-1}\alpha_i^{n-1}$ $(2 \le i \le n)$ で与えられる. $g \in L$ のノルム $Norm(g)$ は g の全ての共役元の積として定義される. すなわち,

$$Norm(g) = g \cdot g_2 \cdots g_n \quad \in K.$$

また, $Norm(g)$ は終結式を用いて

$$Norm(g) = res_t(g(t), m(t))$$

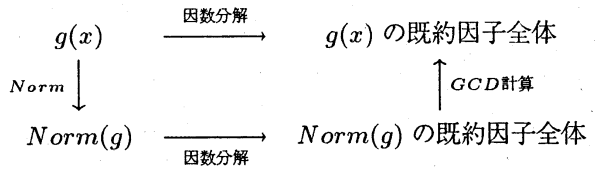
と定義される. $p \in K(\alpha)[x]$ に対してこの定義を拡張して

$$Norm(p) = res_t(p(t,x), m(t)) \quad \in K[x]$$

とする. (実際の計算はこの定義に従うことになる.) ノルムには

$$Norm(a \cdot b) = Norm(a) \cdot Norm(b)$$

という性質がある. よって, $K(\alpha)[x]$ 上で因子に分かれる多項式 $f(x)$ に対して, $Norm(f)$ は $K[x]$ 上で因数分解されるはずである. この手順を逆に用いようとするのが Trager のアイデアである. Trager の因数分解のスキームは, 以下の図式で表すことができる:



ここでの基礎となる定理を挙げておく.

定理 8 $f(x)$ を $L = K(\alpha)$ 上の一変数多項式とする. このとき

(1) f が L 上既約ならば $Norm(f)$ は K 上既約な多項式のベキになる.

(2) $Norm(f)$ が無平方, すなわち重複因子を持たない, とする. このとき, $Norm(f)$ の K 上の既約因子全体と f の L 上の既約因子全体の間に一対一対応が存在する. さらに詳しくいえば, $Norm(f)$ の K 上の既約因子 p に対して, $GCD(f,p)$ が対応する f の L 上の既約因子となる.

(3) f が無平方であるならば, ある整数 s が存在して, $Norm(f(x - s \cdot \alpha))$ は無平方にできる. このような s をとれば, f の L 上の既約因子と $Norm(f(x - s \cdot \alpha))$ の K 上の既約因子との間に次の一対一対応ができる. p を $Norm(f(x - s \cdot \alpha))$ の K 上の既約因子とすれば, $GCD(f(x), p(x + s \cdot \alpha))$ は f の L 上の既約因子となる.

(4) 上記の整数 s は, 以下のように拡大体の意味で特徴付けられる. f の任意の根 β に対して, $\beta - s \cdot \alpha$ は $K(\alpha, \beta)$ の K 上の原始元である. 無平方にならない s に対応する $K(\beta - s \cdot \alpha)$ は $K(\alpha, \beta)/K$ の中間体である.

$Norm$ の計算は, 終結式を用いた定義に従って計算できる. また, 体を係数環とする多項式の GCD は, 体上の四則演算が計算できるならば, 基本的には Euclid の互除法により実現できる. (効率化の工夫として, 部分終結式法, modular 技法による補間法等がある.) よって, L 上の多項式の因数分解は K 上の多項式の因数分解が存在すれば存在することになり, 逐次添加拡大の場合には, これを繰り返せばよい.

9.5.2 分解体の計算

分解体の計算は, 前節で述べた代数拡大体上の因数分解を繰り返し用いることで実現される. 基礎体が $\mathbf{Q}$ の場合には Trager の拡大体上の因数分解法に基づく分解体の計算は Risa/Asir にかなり tune up された形で実装され, そのパフォーマンスは実際にかなりの数の多項式について試され, Galois 群の位数が 200 程度の多項式については数時間程で計算可能である (詳細は [3] 参照).

$\mathbf{Q}$ 上の計算に比べ有理関数体 $\mathbf{Q}(b,c,d,\cdots)$ 上の計算は格段に困難になるのは容易に想像できる通りである. 数式処理でこれまでに有理関数体上の分解体の計算を実際に行なった例は筆者の知る限り見当たらないので, ここでは $g(x;c,d)$ の $\mathbf{Q}(c,d)$ 上の分解体の計算を行なった結果を以下に示す:

一般に, 変数 x_i $(1 \leq i \leq n)$ の順序を $x_1 \prec x_2 \prec \cdots \prec x_n$ とする. 任意の定数でない多項式 h に対して $h \in \mathbf{Q}[x_1,\cdots,x_\ell]$ なる最小の index ℓ をもつ変数 x_ℓ を h の主変数といい $lvar(h)$ と書く. 定数でない多項式の集合 $\{h_1,\cdots,h_r\}$ が $lvar(h_1) \prec lvar(h_2) \prec \cdots \prec lvar(h_r)$ を満たすとき, 三角形式 (triangular form) であるという. また, 任意の多項式 f,g に対して $sdiv(f,g)$ で f を g で割った時の商を表すとする. さて, 次の多項式 $G_1,\cdots,G_5$ を考える:

$$\begin{aligned}
G_1(x) &= g(x;c,d),\\
G_2(x;x_1) &= sdiv(g(x;c,d),(x-x_1))\\
G_3(x;x_1,x_2) &= sdiv(G_2(x),(x-x_2))\\
G_4(x;x_1,x_2,x_3) &= sdiv(G_3(x),(x-x_3))\\
G_5(x;x_1,x_2,x_3,x_4) &= sdiv(G_4(x),(x-x_4))
\end{aligned}$$

多項式集合 $\{G_1(x_1),G_2(x_2),\cdots,G_5(x_5)\}$ は明らかに三角形式である.

■原始元を用いた表現

§4.1 で示した分解体 K の $\mathbf{Q}(c,d)$ 上の原始元 x_2-x_1 を用いた分解体の表現は以下のようにして求まる. まず, $G_2(x_2+x_1;x_1)$ と $G_1(x_1)$ より x_1 を消去する:

$$R = res_{x_1}(G_2(x_2+x_1;x_1),G_1(x_1))$$

R は x_2 について 20 次の多項式で 13.120 sec で得られる. R を因数分解すると 2 つの 10 次既約因子に分解される: $R = R_1 \cdot R_2$ (1.000 sec).

$$\begin{aligned}
R_1 = {} & x_2^{10} + (-4c^2+12c+4d+18)x_2^8 + (6c^4-36c^3+(-4d-2)c^2+(60d+180)c+6d^2+74d+149)x_2^6 + \\
& (-4c^6+36c^5+(-4d-50)c^4+(-72d-264)c^3+(4d^2+172d+278)c^2+(84d^2+696d+1056)c+ \\
& 4d^3+94d^2+478d+612)x_2^4+(c^8-12c^7+(4d+34)c^6+(12d+84)c^5+(6d^2-182d-363)c^4+(60d^2- \\
& 120d-480)c^3+(4d^3+398d^2+1394d+1228)c^2+(36d^3+756d^2+2592d+2448)c+d^4+38d^3+ \\
& 429d^2+1292d+1156)x_2^2+16dc^6+(-80d+16)c^5+(32d^2-188d-80)c^4+(480d^2+848d-172)c^3+ \\
& (16d^3+1640d^2+2600d+748)c^2+(48d^3+2112d^2+2292d+1920)c+36d^3+936d^2+612d+1143
\end{aligned}$$

$$R_2 = x_2^{10} + (-2c^2 + 8c + 6d + 2)x_2^8 + (c^4 - 8c^3 + (-6d + 16)c^2 + (8d - 4)c + 9d^2 - 24d - 9)x_2^6 + ((4d - 2)c^4 + (-16d + 24)c^3 + (8d^2 + 12d - 68)c^2 + (48d^2 - 8d - 8)c + 4d^3 + 14d^2 + 8d + 117)x_2^4 + ((-8d + 1)c^4 + (48d - 20)c^3 + (48d^2 - 14d + 90)c^2 + (48d^2 - 68d - 28)c - 8d^3 + 17d^2 + 14d - 229)x_2^2 + 4dc^4 + (-32d + 4)c^3 + (8d^2 + 40d - 32)c^2 + (96d^2 + 164d + 44)c + 4d^3 + 104d^2 + 68d + 127$$

つまり, $H(x_2) = R_1$ とすれば, $K = \mathbf{Q}(c,d)[x_2]/Id(H(x_2))$ である.

■逐次拡大を用いた表現

さらに, 逐次拡大による分解体の表現を求めてみる. $Gal(K/\mathbf{Q}(c,d))$ の Galois 群が D_{10} なので分解体 K は $\mathbf{Q}(c,d)$ に 2 根添加すれば得られるが, 実際分解体 は

$$K = \mathbf{Q}(c,d)[x_1, x_2]/\mathcal{I}$$

で与えられる. ここで, $\mathcal{I} = Id(P_1, P_2)$ であり

$$P_1(x_1) = x_1^5 + 2cx_1^4 + (c^2 + 2c + d + 2)x_1^3 + (2c^2 + 2c - 2d + 1)x_1^2 + (c^2 + 4c + d + 2)x_1 + 2c + 3$$

$$P_2(x_2; x_1) = (-2c - 3)x_2^2 + ((x_1^2 + 3x_1)c^2 + (2x_1^3 + 4x_1^2 + 4x_1 + 2)c + (x_1^2 - x_1)d + x_1^4 + x_1^3 + 3x_1^2 + x_1 + 3)x_2 + (2x_1 - 2)c + 3x_1 - 3$$

である. 分解体 K は 2 根添加で得られるので, P_2 は, $g(x_2; c, d)$ の $\mathbf{Q}(c,d)(x_1)$ 上で因数分解すなわち, $G_2(x_2; x_1)$ の $\mathbf{Q}(c,d)(x_1)$ 上の因数分解より求まる. そこで, Trager の方法に従って計算する. まず $G_2(x_2; x_1)$ のノルムの計算であるが, 無平方になるように原始元 $x_2 - x_1$ を利用することにする (定理 8(4)):

$$Norm(G_2(x_2 + x_1; x_1)) = res_{x_1}(G_2(x_2 + x_1; x_1), G_1(x_1))$$

これは, 先ほどの R に他ならないことに注意. よって, 後は, R の因子 $\mathbf{Q}(c,d)(x_1)$ 上の 2 つの因子は $GCD(R_i(x_2), G_2(x_2; x_1))$ $(i = 1, 2)$ より求まる. ここで, この GCD 計算の部分は Gröbner 基底の計算を利用する. すなわち, 多項式集合 $\{G_1(x_1), G_2(x_2; x_1), R_i(x_2 - x_1)\}$ $(i = 1, 2)$ の $x_1 \prec x_2$ なる辞書式順序での Gröbner 基底 を計算すればその中に GCD に相当する元, すなわち $G_2(x_2; x_1)$ の $\mathbf{Q}(c,d)(x_1)$ 上の因子が得られる. ここでは, P_2 として $GCD(R_1(x_2), G_2(x_2; x_1))$ をとった. この Gröbner 基底による GCD 計算は 5509.851 sec で得られた.

残りの根 x_3, x_4, x_5 の最小多項式 P_3, P_4, P_5 についても, 同様に逐次拡大体上の因数分解を行なっていけば得られるが, より効率的に求めるため, ここでは $G_1(x)$ の Galois 群が D_{10} であることを利用する. まず, P_3 の場合について考える. D_{10} には $\sigma = (12345)$ なる元が存在する. (実際, $D_{10} = \langle (12345), (25)(34) \rangle$ である.) よって, x_3 は $G_3(x_3; x_1, x_2) = 0$ を満たしているが,

$$P_2(x_3; x_2) = 0$$

も満たす ([3] Theorem 5 参照). $G_3(x_3; x_1, x_2)$ は $P_2(x_3; x_2)$ の倍多項式ではなく, かつ $G_3(x_3; x_1, x_2)$

と $P_2(x_3;x_2)$ は $\mathbf{Q}(c,d)(x_1,x_2)$ 上の x_3 の最小多項式 (1 次式) の倍多項式なので多項式集合

$$\{P_1(x_1), P_2(x_2;x_1), G_3(x_3;x_1,x_2), P_2(x_3;x_2)\}$$

の $x_1 \prec x_2 \prec x_3$ なる辞書式順序での Gröbner 基底には, $\mathbf{Q}(c,d)(x_1,x_2)$ 上の $G_3(x_3;x_1,x_2)$ と $P_2(x_3;x_2)$ の GCD に対応する $x_3 - q(c,d)$ の型の多項式が得られる. ($q(c,d)$ は c,d の有理多項式.) 同様の方法で P_4, P_5 も計算できる. その結果は以下のようになる:

$$\begin{aligned}
P_3(x_3;x_1,x_2) = {} & (-2c-3)x_3 + ((x_2-1)x_1^2 + (2x_2-2)x_1 + x_2 - 1)c^2 + ((2x_2-2)x_1^3 + (2x_2-2)x_1^2 + \\
& (2x_2-2)x_1 + 4x_2 - 4)c + ((x_2-1)x_1^2 + (-2x_2+2)x_1 + x_2 - 1)d + (x_2-1)x_1^4 + \\
& (2x_2-2)x_1^2 + (x_2-1)x_1 + 2x_2 - 2 \\
P_4(x_4;x_1,x_2) = {} & (2c+3)x_4 + (x_2x_1^2 + (2x_2+1)x_1 + x_2 + 3)c^2 + (2x_2x_1^3 + (2x_2+2)x_1^2 + (2x_2+4)x_1 + 4x_2 + \\
& 4)c + (x_2x_1^2 + (-2x_2+1)x_1 + x_2 - 1)d + x_2x_1^4 + x_1^3 + (2x_2+1)x_1^2 + (x_2+3)x_1 + 2x_2 + 1 \\
P_5(x_5;x_1,x_2) = {} & (-2c-3)x_5 + (x_1^2 + 3x_1)c^2 + (2x_1^3 + 4x_1^2 + 4x_1 - 2x_2 + 2)c + (x_1^2 - x_1)d + x_1^4 + \\
& x_1^3 + 3x_1^2 + x_1 - 3x_2 + 3
\end{aligned}$$

これら P_3, P_4, P_5 の計算に要した時間はそれぞれ, 3361.520 sec, 118.706 sec, 7.969 sec である.

9.6 終りに

1960 年代に始まる数式処理 (Computer algebra) の研究の 30 年近い時間の積み重ねと計算機の飛躍的進歩とが合間って, かなりの数学上の操作を計算機で実現することが (実際の計算機で答えがでるという意味で) 可能となってきている. 本稿はその一例である.

数式処理の観点から言うと, 本稿では Galois 群の決定と部分体の計算の問題を扱っている. 定理 2 の証明において Galois 群の決定法の 1 つ, 分解式の既約因子の次数 (partition) の表により Galois 群を同定する方法が現れる. 定理 6 の証明においては, 部分体の判定のために分解体の計算が必要であった. 有理数体上の多項式の分解体の計算は実際にかなりのとこまで計算が可能になっているが, 有理関数体上の計算例はこれまでにほとんど見られない. その意味でもここでの $g(x;c,d)$ の分解体の計算は良い例を与える. また, 今回分解体の計算に Galois 群の知識を利用したがこれは一般に分解体の計算の効率化に有効である. この手法の一般化は現在検討中である.

参考文献

[1]相羽 律子 (1994). 「6 次方程式の研究」 東京女子大学大学院 理学研究科 数学専攻 修士論文.

[2]穴井 宏和, 横山和弘 (1995). 「ガロワ群計算の最新状況」 第 12 回代数的組合せ論シンポジウム 報告集 (近刊) 於 東大駒場 (1995.7.29-31)

[3]Anai, H. , Noro M. , Yokoyama K. (1995). Computation of the splitting fields and the Galois groups of polynomials. MEGA '94.

[4]Arnaudiés, J. M. , Valibouze, A. (1993). *Résolvantes de Lagrange.* Rapport interne LITP 93. 61.

[5]Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 8* Rapport interne LITP 94. 25.

[6]Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 9* Rapport interne LITP 94. 30.

[7]Arnaudiés, J. M. , Valibouze, A. (1994). *Calculs de résolvantes* Rapport interne LITP 94. 46.

[8]Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 4 à 6.* Rapport interne LITP 94. 48.

[9]Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 7* Rapport interne LITP 94. 49.

[10]Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 10 et 11* Rapport interne LITP 94. 50.

[11]近藤 武 (1995). 「ある 6 次式の族とそのガロワ群」 第 12 回代数的組合せ論シンポジウム 報告集 (近刊) 於 東大駒場 (1995.7.29-31)

[12]Olivier, M. (1990). Corps sextique primitifs. Ann.Institute Fourier 40, 757-767

[13]Brumer, A. (1989/1990). Exercises diedraux
et courbes a multiplications reeles.
Actes du theorie des nombres de Paris ,Birkhauser,Boston, a paraitre

[14]Ford, D. J. , McKay, J. (1989). Computation of Galois Groups from Polynomials over the Rationals. Computer algebra.

[15]Geddes, K.O., Czapor, S.R., Labahn, G.
(1992). Algorithms for Computer Algebra. Kluwer Academic Publishers.

[16]Soicher, L. (1984). An Algorithm for Computing Galois Groups. Computational Group Theory, Academic Press, London, 291-296.

[17]Soicher, L. , McKay, J. (1985). Computing Galois Groups over the Rationals. J. Number Theory 20, 273-281.

[18]Noro, M. and Takeshima, T. (1992). Risa/Asir – a computer algebra system, In: *Proceedings of International Symposium on Symbolic and Algebraic Computation 1992.* New York: ACM Press, 387-396.

[19]Trager, B. M. (1976). Algebraic factoring and rational function integration. in Proc. SYMSAC

'76, ACM Press, 219-226.

[20]Valibouze , A. (1995). Computation of the Galois Groups of the Resolvant Factors for the Direct and Inverse Galois Problem. AAECC 11 (July 17-21).

[21]B.L. van der Waerden. (1991). Algebra, Volume I, Springer-Verlag New York, Inc.

[22]Becker, T., Weispfenning, V. (1993). Gröbner Bases. GTM Springer-Verlag.