数理解析研究所講究録
第848巻 1993年 1-5

5次方程式の可解性の高速判定法

電子技術総合研究所　元吉 文男 (Fumio MOTOYOSHI)

有理数係数の5次の既約多項式が可解であるかどうかを、(大部分の場合に) 有理数演算だけで高速に判定する方法を紹介する。

1. ガロア群の計算原理

5次の推移群は以下の5種類である。

- S_5 対称群 (位数 120)
- A_5 交代群 (位数 60)
- B_5' メタ巡回群 (位数 20)
- B_5 半メタ巡回群 (位数 10)
- C_5 巡回群 (位数 5)

ここで可解なものは、B_5'、B_5、C_5 であり、$B_5' \supset B_5 \supset C_5$ という関係にある。そこで、方程式が可解かどうかはそのガロア群が B_5' に含まれているかどうかを調べればよい。

$f(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5$ を数体 P 上の既約多項式とし、x_1, x_2, x_3, x_4, x_5 を $f(x) = 0$ の根とする。

$$h = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1$$

としたときに多項式

$$g = h^2$$

は、B_5' の置換で不変であり、A_5 や S_5 の置換では不変ではない。B_5' の共役群は6つであるので、g に S_5 のすべての元を作用させたときに生成される多項式のうちで異なるものは6個であり、それを $g_0 = g, g_1, g_2, \ldots, g_5$ とする。このとき

$$G(z) = (z - g_0)(z - g_1)(z - g_2)(z - g_3)(z - g_4)(z - g_5)$$

という多項式が重根を持たず、かつ、P の中に根を持つならば元の多項式の P でのガロア群は B_5' の部分群である。

2. $G(z)$ の計算法

$G(z)$ は x_1, x_2, x_3, x_4, x_5 の対称式であるので、原理的には $G(z)$ の式を展開して、根と係数の関係から z の係数を a_1, a_2, a_3, a_4, a_5 で表すことができるが、計算量が膨大になるので以下に示す方法 [1] を利用する。

g から $g_0 = g, g_1, g_2, \ldots, g_5$ を生成する置換の代表として

$$s_0 = e,\ s_1 = (1\ 2\ 3),\ s_2 = (2\ 3\ 4),\ s_3 = (3\ 4\ 5),\ s_4 = (1\ 4\ 5),\ s_5 = (1\ 2\ 5)$$

とする。h に a を作用させたときの結果を h_a と書くことにすると

$$G(z) = (z - h^2)(z - h_{s_1}^2)(z - h_{s_2}^2)(z - h_{s_3}^2)(z - h_{s_4}^2)(z - h_{s_5}^2)$$

である。ここで

$$H(z) = (z - h)(z - h_{s_1})(z - h_{s_2})(z - h_{s_3})(z - h_{s_4})(z - h_{s_5})$$

とすると

$$G(z^2) = h(z)h(-z)$$

であるので $H(z)$ が求まれば $G(z)$ も求まる。

$$H(z) = z^6 + b_1 z^5 + b_2 z^4 + b_3 z^3 + b_4 z^2 + b_5 z + b_6$$

とする。

任意の置換 $a \in S_5$ について、h_a は a が偶置換の場合は h_{s_i} のどれかと、奇置換の場合は $-h_{s_i}$ のどれかと一致する。すると、$H(z)$ の偶数次の係数 b_2, b_4, b_6 は a で不変であり、根の対称式となり、b_1, b_3, b_5 はその符号を変えたものであり、差積

$$\Delta = \Delta(x_1, x_2, x_3, x_4, x_5)$$

で割り切れ、その商は根の対称式である。そこで $H(z)$ は次の形になる

$$H(z) = z^6 + b_2 z^4 + b_4 z^2 + b_6 + \Delta(c_1 z^5 + c_3 z^3 + c_5 z)$$

ここで、$b_2, b_4, b_6, c_1, c_3, c_5$ は x_1, x_2, x_3, x_4, x_5 の対称式である。ところが、多項式 h_{s_i} は x_i の 2 次同次式であるので b_i は x_i の $2i$ 次同次式である。一方で Δ は x_i の 10 次式であるので、

$$c_1 = 0, \quad c_3 = 0, \quad c_5 = c\ (\text{定数})$$

となる。そこで

$$H(z) = z^6 + b_2 z^4 + b_4 z^2 + b_6 + \Delta c z$$

であり、

$$G(z) = (z^3 + b_2 z^2 + b_4 z + b_6)^2 - D c^2 z$$

となる。ここで、$D = \Delta^2$ は $f(x)$ の判別式である。

文献 [1] では、 $a_1 = a_2 = a_3 = 0$ の場合に b_2, b_4, b_6, c の値を計算している。しかし、$f(x)$ を $x^5+a_4x+a_5$ という形の標準形にするには一般には体の拡大が必要であり、拡大体上での演算が必要になる。それよりも、(体を拡大せずに変形できる) a_1 だけが 0 の場合について係数を計算しておけば、可解性の判定が体 P だけの演算で実現できる。($G(z)$ が重根を持つ場合には、ここでの方法が適用できないので拡大体上での因数分解を使用した方法を用いることになるが、以下の実験では $f(x)$ が既約な場合にはこのような事態は生じなかった。)

b_2 を例にして実際の値を求めてみる。b_2 は x_i の 4 次同次式であり、また、a_i は x_i の i 次同次式であるので、c_{22}, c_4 を定数として

$$b_2 = c_{22}a_2^2 + c_4a_4$$

となる。この c_{22} と c_4 の値を求めればよいが、各 x_i に数値を入れて $H(z)$ を計算すれば、c_{22}, c_4 に関する一次式が得られるので、必要なだけの組について計算すれば連立方程式が解けるようになる。具体的には

$$x_1 = 0,\ x_2 = 0,\ x_3 = 0,\ x_4 = 1,\ x_5 = -1$$

とすると

$$H(z) = z^6 - 3z^4 + 3z^2 - 1$$

となり、

$$b_2 = -3 = c_{22}$$

である。また

$$x_1 = 0,\ x_2 = 1,\ x_3 = -1,\ x_4 = 1,\ x_5 = -1$$

では

$$H(z) = z^6 - 32z^4 + 256z^2$$

であり、

$$b_2 = -32 = 4c_{22} + c_4$$

となるので $c_4 = -20$ が求まり、結局

$$b_2 = -3a_2^2 - 20a_4$$

となる。同様にして他の係数を求めると

$$\begin{aligned}
b_2 &= -3a_2^2 - 20a_4 \\
b_4 &= 3a_2^4 + 16a_3^2a_2 - 8a_4a_2^2 + 240a_4^2 - 400a_5a_3 \\
b_6 &= -a_2^6 - 16a_3^2a_2^3 - 64a_3^4 + 28a_4a_2^4 + 224a_4a_3^2a_2 - 176a_4^2a_2^2 + 320a_4^3 - 80a_5a_3a_2^2 \\
&\quad -1600a_5a_4a_3 + 4000a_5^2a_2 \\
c &= 32
\end{aligned}$$

となる。また判別式も

$$D = 108a_2^5a_5^2 - 72a_2^4a_3a_4a_5 + 16a_2^4a_4^3 + 16a_2^3a_3^3a_5 - 4a_2^3a_3^2a_4^2 - 900a_2^3a_4a_5^2$$
$$+825a_2^2a_3^2a_5^2 + 560a_2^2a_3a_4^2a_5 - 128a_2^2a_4^4 - 630a_2a_3^3a_4a_5 + 144a_2a_3^2a_4^3$$
$$-3750a_2a_3a_5^3 + 2000a_2a_4^2a_5^2 + 108a_3^5a_5 - 27a_3^4a_4^2 + 2250a_3^2a_4a_5^2 - 1600a_3a_4^3a_5$$
$$+256a_4^5 + 3125a_5^4$$

と求まる。

まとめると、既約な5次方程式 $f(x)$ の可解性の判定には、まず、与えられた式の係数から $G(z)$ を計算して、それが重根を持つかどうかを $G'(z)$ との GCD を計算して調べる。重根を持つ場合には、任意の2根を添加した体が分解体になっているかどうかを調べる。重根を持たない場合には、$G(z)$ が P 中に根を持てば、$f(x) = 0$ は P で可解である。また、D が P で完全平方ならばガロア群は交代群の部分群であるので、可解の場合は B_5 か C_5 であり、非可解の場合は A_5 である。B_5 か C_5 かの判定には1根添加で一次因子に因数分解できるかどうかで行なう。

次頁に、付録として、$-12 \leq a_2, a_3, a_4 \leq 12,\ \ 1 \leq a_5 \leq 12$ の多項式についてのガロア群の判定結果を示す。

参 考 文 献

[1] エム・ポストニコフ、「ガロアの理論」、東京図書、1964。

A. 付録

a_2	非可解		可解				
			既約			可約	
	S_5	A_5	B_5'	B_5	C_5	$2+3$	一次
-12	7031	0	0	1	0	60	408
-11	6967	0	0	3	1	75	454
-10	6935	1	0	1	1	73	489
-9	6893	0	1	2	0	79	525
-8	6852	1	0	2	0	91	554
-7	6830	0	0	2	0	91	577
-6	6798	3	1	2	0	106	590
-5	6801	1	10	6	0	104	578
-4	6816	1	0	2	0	114	567
-3	6807	7	0	6	0	120	560
-2	6805	10	0	4	0	119	562
-1	6822	2	1	8	0	114	553
0	6827	2	14	5	0	108	544
1	6856	4	0	5	0	110	525
2	6886	9	1	4	0	100	500
3	6914	12	0	4	0	97	473
4	6960	0	1	4	0	92	443
5	6980	3	13	3	0	84	417
6	7019	9	1	3	0	74	394
7	7049	5	0	6	0	64	376
8	7084	2	1	2	0	51	360
9	7121	1	0	1	0	35	342
10	7139	5	2	2	0	30	322
11	7170	1	0	2	0	27	300
12	7187	2	0	0	0	23	288
計	173549	81	46	80	2	2041	11701

$x^5 + a_2x^3 + a_3x^2 + a_4x + a_5$
$-12 \le a_2, a_3, a_4 \le 12,\ 1 \le a_5 \le 12$
の全数 (187500 個の多項式) についてのガロア群の決定

注)
巡回群になるものは次の 2 つ
$x^5 - 11x^3 - 11x^2 + 11x + 11$
$x^5 - 10x^3 + 5x^2 + 10x + 1$

次のものは a によらず可解
$x^5 + a$
$x^5 \pm 5x^3 + 5x + a$