因数分解に基づく低次一変数代数方程式の代数的解法

Algebraic Solution Method of Low-Degree Algebraic Equations Based on Factorizations

東京都立大学・数理科学専攻・客員研究員　　村上 弘[*1]
Hiroshi Murakami (Retiree Affiliate)
Department of Mathematical Sciences, Tokyo Metropolitan University

Abstract

We attempted to derive a radical representations of solutions for a univariate algebraic equation of lower degree, relying solely on elementary arguments based on the factorization of the polynomial over the field extended by radicals, without resorting to Galois theory. In this case, factorization reduces to solving a system of multivariate algebraic equations, which presents difficulties such as requiring a significant amount of time for computation; however, this serves as a good example for evaluating performances of symbolic algebraic computation systems.

1　はじめに

次数の比較的小さい 2 次から 9 次までの一変数代数方程式について，その解の巾根による表示の構成を行うのに，ガロア理論を持ち出さずに方程式の多項式の冪根拡大体上での因数分解だけを用いて数式処理に沿う素朴な方法で求めることを試みた．冪根拡大体上での因数分解は多変数多項式の連立代数方程式を解く計算に帰着させるので，消去法などの計算を行うために数式処理システムの高度な計算能力が求められる．

2　2 次方程式の場合

K 係数の monic な 2 次多項式を $f = x^2 + 2\,p_1\,x + p_0$ とする．f が体 K 上可約の場合には，1 次因子 2 つに $f = (x+\alpha_1)\,(x+\alpha_2)$ と分解されて，$f = 0$ の 2 根は $x = -\alpha_1, -\alpha_2 \in K$ である．そうではなくて f が体 K 上既約の場合には，体 K から何回か巾根拡大した体を M とするとき．f は M 上で既約だが，M のある非平方元 R の平方根を添加した体 $M(\sqrt{R})$ 上では可約になるとし，$M(\sqrt{R})$ 上での f の 1 次因子の 1 つを $x+a+b\sqrt{R}$ とする（ただし $a,\, b,\, R \in M$，$\sqrt{R} \notin M$）．するともう 1 つの 1 次因子は $x+a-b\sqrt{R}$ になることがいえる．よって $f = \left(x+a+b\sqrt{R}\right)\left(x+a-b\sqrt{R}\right) = x^2+2\,ax+a^2-b^2R$．そこで $f = x^2+2\,p_1\,x+p_0$ と x の同次項の係数を等置すると，1 次の項から $p_1 = a$，定数項から $p_0 = a^2 - b^2R$ が得られる．この関係を解けば $a := p_1$，$b^2R := {p_1}^2 - p_0$ となる．すると f の 2 根は $x = -a \pm b\,\sqrt{R} = -p_1 \pm \sqrt{{p_1}^2 - p_0}$ である．f は K で既約と仮定したので，$D \equiv p_1^2 - p_0$ は K の非平方元である．（もしも D が体 K の平方元なら，f は K 上可約であり，2 根は K に含まれて，$D = 0$ の場合にだけ重複する．）

[*1] 〒 191-0397 東京都八王子市南大沢 1-1　E-mail: mrkmhrsh@tmu.ac.jp

3　3 次方程式の場合

係数体が K の monic な 3 次多項式を $f = x^3 + 3\,p_2\,x^2 + 3\,p_1\,x + p_0$ とする．f が K 上可約である場合には，f は K 上で 1 次因子を少なくとも 1 つ持ち，それに対応する根は K の元であり，他の 2 根はその 1 次因子を除いた K 係数の 2 次多項式の根である．そうではなくて f が K 上既約の場合には，K のある代数拡大体を M として，f は体 M 上では既約だが，体 $M(R^{1/3})$ 上では可約となるような体 M の非立方元 R の存在を仮定する．そのとき f は体 $M(R^{1/3})$ 上では式 (1) の形の 1 次の因子 $f_0^{(1)}$ を持つ．

$$f_0^{(1)} = x + a_0 + a_1 R^{1/3} + a_2 R^{2/3}\,. \tag{1}$$

ただし a_0，a_1，a_2，R はどれも体 M の元で，R は M の非立方元であり，少なくとも a_1 と a_2 の一方が零ではないとする．さらに M が 1 の原始 3 乗根 ω_3 を含む場合には $M(R^{1/3})$ のままの体を，そうではなくて M が ω_3 を含まない場合には体 $M(R^{1/3})$ に ω_3 を添加した体を考えると，もしも f が体 $M(R^{1/3})$ において式 (1) の形の 1 次因子 $f_0^{(1)}$ を持つならば，体 $M(R^{1/3},\omega_3)$ では式 (2) 中の 2 つの 1 次式もまた f の 1 次因子となることが示せる．

$$f_1^{(1)} = x + a_0 + a_1\,\omega_3\,R^{1/3} + a_2\,\omega_3^2\,R^{2/3},\quad f_2^{(1)} = x + a_0 + a_1\,\omega_3^2\,R^{1/3} + a_2\,\omega_3\,R^{2/3}\,. \tag{2}$$

f が M で既約であることから 3 つの因子は相異なり，また R は非零である．すると積 $f_0^{(1)} f_1^{(1)} f_2^{(1)}$ は M 係数の f を割る monic な 3 次式になり，f と一致する．

$$f = f_0^{(1)} f_1^{(1)} f_2^{(1)} = x^3 + 3a_0x^2 + 3(a_0^2 - a_1a_2R)x + a_0^3 + a_1^3R + a_2^3R^2 - 3a_0a_1a_2R. \tag{3}$$

すると f について x の同次項の係数等置により，2 次項から $p_2 = a_0$ が，1 次項から $p_1 = a_0^2 - a_1a_2R$ が，定数項から $p_0 = a_0^3 + (a_1^2 - 3\,a_0\,a_2)\,a_1R + a_2^3\,R^2$ という 4 変数 a_0，a_1，a_2，R の 3 連立方程式が得られるが，一般性を失わずに $a_1 = 1$ にとれる（なぜならば，もしも $a_1 = 0$ ならば $f_0^{(1)} = x + a_0 + a_2R^{2/3} = x + a_0 + (a_2^3\,R^2)^{1/3}$ だから，$R' = a_2^3R^2$ とおくと，$f_0^{(1)} = x + a_0 + R'^{1/3}$ となり，R' を R と書き換えれば，結局 $a_1 = 1$ の場合に帰着できる）．すると連立方程式は 3 変数 a_0，a_2，R の 3 連立式 (4) になり，それから式 (5) を得る．

$$p_2 = a_0,\quad p_1 = a_0^2 - a_2\,R,\quad p_0 = a_0^3 + (1 - 3\,a_0\,a_2)\,R + a_2^3\,R^2\,. \tag{4}$$

$$a_0 := p_2,\quad R^2 - (2\,{p_2}^3 - 3\,p_1\,p_2 + p_0)\,R + (p_2^2 - p_1)^3 = 0,\quad a_2 := ({p_2}^2 - p_1)/R\,. \tag{5}$$

式 (5) の中の R の 2 次方程式が K 上で可約な場合には R と a_2 は体 K に属するが，R の 2 次方程式が K 上既約な場合には R と a_2 は体 K の 2 次拡大体 M に属する．そうして R の 2 次方程式の（どちらか 1 方の）解 R を用いて f の 3 根は式 (6) で表される．

$$x_j := -\,p_2 - \omega_3^j\,R^{1/3} - (p_2^2 - p_1)/(\omega_3^j\,R^{1/3})\quad,\ j = 0,1,2\,. \tag{6}$$

付記：3 次式に 2 次項が無くて $f = x^3 + 3\,p_1x + p_0$ の場合は，係数の等置から式 (7) が得られる．

$$a_0 = 0,\quad R^2 - p_0\,R - p_1^3 = 0,\quad a_2 = -p_1/R\,. \tag{7}$$

R の 2 次方程式の 2 根を入れ替えると，因子の $f_0^{(1)}$ は不変で，$f_1^{(1)}$ と $f_2^{(1)}$ は入れ替わるが，3 根全体は同じになる．

f が K 上既約であって R の 2 次方程式が K 上可約な場合には，体 K に R と a_2 は属して，$f = 0$ の 3 根は $K(R^{1/3},\omega_3)$ に属する．

f が K 上既約であって R の 2 次方程式が K 上既約な場合には，K のある数の平方根を 1 つ K に添加した体 M に R と a_2 は続して，$f = 0$ の 3 根は $M(R^{1/3},\omega_3)$ に属する．

補注：体 M で既約な 3 次多項式 f は，R を M のある非平方元とすると，体 $M(\sqrt{R})$ では可約にはならない．なぜなら，もしも f が $M(\sqrt{R})$ で 1 次因子 $f_0^{(1)}$ を持てば，その中の $\sqrt{R}$ を $-\sqrt{R}$ に置換した $f_1^{(1)}$ は $f_0^{(1)}$ とは異なる f の因子になり，それらの積 $f_0^{(1)} f_1^{(1)}$ は f を割り切る体 M 上の 2 次式なので，f が体 M 上で既約とした仮定に反する．

あるいはもしも f が $M(\sqrt{R})$ で既約な 2 次の因子 $f_0^{(2)}$ を持てば，その中の $\sqrt{R}$ を $-\sqrt{R}$ に置換した $f_1^{(2)}$ は $f_0^{(2)}$ とは異なる $M(\sqrt{R})$ 上での f の 2 次の既約因子になるが，因子の積 $f_0^{(2)} f_1^{(2)}$ は 4 次で f を割り切るので，f が 3 次であることに矛盾する．

同様にして体 M で既約な 3 次式 f は体 $M(R^{1/3})$ 上では既約な 2 次の因子を持たないことも示せる．

一般に係数が K に属する monic な n 次方程式の多項式 f の場合には，f は K のある拡大体 M では既約だが，p を次数 n を割り切る素数とするとき，M に於けるある非 p 乗数を R として，体 $M(R^{1/p})$ 上では次数 $m = n/p$ の monic な既約因子 $f_0^{(m)}$ を持つ場合を考えればよいことが示せる．

f が体 $M(R^{1/p})$ 上で m 次の既約因子 $f_0^{(m)}$ を持つときは，1 の原始 p 乗根を ω とすると，体 $M(R^{1/p}, \omega)$ では，既約因子 $f_0^{(m)}$ に含まれる $R^{1/p}$ を $\omega^j R^{1/p}$ に置き換えた多項式 $f_j^{(m)}$, $j = 1, 2, \ldots, p-1$ もまた f の相異なる m 次の既約因子になる．そうして $f = \prod_{j=0}^{p-1} f_j^{(m)}$ である．

4　4 次方程式の場合

係数が体 K に属する monic で既約な 4 次多項式 f を式 (8) とする．

$$f = x^4 + 2\,p_3\,x^3 + p_2\,x^2 + 2\,p_1\,x + p_0\,. \tag{8}$$

f は K のある拡大体 M では既約だが，M のある非平方元 R の平方根を M に添加した体 $M(R^{1/2})$ 上では互いに共役な 2 つの 2 次因子の積に分解されるとする．つまり a_0，a_1，b_0，b_1，R がそれぞれ M に属するとし，R は M の非平方元として式 (9) が成り立つとする．

$$\begin{aligned} f &= \left\{x^2 + (a_0 + a_1\sqrt{R})\,x + b_0 + b_1\sqrt{R}\right\}\left\{x^2 + (a_0 - a_1\sqrt{R})\,x + b_0 - b_1\sqrt{R}\right\} \\ &= (x^2 + a_0\,x + b_0)^2 - (a_1\,x + b_1)^2\,R \\ &= x^4 + 2\,a_0\,x^3 + (a_0^2 + 2\,b_0)\,x^2 + 2\,a_0 b_0\,x + b_0^2 - (a_1^2\,x^2 + 2\,a_1\,b_1\,x + b_1^2)\,R. \end{aligned} \tag{9}$$

すると x の同次項の係数等置から 5 変数 a_0，a_1，b_0，b_1，R についての 4 連立の方程式 (10) が得られる．

$$p_3 = a_0,\ p_2 = a_0^2 + 2\,b_0 - a_1^2\,R,\ p_1 = a_0\,b_0 - a_1\,b_1\,R,\ p_0 = b_0^2 - b_1^2\,R. \tag{10}$$

4 次多項式 (8) の 3 次の項が欠けていれば $p_3 = 0$ により $a_0 = 0$ なので，式 (9) はより簡単となり，その f の x についての同次項の係数等置から，2 次項より $p_2 = 2\,b_0 - a_1^2\,R$，1 次項より $p_1 = -\,a_1\,b_1\,R$，定数項より $p_0 = b_0^2 - b_1^2\,R$ という 3 連立の方程式が得られる．

$p_1 = 0$ である場合には，元の 4 次方程式は複 2 次方程式 $x^4 + p_2 x^2 + p_0 = 0$ なので，$t = x^2$ についての既約な 2 次方程式 $t^2 + p_2 t + p_0 = 0$ の 2 根を平方根を用いて表し，それらの平方根をとして 4 根 x は容易に求まる（それらの根は K から平方根拡大を 2 回行った体に属している）．

$p_1 \neq 0$ の場合には $a_1\,b_1 \neq 0$ であり，式 (11) に示した 3 通りの R の表現が得られる．それから容易に b_0 についての K 係数の 3 次方程式 (12) が得られる．

$$R = (2\,b_0 - p_2)/a_1^2,\ \ R = -\,p_1/(a_1 b_1),\ \ R = (b_0^2 - p_0)/b_1^2\,. \tag{11}$$

$$(b_0^2 - p_0)(2\,b_0 - p_2) = {p_1}^2\,. \tag{12}$$

もしもこの 3 次方程式 (12) が K 上で可約ならば，b_0 は K の元にとれる．

式 (12) の 3 つの解 b_0 のどれかを含む K の最小の拡大体を M とする．また一般性を失わずに $a_1 = 1$ にとれて，R と b_1 は式 (13) になる．R と b_1 は体 M の元で R は M の非平方元である．

$$R := 2\,b_0 - p_2,\ \ b_1 := -\,p_1/R. \tag{13}$$

そのとき f の 2 つの 2 次因子は式 (14) であり，2 次因子の方程式をそれぞれ解けば 4 次方程式の 4 根が得られる．

$$\left\{\begin{array}{lcl} f_0^{(2)} & := & x^2 + \sqrt{2\,b_0 - p_2}\,x + b_0 - p_1/\sqrt{2\,b_0 - p_2}\,, \\ f_1^{(2)} & := & x^2 - \sqrt{2\,b_0 - p_2}\,x + b_0 + p_1/\sqrt{2\,b_0 - p_2}\,. \end{array}\right. \tag{14}$$

5　5 次方程式の場合

係数が体 K に属する monic な方程式の既約 5 次多項式 f を式 (15) とする．

$$f = x^5 + 5\,p_4\,x^4 + 5\,p_3\,x^3 + 5\,p_2\,x^2 + 5\,p_1\,x + p_0. \tag{15}$$

K から巾根拡大を何回か行った体を M として，f は M では既約だが，体 M のある非 5 乗元を R として，f が体 $M(R^{1/5})$ 上では可約と仮定すると，f は $M(R^{1/5})$ では式 (16) で表される 1 次因子 $f_0^{(1)}$ を持つ．ただし $a_j \in M$，$j = 0, 1, 2, 3, 4$，$R \in M$，$R^{1/5} \notin M$ である．

$$f_0^{(1)} = x + a_0 + a_1\,R^{1/5} + a_2\,R^{2/5} + a_3\,R^{3/5} + a_4\,R^{4/5}\,. \tag{16}$$

そのとき，さらに 1 の原始 5 乗根 ω_5 を添加した体 $M(R^{1/5}, \omega_5)$ の上では，f は式 (17) で表される相異なる 1 次因子 5 つ $f_j^{(1)}$，$j = 0, 1, 2, 3, 4$ を持つことが言える．

$$f_j^{(1)} = x + a_0 + a_1\,\omega_5^j R^{1/5} + a_2\,\omega_5^{2j} R^{2/5} + a_3\,\omega_5^{3j} R^{3/5} + a_4\,\omega_5^{4j} R^{4/5}\,. \tag{17}$$

それら 5 つの 1 次因子の積 $f_0^{(1)} f_1^{(1)} f_2^{(1)} f_3^{(1)} f_4^{(1)}$ は M 係数で monic で 5 次で f を割ることから f に等しい．f が最初から 4 次項の欠けた形 $p_4 = 0$ にとってあれば $a_0 = 0$ である．また一般性を失わずに $a_1 = 1$ としてよい．そのとき x の同次項の係数等置から式 (18) を得る．この 4 元 4 連立方程式を解いて 4 つの変数 a_4，a_3，a_2，R が求まれば，元の 5 次方程式の 5 つの解は式 (19) で表せることになる．

$$\left\{\begin{array}{lcl} p_3 & = & -\,(a_4 + a_2\,a_3)\,R,\ \ p_2 = (a_2\,a_4^2 + a_3^2\,a_4)\,R^2 + (a_3 + a_2^2)\,R, \\ p_1 & = & -\,a_3\,a_4^3\,R^3 + (a_4^2 - a_2\,a_3\,a_4 - a_2^3\,a_4 - a_3^3 + a_2^2\,a_3^2)\,R^2 - a_2\,R, \\ p_0 & = & a_4^5\,R^4 + (-5\,a_2\,a_4^3 + 5a_3^2\,a_4^2 + 5\,a_2^2\,a_3\,a_4^2 - 5\,a_2\,a_3^3\,a_4 + a_3^5)\,R^3 \\ & & \quad + (-5\,a_3\,a_4 + 5a_2^2\,a_4 + 5\,a_2\,a_3^2 - 5a_2^3\,a_3 + a_2^5)\,R^2 + R\,. \end{array}\right. \tag{18}$$

$$x_j = -\omega_5^j R^{1/5} - a_2\,\omega_5^{2j} R^{2/5} - a_3\,\omega_5^{3j} R^{3/5} - a_4\,\omega_5^{4j} R^{4/5}\,,\ j = 0, 1, 2, 3, 4\,. \tag{19}$$

4 元 4 連立方程式 (18) から a_4，a_3，a_2 を消去すると，R 単独についての K 係数の 24 次方程式が得られる（この消去を手計算で行うのは困難である）．この R の 24 次方程式は一般には K 上既約である．しかし R の方程式が K 上可約で，もしも低次の 1 次，2 次，4 次などの因子を持てば，直ちに R を巾根を用いて表すことができる．R が巾根表示を持つ場合には他の変数 a_2, a_3, $a_4 \in M$ についても同様になり，5 次方程式 $f = 0$ の解が巾根表示を持つことになる．

ガロア理論からは K 係数の既約な 5 次方程式は K 上のガロア群が位数 120 の 5 次対称群 S_5 や位数 60 の交代群 A_5 の場合には，K から始めて巾根を何度か用いて表せる解を持たないが，位数がそれぞれ 20，10，5 である群 F_{20}，F_{10}，F_5 の場合には巾根で表される解を持つことが知られている．

Q 上のガロア群が S_5 の場合の例 (maxima) 5 次方程式として $f = x^5 - 5\,x^3 + 1 = 0$ をとった．4 変数 a_4，a_3，a_2，R の 4 連立方程式のグレブナ基底の数は 148 であった．計算時間の例は CPU が 1.94 時間，Elapsed が 2.24 時間であった．計算は maxima-5.48.1 (GCL) の "poly_grobner"を用いて，計算機システムは VMware Workstation による仮想環境で CPU は intel Core i5-6400，2.7GHz，メモリ 16GB のものである．グレブナ基底の maxima による構成には長時間を要した．グレブナ基底により求めた R 単独の方程式の係数は長大な整数で，次数は 24 であり，Q 上で既約であった．また $Q(\omega_5)$ 上でも既約であった．f の判別式の値は -334375 で負であった．

Q 上のガロア群が A_5 の場合の例 (maxima) 5 次方程式として $f = x^5 + 5\,x^3 + 1 = 0$ をとった．4 変数 a_4，a_3，a_2，R の 4 連立方程式のグレブナ基底の数は 148 であった．計算時間の例は CPU が 1.86 時間，Elapsed が 2.19 時間であった．R 単独の方程式の係数は長大な整数で，次数は 24 であり，Q 上で既約であった．また $Q(\omega_5)$ 上でも既約であった．f の判別式の値は 340625 で正であった．

Q 上のガロア群が F_{20} の場合の例 (maxima) 5 次方程式として $f = x^5 + 15\,x + 12 = 0$ をとった．4 変数 a_4，a_3，a_2，R の 4 連立方程式のグレブナ基底の数は 142 であった．計算時間の例は CPU が 2.66 時間，Elapsed が 3.21 時間であった．R 単独の方程式は係数は長大な整数で，次数は 24 であり，Q 上での既約因子は 2 次のものが 2 つと 10 次のものが 2 つであった．それらの既約因子は $Q(\omega_5)$ でも既約であった．2 次の既約因子は $3125R^2 - 3750R + 243$ と $3125R^2 + 11250R - 243$ であり，それぞれの根は $R = \frac{75 \pm 21\sqrt{10}}{125}$ および $R = \frac{-225 \pm 72\sqrt{10}}{125}$ である．

Q 上のガロア群が F_{10} の場合の例 (maxima) 5 次方程式として $f = x^5 - 5\,x + 12 = 0$ をとった．4 変数 a_4，a_3，a_2，R の 4 連立方程式のグレブナ基底の数は 142 であった．計算時間の例は CPU が 2.48 時間，Elapsed が 2.97 時間であった．R 単独の方程式の係数は長大な整数で，次数は 24 であり，Q 上での既約因子は 4 次のものが 1 つと 20 次のものが 1 つであった．4 次の既約因子は $3125R^4 - 12500R^3 + 2500R^2 + 200R - 1$ であり，その 4 根は式 (20) になる：

$$R = 1 - \frac{2}{\sqrt{5}} \pm \frac{1}{2}\sqrt{\frac{36}{5} - \frac{396}{25\sqrt{5}}}\,,\ 1 + \frac{2}{\sqrt{5}} \pm \frac{1}{2}\sqrt{\frac{36}{5} + \frac{396}{25\sqrt{5}}}\,. \tag{20}$$

なお，Q 上 4 次の既約因子は $Q(\omega_5)$ 上では 2 次の既約因子 2 つに分解した（式 (21)）．また Q 上 20 次の既約因子は $Q(\omega_5)$ 上では 10 次の既約因子 2 つに分解した．

$$\begin{cases} 125\,R^2 - (200\,w^3 + 200\,w^2 + 350)\,R + (2\,w^3 + 2\,w^2 + 1), \\ 125\,R^2 + (200\,w^3 + 200\,w^2 - 150)\,R - (2\,w^3 + 2\,w^2 + 1)\,. \end{cases} \tag{21}$$

Q 上のガロア群が F_5 の場合の例 (maxima) 5 次方程式として $f = x^5 - 10\,x^3 + 5\,x^2 + 10\,x + 1 = 0$ をとった．4 変数 a_4，a_3，a_2，R の 4 連立方程式のグレブナ基底の数は 159 であった．計算時間の例は CPU が 11.15 時間，Elapsed が 13.16 時間であった．R 単独の方程式の係数は長大な整数で，次数は 24 であり，Q 上での既約因子は 4 次のものが 1 つと 20 次のものが 1 つであった．4 次の既約因子は $R^4 - R^3 + R^2 - R + 1$ であり，その 4 つの根は式 (22) である．

$$R = \frac{1 - \sqrt{5}}{4} \pm \frac{1}{2}\sqrt{\frac{-5 - \sqrt{5}}{2}}\,,\quad \frac{1 + \sqrt{5}}{4} \pm \frac{1}{2}\sqrt{\frac{-5 + \sqrt{5}}{2}}\,. \tag{22}$$

なお Q 上の 4 次の既約因子は $Q(\omega_5)$ 上では 1 次の因子 4 つに分解された（式 (23)）．また Q 上の 20 次の既約因子は $Q(\omega_5)$ 上では 5 次の既約因子 4 つに分解された．

$$(R + \omega_5)\,(R + \omega_5^2)\,(R + \omega_5^3)\,(R + \omega_5^4)\,. \tag{23}$$

5.1 「消去法」による 4 元 4 連立方程式の計算例 (maxima)

方程式系 (18) を maxima の関数"`eliminate`"を用いて，変数を 1 つずつ a_4, a_2, a_3 の順に消去して R 単独の方程式を作る．そのとき $R = 0$ は不要解なので，変数を 1 つ消去するたびに，得られた連立多項式から R の巾の因子を除去した．4 次の項の欠けた 5 次方程式の係数 p_0，p_1，p_2，p_3 をパラメタのままで扱うことは，消去法を用いても数式が膨大になり不可能であったので，係数に値を先に与えて計算を行った．

ガロア群が S_5 の例：例にした 5 次方程式は $f = x^5 - 5\,x^3 + 1 = 0$ で，消去計算に掛かった時間は `CPU` が 11.01 秒，`Elapsed` が 11.55 秒であった．消去法で得られた R 単独の方程式は 240 次であり，その Q 上の既約因子は 24 次のものが 1 つと 216 次のものが 1 つであった．

ガロア群が A_5 の例：例にした 5 次方程式は $f = x^5 + 5\,x^3 + 1 = 0$ で，消去計算に掛かった時間は `CPU` が 11.66 秒，`Elapsed` が 12.08 秒であった．消去法で得られた R 単独の方程式は 240 次であり，その Q 上の既約因子は 24 次のものが 1 つと 216 次のものが 1 つであった．

ガロア群が F_{20} の例：例にした 5 次方程式は $f = x^5 + 15\,x + 12 = 0$ で，消去計算に掛かった時間は `CPU` が 9.50 秒，`Elapsed` が 9.83 秒であった．消去法で得られた R 単独の方程式は 180 次で，その Q 上の既約因子は 2 次のものが 2 つと 10 次のものが 2 つと 156 次のものが 1 つであった．2 次の既約因子 2 つは $3125R^2 - 3750R + 243$ と $3125R^2 + 11250R - 243$ であった．

ガロア群が F_{10} の例：例にした 5 次方程式は $f = x^5 - 5\,x + 12 = 0$ で．消去計算に掛かった時間は `CPU` が 6.92 秒，`Elapsed` が 7.93 秒であった．消去法で得られた R 単独の方程式は 180 次で，その Q 上の既約因子は 4 次のものが 1 つと 20 次のものが 1 つと 156 次のものが 1 つであった．4 次の既約因子は $3125R^4 - 12500R^3 + 2500R^2 + 200R - 1$ であった．

ガロア群が F_5 の例：例にした 5 次方程式は $f = x^5 - 10\,x^3 + 5\,x^2 + 10\,x + 1 = 0$ で，消去計算の時間は `CPU` が 11.62 秒，`Elapsed` が 12.03 秒であった．消去法で得られた R 単独の方程式は 240 次で，Q 上の既約因子は 4 次のものが 1 つと 20 次のものが 1 つと 216 次のものが 1 つであった．4 次の既約因子は $R^4 - R^3 + R^2 - R + 1$ であった．

パラメタを 1 つだけ含む方程式の例：例にした 5 次方程式は $f = x^5 + 5\,p_1\,x + 1$ であり，係数 p_1 はパラメタとする．消去計算の時間は `CPU` が 20.0 分，`Elapsed` が 33.0 分であった．消去法で得られた R 単独の方程式は 180 次で $Q(p_1)$ 係数，Q 上の既約因子は 24 次のものが 1 つと 156 次のものが 1 つであった．それらの既約因子は $Q(\omega_5)$ 上でも既約であった．

maxima 上ではグレブナ基底の構成よりも消去法の方がかなり高速に結果が得られることがわかる．しかし導かれた R 単独の方程式は，グレブナ基底を用いた場合には常に 24 次になるのに対して，消去法では 240 次や 180 次などとなり，216 次や 156 次などの余分と思われる既約因子が出現した．これらの余計と思われる既約因子の存在をどのように考えるべきかは不明である．

5.2 連立方程式をグレブナ基底計算を用いて Risa/Asir で解いた例

連立方程式から Risa/Asir のグレブナ基底を用いて R 単独の方程式を作り，それを Q 上で既約分解した．maxima でのグレブナ基底によるものと全く同一の結果が得られたが，Risa/Asir によるグレブナ基底の計算は maxima のものに比べて極めて速いことがわかる（下表に合計の CPU 時間と経過時間を示す）．パラメタを含んでいない場合のこれらの経過時間はどれも 0.1 秒未満である．パラメタを 1 つ含む 5 次方程式 $f = x^5 + 5p_1x + 1$ についての計算では，4 変数 4 連立方程式 (18) からグレブナ基底の構成までは 3.07 秒

ガロア群	多項式 f	（CPU，Elapsed）
S_5	x^5-5x^3+1	（0.0659 秒，0.0689 秒）
A_5	x^5+5x^3+1	（0.0653 秒，0.0774 秒）
F_{20}	$x^5+15x+12$	（0.0696 秒，0.0746 秒）
F_{10}	$x^5-5x+12$	（0.0748 秒，0.0792 秒）
F_5	$x^5-10x^3+5x^2+10x+1$	（0.0708 秒，0.0738 秒）

であったが，グレブナ基底から R 単独の方程式の多項式を求める計算はいつまでも終わらず，結果が得られなかった．その原因は不明である．

6　6 次方程式の場合

6 次方程式の場合には次数の 6 が素因数として 2 と 3 を持つことから，体 K で既約な monic な 6 次多項式 f は K のある拡大体 M までは既約だが，（R を M のある非平方元として）体 $M(R^{1/2})$ 上では 3 次の既約因子 2 つに分解するという場合と，（R を M のある非立方元とし，ω_3 を 1 の原始 3 乗根として）体 $M(R^{1/3},\omega^3)$ 上では 2 次の既約因子 3 つに分解するという場合の 2 つの場合について考える必要がある．

6.1　6 次方程式が平方根拡大で分解する場合

体 K の中で monic な方程式の既約 6 次多項式 f を式 (24) とする．

$$f=x^6+p_5\,x^5+p_4\,x^4+p_3\,x^3+p_2\,x^2+p_1\,x+p_0\,. \tag{24}$$

そうして f は K のある拡大体 M では既約だが，（R を M のある非平方元として）体 $M(\sqrt{R})$ では可約になると仮定する．そのとき既約因子の次数が 3 になることが示せる．そこで f が体 $M(\sqrt{R})$ では 3 次の既約因子 $f_0^{(3)}$（式 (25)）を持つと仮定する．ただし a_0，a_1，b_0，b_1，c_0，c_1，R はどれも M の元であり，R は M の非平方元であり，a_1，b_1，c_1 の中には非零のものが存在する．そのとき f は必ず別の 3 次の既約因子 $f_1^{(3)}$（式 (26)）も持つ．

$$f_0^{(3)}=x^3+(a_0+a_1\sqrt{R})x^2+(b_0+b_1\sqrt{R})x+c_0+c_1\sqrt{R}\,. \tag{25}$$

$$f_1^{(3)}=x^3+(a_0-a_1\sqrt{R})x^2+(b_0-b_1\sqrt{R})x+c_0-c_1\sqrt{R}\,. \tag{26}$$

これら 2 つの 3 次因子の積 $f_0^{(3)}f_1^{(3)}$ は係数が M で f を割り切る monic な 6 次式なので f に一致する．すると 2 通りに表された f の x の同次項の係数の等置から関係が得られる．その際に 6 次多項式 f の 5 次の項があらかじめ欠けていれば $a_0=0$ なので，式が少し簡単になる（式 (27)）．

$$\begin{cases} p_4=2b_0-a_1^2R\,,\ \ p_3/2=c_0-a_1\,b_1R\,,\ \ p_2=b_0^2-(2\,a_1\,c_1+b_1^2)R\,, \\ p_1/2=b_0\,c_0-b_1\,c_1R\,,\ \ p_0=c_0^2-c_1^2R\,. \end{cases} \tag{27}$$

この 6 つの変数 a_1，b_0，b_1，c_0，c_1，R を含む 5 連立の方程式 (27) を解くことになるが，体 M 上での平方数倍の自由度を R に吸収させることで変数の数を 1 つ減らせる．ただし a_1，b_1，c_1 の中には非零のものが存在することが必要なので，式 (25) の 3 次因子の係数に沿って，全部で 3 通りの排他的な場合に分けて扱う．場合 1 は $a_1=1$ であり，場合 2 は $a_1=0$ かつ $b_1=1$ であり，場合 3 は $a_1=b_1=0$ かつ $c_1=1$ である（非零の値を 1 にできる理由は，値の 2 乗を平方根号の内側の R が持つ自由度に吸収させるからである）．

場合 1：$a_1 = 1$. これは f が $M(\sqrt{R})$ で分解するような最も普通の場合であり，対応する連立方程式は式 (28) になる．

$$\begin{cases} p_4 = 2\,b_0 - R\,,\ \ p_3/2 = c_0 - b_1 R\,,\ \ p_2 = b_0^2 - (2\,c_1 + b_1^2)R\,, \\ p_1/2 = b_0\,c_0 - b_1\,c_1 R\,,\ \ p_0 = c_0^2 - c_1^2 R\,. \end{cases} \tag{28}$$

式 (28) 中の最初の 2 つを解いた $b_0 = (R + p_4)/2$ と $c_0 = b_1\,R + p_3/2$ を残りの 3 つに代入すると式 (29) が得られる．この 3 元 3 連立方程式 (29) を解いて変数 b_1，c_1，R を求める（6 次方程式の係数 p_0，p_1，p_2，p_3，p_4 はパラメタである）．これを手計算で解くのは面倒である．

$$\begin{cases} 4\,p_2 &=& (R + p_4)^2 - 4(2\,c_1 + b_1^2)\,R\,, \\ 2\,p_1 &=& (R + p_4)(2\,b_1 R + p_3) - 4\,b_1\,c_1\,R\,, \\ 4\,p_0 &=& (2\,b_1\,R + p_3)^2 - 4\,c_1^2\,R\,. \end{cases} \tag{29}$$

パラメタ 5 つ p_0，p_1，p_2，p_3，p_4 を含む 3 元 3 連立の式 (29) から変数 b_1 と c_1 を消去すると，R 単独の 20 次方程式が得られた（これは maxima の関数 eliminate を用いた消去計算によるもので，消去の計算時間は `CPU` が 0.91 秒，`Elapsed` が 0.92 秒であった）．その R の 20 次多項式は Q 上で既約な 10 次因子を 2 つに分解されて，各因子の展開形での項数は 156 と 158 であった（これは maxima の関数 factor を用いた多項式の因数分解の結果による）．

もしも 6 次方程式の係数 p_0，p_1，p_2，p_3，p_4 の値の組が特殊であって，2 つある R 単独の 10 次因子のどちらかがより低次の因子に分解されて，そのどれかが巾根で解ける解を持っている場合には，f の 6 次多項式は 3 次の因子 2 つに分解できるので，それからさらに各 3 次の因子の方程式を巾根を用いた表示で解くことができる（しかし以上の議論だけでは，2 つある 10 次の因子に対応する R 単独の 10 次方程式がどちらも既約の場合やどちらかが可約であっても 5 次の因子だけを持っていて 4 次以下の因子を持たない場合には，R の値が巾根で表されるのかどうかは分からない．）

場合 2：$a_1 = 0$ かつ $b_1 = 1$. この場合に解くべき連立方程式は式 (30) で与えられる．

$$p_4 = 2\,b_0\,,\ p_3/2 = c_0\,,\ \ p_2 = b_0^2 - R\,,\ \ p_1/2 = b_0\,c_0 - c_1 R\,,\ \ p_0 = c_0^2 - c_1^2 R\,. \tag{30}$$

式 (30) の中の最初の 2 式から $b_0 := p_4/2$，$c_0 := p_3/2$ であり，残りの 3 つの条件式 (31) が解を持つためには，パラメタは式 (32) の関係を満たす必要があることがわかる．そうしてパラメタが関係 (32) を満たす場合には残りの 2 つの変数 R と c_1 の値は式 (33) で与えられる．

$$4\,R = p_4^2 - 4\,p_2\,,\ \ 4\,c_1\,R = p_3\,p_4 - 2\,p_1\,,\ \ 4\,c_1^2\,R = p_3^2 - 4\,p_0\,, \tag{31}$$

$$(p_4^2 - 4\,p_2)(p_3^2 - 4\,p_0) = (p_3\,p_4 - 2\,p_1)^2\,. \tag{32}$$

$$R := (p_4^2 - 4\,p_2)/4\,,\ c_1 := (p_3\,p_4 - 2\,p_1)/(p_4^2 - 4\,p_2)\,. \tag{33}$$

場合 3：$a_1 = b_1 = 0$ かつ $c_1 = 1$. この場合には解くべき 5 連立の方程式は式 (34) になる．

$$p_4 = 2\,b_0\,,\ \ p_3/2 = c_0\,,\ \ p_2 = b_0^2\,,\ \ p_1/2 = b_0\,c_0\,,\ \ p_0 = c_0^2 - R\,. \tag{34}$$

解があるためにはパラメタは 2 つの条件式 $p_4^2 = 4\,p_2$，$2\,p_1 = p_3\,p_4$ を満たす必要がある．そうして残りの 3 変数 b_0，c_0，R の値はパラメタの値を使って $b_0 := p_4/2$，$c_0 := p_3/2$，$R := p_3^2/4 - p_0$ と決まる．

6.2　6 次方程式が立方根拡大で分解する場合

6 次多項式 f が K のある拡大体 M では既約だが,（M のある非立方元を R として）体 $M(R^{1/3})$ では可約とする．そのとき f は体 $M(R^{1/3})$ では式 (35) の形で表される 2 次の既約因子 $f_0^{(2)}$ を持つことになる．

$$f_0^{(2)} = x^2 + (a_0 + a_1 R^{1/3} + a_2 R^{2/3})\, x + b_0 + b_1 R^{1/3} + b_2 R^{2/3}\,. \tag{35}$$

そのとき 1 の原始 3 乗根を ω として，f は $M(R^{1/3}, \omega)$ において $f_0^{(2)}$ とは相異なる 2 次の既約因子 $f_1^{(2)}$ と $f_2^{(2)}$（式 (36)）も必ず持つということが言える．

$$\left\{ \begin{array}{l} f_1^{(2)} = x^2 + (a_0 + a_1\,\omega R^{1/3} + a_2\,\omega^2 R^{2/3})\, x + b_0 + b_1\,\omega R^{1/3} + b_2\,\omega^2 R^{2/3}\,, \\ f_2^{(2)} = x^2 + (a_0 + a_1\,\omega^2 R^{1/3} + a_2\,\omega R^{2/3})\, x + b_0 + b_1\,\omega^2 R^{1/3} + b_2\,\omega R^{2/3}\,. \end{array} \right. \tag{36}$$

3 つの異なる既約 2 次因子の積 $f_0^{(2)} f_1^{(2)} f_2^{(2)}$ は，M 係数で f を割り切る monic な 6 次多項式であるので，f に等しい．すると 2 通りに表された f の x についての同次項の係数を等置して関係が得られる．特に元の 6 次多項式 f の 5 次の項が欠けている場合には $a_0 = 0$ であり，関係は簡単化されて式 (37) になる．以下ではこの 5 次項の欠けた $a_0 = 0$ の場合についてだけ考えることにする．

$$\left\{ \begin{array}{rcl} p_4/3 &=& -\,a_1\,a_2 R + b_0,\ \ p_3 = a_2^3\,R^2 + (-3\,a_1\,b_2 - 3\,a_2\,b_1 + a_1^3)R, \\ p_2/3 &=& a_2^2\,b_2\,R^2 + (-b_1\,b_2 + a_1^2\,b_1 - a_1\,a_2\,b_0)R + b_0^2, \\ p_1/3 &=& a_2\,b_2^2\,R^2 + (-a_1\,b_0\,b_2 + a_1\,b_1^2 - a_2\,b_0\,b_1)R, \\ p_0 &=& b_2^3\,R^2 + (b_1^3 - 3\,b_0\,b_1\,b_2)R + b_0^3\,. \end{array} \right. \tag{37}$$

残る 6 変数 a_1，a_2，b_0，b_1，b_2，R についての 5 連立の方程式を解く際には，変数を 1 つ減らす必要があるが，いま仮定した 1 つの 2 次因子の形は (35) であった．すると次の排他的な 2 通りの場合だけを扱えば十分なことがわかる．場合 1 は $a_1 = 1$ であり，場合 2 は $a_1 = a_2 = 0$ かつ $b_1 = 1$ である．

場合 1：$a_1 = 1$. これは 5 次項が欠けた monic な 6 次方程式で最も普通の場合であり，式 (38) を解く必要がある．これは 5 つの変数 a_2，b_0，b_1，b_2，R の 5 連立方程式で，パラメタは p_0，p_1，p_2，p_3，p_4 の 5 つである．

$$\left\{ \begin{array}{rcl} p_4/3 &=& -\,a_2 R + b_0,\ \ p_3 = a_2^3\,R^2 + (-3\,b_2 - 3\,a_2\,b_1 + 1)R, \\ p_2/3 &=& a_2^2\,b_2\,R^2 + (-b_1\,b_2 + b_1 - a_2\,b_0)\,R + b_0^2,\ \ p_1/3 = a_2\,b_2^2\,R^2 + (-b_0\,b_2 + b_1^2 - a_2\,b_0\,b_1)R, \\ p_0 &=& b_2^3\,R^2 + (b_1^3 - 3\,b_0\,b_1\,b_2)R + b_0^3\,. \end{array} \right. \tag{38}$$

例題 1：5 次の項が欠けた 6 次方程式の多項式を $f = x^6 + 5x^4 + x^3 + x^2 + 2x + 1$ とする．これは各パラメタが $p_4 = 5$，$p_3 = 1$，$p_2 = 1$，$p_1 = 2$，$p_0 = 1$ の場合である．

連立方程式から変数を a_2，b_2，b_1，b_0 の順に消去し，R 単独の方程式にするための消去時間は `CPU` が 7.18 時間，`Elapsed` が 8.24 時間であった（maxima による）．R 単独の方程式の 1134 次多項式の Q 上での各既約因子は 30 次のものが 1 つ，60 次のものが 4 つ，96 次のものが 1 つ，192 次のものが 2 つ，384 次のものが 1 つであった．それらの既約な因子の中に巾根で解けるものがあるのかは，今の方法だけからでは分からない．

例題 2：5 次の項が欠けた 6 次方程式の多項式を $f = x^6 + 3x^4 + x^3 - 3x^2 + 3x + 1$ とする．これは各パラメタが $p_4 = 3$, $p_3 = 1$, $p_2 = -3$, $p_1 = 3$, $p_0 = 1$ の場合である．

連立方程式から変数を a_2，b_2，b_1，b_0 の順に消去し，R 単独の方程式にするための消去時間は `CPU` が 1.054 時間，`Elapsed` が 1.215 時間であった．R 単独の方程式の多項式の次数は 1134 で，その Q 上での既約分解の計算は，メモリ容量が 16GB では不足して破綻した（by maxima 5.48.1(GCL)）.（この既約分解の計算は Reduce や Risa/Asir を用いても同様にメモリ容量不足で破綻した）.

場合 2：$a_1 = a_2 = 0$ かつ $b_1 = 1$. この場合の解くべき連立方程式は式 (39) になる．

$$p_4/3 = b_0,\ \ p_3 = 0,\ \ p_2/3 = -b_2\,R + b_0^2,\ \ p_1/3 = 0,\ \ p_0 = b_2^3\,R^2 + (1 - 3\,b_0\,b_2)R + b_0^3\,. \tag{39}$$

これから $p_1 = 0$，$p_3 = 0$ であることが必要であり，$b_0 := p_4/3$ となるので関係式は式 (40) になる．

$$p_2/3 = -b_2\,R + (p_4/3)^2,\ \ p_0 = b_2^3\,R^2 + (1 - p_4\,b_2)R + (p_4/3)^3\,. \tag{40}$$

式 (40) から，$A \equiv (p_4/3)^2 - p_2/3$，$B \equiv (p_4/3)^3 - p_4\,A - p_0$，ただし $A \neq 0$ とおくと，式は (41) となり，この K 係数の b_2 の 2 次方程式を解くと，そのあとは $R := A/b_2$ となる．

$$b_2\,R = A,\ \ A^2\,b_2^2 + B\,b_2 + A = 0. \tag{41}$$

注：実はこの $a_0 = a_1 = a_2 = 0$ の場合は，$p_1 = p_3 = 0$ の場合で，元の 6 次方程式は奇数次項を欠けているから，$t = x^2$ とおくと $f = t^3 + p_4\,t^2 + p_2\,t + p_0$ となる．この K 上の t の 3 次方程式の 3 根を巾根を用いて表して，それらの平方根に正負の符号を付けたものが元の 6 次方程式の 6 つの解の巾根表示になる．

7　7 次方程式の場合

K 係数の 7 次多項式が K のある拡大体 M までは既約だが，(R を体 M のある非 7 乗数として) $M(R^{1/7})$ では分解すると仮定する．そうして f が $M(R^{1/7})$ では式 (42) で表される 1 次因子 $f_0^{(1)}$ を持つとする

$$f_0^{(1)} = x + a_0 + \sum_{k=1}^{6} a_k\,R^{k/7}\,. \tag{42}$$

すると ω_7 を 1 の原始 7 乗根として，f は $M(R^{1/7}, \omega_7)$ では式 (43) で表される相異なる 7 つの 1 次因子 $f_j^{(1)}$，$j = 0, 2, \ldots, 6$ を必ず持ち，それら 7 つの 1 次因子の積は f に等しい，つまり $f = \prod_{j=0}^{6} f_j^{(1)}$ である．

$$f_j^{(1)} = x + a_0 + \sum_{k=1}^{6} a_k\,\omega_7^{kj} R^{k/7}\,,\ j = 0, 1, \ldots, 6\,. \tag{43}$$

以下では簡単のため f は最初から 6 次の項が欠けた形とする（式 (44)）．

$$f = x^7 + 7p_5\,x^5 + 7p_4\,x^4 + 7p_3\,x^3 + 7p_2\,x^2 + 7p_1\,x + p_0\,. \tag{44}$$

すると $a_0 = 0$ である．さらに $a_1 = 1$ としてもよくて，f の x についての同次項の係数等置から 6 つの変数 a_6，a_5，a_4，a_3，a_2，R についての 6 連立方程式を得る（具体的な式はかなり長いので省略する）．その 6 連立方程式の解を巾根を用いて何回か拡大した体 M の中で表せれば，元の 7 次方程式の 7 つの解は R の 7 乗根と 1 の原始 7 乗根 ω_7 を M に添加した体の中で，それぞれ式 (45) で表せる．

$$x_j = -a_0 - \sum_{k=1}^{6} a_k\,\omega_7^{kj} R^{k/7}\,,\ j = 0, 1, \ldots, 6\,. \tag{45}$$

しかし，この複雑な 6 元 6 連立の方程式を代数的消去で解くことは，たとえ K が有理数体 Q で，方程式の係数 p_5，p_4，p_3，p_2，p_1，p_0 が全て簡単な定数であっても計算量が非常に多くなり過ぎるように思われる．現状ではごく簡単な例以外では，R 単独の方程式を導くことが Risa/Asir を用いてもできなかった．

- 例題 $f = x^7 - 2 = 0$ の場合．変数のリストは a_6，a_5，a_4，a_3，a_2，R で Risa/Asir のグレブナ基底計算により得られた R 単独の方程式の次数は 35 であり，その Q 上の既約因子は 1 次のものが 1 つ，2 次のものが 2 つ，3 次のものが 6 つ，6 次のものが 2 つであった．1 次因子は $R-2$ で，2 次の既約因子は $823543R^2+4$ と $823543R^2+33614R+512$ であった．この計算には約半日ほど掛かった．

- 例題 $f = x^7 + 7x + 2 = 0$ の場合．変数のリスト a_6，a_5，a_4，a_3，a_2，R で Risa/Asir のグレブナ基底計算により得られた R 単独の方程式の次数は 720 であった．グレブナ基底を作る計算の時間には `CPU` が 40.6 時間，`Elapsed` が 41.6 時間であった．R 単独の方程式を作る計算には `CPU` が 2.90 時間，`Elapsed` が 2.94 時間であった．得られた R の 720 次の多項式の Risa/Asir による Q 上の既約分解はどれだけ待っても終わらなかった．

8　8 次方程式の場合

体 K 上 monic な既約 8 次多項式 f が，ある拡大体 M 上では既約だが，体 M のある非平方元 R の平方根で拡大した体 $M(R^{1/2})$ では可約ならば，それらは式（式 (46)）の形で表せる相異なる既約 4 次の因子 2 つであって，$f = f_0^{(4)} f_1^{(4)}$ である（(47)）．

$$\left\{ \begin{array}{lcl} f_0^{(4)} & = & x^4 + (a_3 + b_3\sqrt{R})\,x^3 + (a_2 + b_2\sqrt{R})\,x^2 + (a_1 + b_1\sqrt{R})\,x + (a_0 + b_0\sqrt{R}), \\ f_1^{(4)} & = & x^4 + (a_3 - b_3\sqrt{R})\,x^3 + (a_2 - b_2\sqrt{R})\,x^2 + (a_1 - b_1\sqrt{R})\,x + (a_0 - b_0\sqrt{R}), \end{array} \right. \tag{46}$$

$$f = (x^4 + a_3\,x^3 + a_2\,x^2 + a_1\,x + a_0)^2 - (b_3\,x^3 + b_2\,x^2 + b_1\,x + b_0)^2\,R. \tag{47}$$

monic な 8 次多項式 f が最初から 7 次の項を欠いた形をしていれば $a_3 = 0$ である．そこで f を（式 (48)）で与えて x についての同次の項の係数を等置する．

$$f = x^8 + p_6\,x^6 + 2\,p_5\,x^5 + p_4\,x^4 + 2\,p_3 x^3 + p_2\,x^2 + 2\,p_1 x + p_0\,. \tag{48}$$

それから式 (49) の 8 変数 a_2，a_1，a_0，b_3，b_2，b_1，b_0，R の 7 連立の方程式が得られる．

$$\left\{ \begin{array}{l} p_6 = -{b_3}^2\,R + 2\,a_2,\ \ p_5 = -b_2\,b_3\,R + a_1, \\ p_4 = -(2\,b_1\,b_3 + {b_2}^2)\,R + {a_2}^2 + 2\,a_0,\ \ p_3 = -(b_0\,b_3 + b_1\,b_2)\,R + a_1\,a_2, \\ p_2 = -(2\,b_0\,b_2 + {b_1}^2)\,R + 2\,a_0\,a_2 + {a_1}^2,\ \ p_1 = -b_0\,b_1\,R + a_0\,a_1,\ \ p_0 = -{b_0}^2\,R\ + {a_0}^2\,. \end{array} \right. \tag{49}$$

R が持つ M の平方数を乗じる自由度を使うと，以下の排他的な 4 通りの場合についてを考えれば良いことがわかる．場合 1 は $b_3 = 1$ であり，場合 2 は $b_3 = 0$ かつ $b_2 = 1$ であり，場合 3 は $b_3 = b_2 = 0$ かつ $b_1 = 1$ であり，場合 4 は $b_3 = b_2 = b_1 = 0$ かつ $b_0 = 1$ である．後のものほど方程式の係数が特別な関係を満たしている必要がある．

<u>場合 1：$b_3 = 1$.</u> これは 7 次の項の欠けた 8 次方程式についての最も普通の場合になる．7 つの変数 b_2，b_1，b_0，a_2，a_1，a_0，R についての 7 連立の方程式 (50) を解く必要がある．

$$\left\{ \begin{array}{l} p_6 = -R + 2\,a_2,\ \ p_5 = -b_2\,R + a_1, \\ p_4 = -(2\,b_1 + {b_2}^2)\,R + {a_2}^2 + 2\,a_0,\ \ p_3 = -(b_0 + b_1\,b_2)\,R + a_1\,a_2, \\ p_2 = -(2\,b_0\,b_2 + {b_1}^2)\,R + 2\,a_0\,a_2 + {a_1}^2,\ \ p_1 = -b_0\,b_1\,R + a_0\,a_1,\ \ p_0 = -{b_0}^2\,R\ + {a_0}^2\,. \end{array} \right. \tag{50}$$

この連立方程式 (50) の解が，体 K を何回か巾根を添加して拡大した体 M に含まれるならば，元の K 係数の 8 次方程式 $f = 0$ は M 係数の 4 次方程式 2 つに分解され，各 4 次方程式の解を巾根を用いて表せば f の 8 つの解が巾根を用いた表現で得られる．この連立方程式をパラメタ付きで解くことは相当に困難であろう．

8.0.1　7 変数 7 連立方程式の計算例 (Risa/Asir)

- 8 次方程式 $f = x^8 + x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7$ の場合は，R 単独の方程式は次数 35 で，Q 上既約であった．

計算処理内容	(　CPU，Elapsed)
グレブナ基底を求める	(0.0370 秒，0.0374 秒)
R 単独の多項式を求める	(0.0422 秒，0.0426 秒)
R 単独の方程式の既約因数分解	(0.0091 秒，0.0092 秒

- 8 次方程式 $f = x^8 + x^5 + 2x^3 + 1$ の場合は，R 単独の方程式は次数 35 で，Q 上で 5 次と 30 次の既約因子に分解された．5 次の既約因子は $R^5 - 2R^4 + 5R^3 + 16R - 1$ であった．

計算処理内容	(　CPU，Elapsed)
グレブナ基底を求める	(0.0240 秒，0.0245 秒)
R 単独の多項式を求める	(0.0353 秒，0.0357 秒)
R 単独の方程式の既約因数分解	(0.0096 秒，0.0098 秒)

- 8 次方程式 $f = x^8 + 2x^6 + 3x^5 + 5x^4 + 3x^3 + 2x^2 + 1$ の場合は，R 単独の方程式は次数 35 で，Q 上 3 次と 8 次と 24 次の既約因子に分解された．3 次の既約因子は $R^3 - 4R^2 - 8R - 9$ であった．

計算処理内容	(　CPU，Elapsed)
グレブナ基底を求める	(0.0319 秒，0.0322 秒)
R 単独の多項式を求める	(0.0437 秒，0.0443 秒)
R 単独の方程式の既約因数分解	(0.0046 秒，0.0047 秒)

- 8 次方程式 $f = x^8 - 11x^6 - 50x^5 - 92x^4 + 2x^3 - 170x^2 + 48x - 62$ の場合は，R 単独の方程式は次数 35 で，Q 上 1 次と 16 次と 18 次の既約因子に分解された．1 次の因子は $R - 7$ であった．

計算処理内容	(　CPU，Elapsed)
グレブナ基底を求める	(0.0449 秒，0.0454 秒)
R 単独の多項式を求める	(0.0439 秒，0.0445 秒)
R 単独の方程式の既約因数分解	(0.0059 秒，0.0060 秒)

場合 2：$b_3 = 0$ かつ $b_2 = 1$. この場合には解くべき連立方程式は式 (51) になる．

$$\left\{ \begin{array}{lcl} p_6 &=& 2\,a_2,\ p_5 = a_1,\ p_4 = -R + {a_2}^2 + 2\,a_0,\ p_3 = -b_1\,R + a_1\,a_2, \\ p_2 &=& -(2\,b_0 + {b_1}^2)\,R + 2\,a_0\,a_2 + {a_1}^2,\ p_1 = -b_0\,b_1\,R + a_0\,a_1,\ p_0 = -{b_0}^2\,R\ + {a_0}^2\,. \end{array} \right. \tag{51}$$

すると，まず $a_2 := p_6/2$，$a_1 := p_5$ であるから，4 変数 b_1，b_0，a_0，R の 5 連立方程式 (52) になるが，それからはパラメタが満たすべき条件式が 1 つ出る．

$$\left\{ \begin{array}{l} p_4 = -R + (p_6/2)^2 + 2\,a_0,\ p_3 = -b_1\,R + p_5\,(p_6/2), \\ p_2 = -(2\,b_0 + {b_1}^2)\,R + 2\,(p_6/2)\,a_0 + {p_5}^2, \\ p_1 = -b_0\,b_1\,R + p_5\,a_0,\ p_0 = -{b_0}^2\,R\ + {a_0}^2\,. \end{array} \right. \tag{52}$$

式 (52) の中の 3 番目の式を飛ばした 4 連立式 (53) を考える．

$$R = 2a_0 + (p_6/2)^2 - p_4,\ b_1R = p_5(p_6/2) - p_3,\ b_0b_1R = p_5a_0 - p_1,\ b_0^2R = a_0^2 - p_0. \tag{53}$$

それの 1 番目と 3 番目の 2 乗の積，2 番目の 2 乗と 4 番目の積からそれぞれ関係 (54) が得られる．

$$\begin{cases} R\times(b_0b_1R)^2=\{2a_0+(p_6/2)^2-p_4\}\times(p_5a_0-p_1)^2. \\ (b_1R)^2\times(b_0^2R)=\{p_5(p_6/2)-p_3\}^2(a_0^2-p_0). \end{cases} \tag{54}$$

両者の左辺の一致から a_0 の 3 次方程式 (55)（ただし $p_5=0$ の場合は 2 次方程式になる）を得る．

$$\big\{2\,a_0+(p_6/2)^2-p_4\big\}(p_5\,a_0-p_1)^2-\big\{p_5\,(p_6/2)-p_3\big\}^2(a_0^2-p_0)=0\,. \tag{55}$$

この 3 次方程式を巾根を用いて解いて a_0 を表せば，式 (56) から R，b_1，b_0 が順番に求まる．

$$R:=2a_0+(p_6/2)^2-p_4\,,\ \ b_1:=\{p_5(p_6/2)-p_3\}/R\,,\ \ b_0:=\{2(p_6/2)a_0+p_5^2-p+2\}/(2R)-b_1^2/2\,. \tag{56}$$

そうして整合条件は $b_0^2\,R=a_0^2-p_0$ となる．

あるいは $b_1\neq0$ であるときは，$b_0:=(p_5\,a_0-p_1)/\{p_5(p_6/2)-p_3\}$ で，整合条件は $p_2=-(2\,b_0+{b_1}^2)\,R+2\,(p_6/2)\,a_0+{p_5}^2$ となる．

<u>場合 3：$b_3=b_2=0$ かつ $b_1=1$.</u> この場合は 5 変数 a_2，a_1，a_0，b_0，R についての 7 連立の方程式 (57) となる．

$$\begin{cases} p_6=2\,a_2,\ \ p_5=a_1,\ \ p_4={a_2}^2+2\,a_0,\ \ p_2=-R+2\,a_0\,a_2+{a_1}^2, \\ p_1=-b_0\,R+a_0\,a_1,\ \ p_3=a_1\,a_2,\ \ p_0=-{b_0}^2\,R\ +{a_0}^2\,. \end{cases} \tag{57}$$

解は順番に $a_2:=p_6/2$，$a_1:=p_5$，$a_0:=(p_4-a_2^2)/2$，$R:=2\,a_0\,a_2+a_1^2-p_2$，$b_0:=(a_0\,a_1-p_1)/R$ と解ける（方程式の多項式 f の体 M での既約性の仮定から R は必ず非零である）．

ただしパラメタ p_0，p_1，p_2，p_3，p_4，p_5，p_6 は 2 つの必要条件を満たす必要がある．それらはまず $p_3=p_5\,(p_6/2)$ であり，さらに a_0，b_0，R をパラメタで表した等式 $p_0=-b_0^2\,R+a_0^2$ である．

<u>場合 4：$b_3=b_2=b_1=0$ かつ $b_0=1$.</u> この場合は 4 変数 a_2，a_1，a_0，R で 7 連立の方程式 (58) になる．

$$\begin{cases} p_6=2\,a_2,\ \ p_5=a_1,\ \ p_4={a_2}^2+2\,a_0,\ \ p_0=-R\ +{a_0}^2\,,\ \ p_3=a_1\,a_2, \\ p_2=2\,a_0\,a_2+{a_1}^2,\ \ p_1=a_0\,a_1\,. \end{cases} \tag{58}$$

この解は $a_2:=p_6/2$，$a_1:=p_5$，$a_0:=(p_4-a_2^2)/2$，$R:=a_0^2-p_0$ となる．ただしパラメタは次の 3 つの条件を満たしていることが必要である．まず条件 $p_3=p_5\,(p_6/2)$ および，2 つの等式 $p_2=2\,a_0\,a_2+a_1^2$ と $p_1=a_0\,a_1$ をが含む a_2，a_1，a_0 をそれぞれパラメタで表したものをそれぞれ満たすことである．

9　9 次方程式の場合

体 K 上 monic な既約 9 次多項式 f がある拡大体 M 上では既約だが，体 M のある非立方元を R として，体 $M(R^{1/3})$ では分解するならば，f は $M(R^{1/3},\omega_3)$ で相異なる既約な 3 次因子 3 つ（式 (60)）を持つことが言える．そうして $f=f_0^{(3)}f_1^{(3)}f_2^{(3)}$ である．

$$\begin{cases} f_0^{(3)}=x^3+(a_2+b_2R^{1/3}+c_2R^{2/3})x^2+(a_1+b_1R^{1/3}+c_1R^{2/3})x+a_0+b_0R^{1/3}+c_0R^{2/3}, \\ f_1^{(3)}=x^3+(a_2+b_2R^{1/3}\omega_3+c_2R^{2/3}\omega_3^2)x^2+(a_1+b_1R^{1/3}\omega_3+c_1R^{2/3}\omega_3^2)x+a_0+b_0R^{1/3}\omega_3+c_0R^{2/3}\omega_3^2, \\ f_2^{(3)}=x^3+(a_2+b_2R^{1/3}\omega_3^2+c_2R^{2/3}\omega_3)x^2+(a_1+b_1R^{1/3}\omega_3^2+c_1R^{2/3}\omega_3)x+a_0+b_0R^{1/3}\omega_3^2+c_0R^{2/3}\omega_3\,. \end{cases} \tag{59}$$

K 係数の monic な 9 次多項式 f を式 (60) で与えて x の同次項の係数を等置する．

$$f=x^9+3\,p_8\,x^8+3\,p_7\,x^7+p_6\,x^6+3\,p_5\,x^5+3\,p_4\,x^4+p_3\,x^3+3\,p_2\,x^2+3\,p_1\,x+p_0\,. \tag{60}$$

ただし以下では f は 8 次項が欠けているとする．すると $a_2 = 0$ となり，9 変数 b_2，c_2，a_1，b_1，c_1，a_0，b_0，c_0，R についての 8 連立代数関係式 (61) が得られる．

$$\left\{\begin{array}{rcl} p_7 &=& -c_2\,b_2\,R + a_1, \quad p_6 = c_2^3\,R^2 + (b_2^3 - 3\,c_1\,b_2 - 3\,c_2\,b_1)\,R + 3\,a_0, \\ p_5 &=& c_1\,{c_2}^2\,R^2 + (b_1\,b_2^2 - c_2\,b_2\,a_1 - c_0\,b_2 - c_1\,b_1 - c_2\,b_0)\,R + a_1^2, \\ p_4 &=& (c_0\,c_2^2 + c_1^2\,c_2)\,R^2 + (b_0\,b_2^2 + b_1^2\,b_2 - c_1\,b_2\,a_1 - c_2\,b_1\,a_1 - c_2\,b_2\,a_0 - c_0\,b_1 - c_1\,b_0)\,R + 2\,a_0\,a_1, \\ p_3 &=& (6\,c_0\,c_1\,c_2 + c_1^3)\,R^2 + (6\,b_0\,b_1\,b_2 + b_1^3 - 3\,c_0\,b_2\,a_1 - 3\,c_1\,b_1\,a_1 \\ && -3\,c_2\,b_0\,a_1 - 3\,c_1\,b_2\,a_0 - 3\,c_2\,b_1\,a_0 - 3\,c_0\,b_0)\,R + a_1^3 + 3\,a_0^2, \\ p_2 &=& (c_0^2\,c_2 + c_0\,c_1^2)\,R^2 + (b_0^2\,b_2 + b_0\,b_1^2 - c_0\,b_1\,a_1 - c_1\,b_0\,a_1 - c_0\,b_2\,a_0 - c_1\,b_1\,a_0 - c_2\,b_0\,a_0)\,R + a_0\,a_1^2, \\ p_1 &=& c_0^2\,c_1\,R^2 + (b_0^2\,b_1 - c_0\,b_0\,a_1 - c_0\,b_1\,a_0 - c_1\,b_0\,a_0)\,R + a_0^2\,a_1, \\ p_0 &=& c_0^3\,R^2 + (b_0^3 - 3\,c_0\,b_0\,a_0)\,R + a_0^3\,. \end{array}\right. \tag{61}$$

式 (60) の 3 次因子の形から（但し $a_2 = 0$ とした），9 変数の 8 連立方程式 (61) を次の 3 通りの排他的な場合に分けて解く．場合 1 は $b_2 = 1$ であり，場合 2 は $b_2 = c_2 = 0$ かつ $b_1 = 1$ であり，場合 3 は $b_2 = c_2 = b_1 = c_1 = 0$ かつ $b_0 = 1$ である（場合分けで非零の係数を 1 にできる理由は，R に非零倍の自由度を吸収させられるからである）．

場合 1：$b_2 = 1$. これは 8 次の項が欠けた 9 次方程式についての最も普通の場合である．変数が 8 つ a_1，a_0，b_1，b_0，c_2，c_1，c_0，R の 8 連立代数関係式 (62) を解く必要がある．

$$\left\{\begin{array}{rcl} p_7 &=& -c_2\,R + a_1, \;\; p_6 = c_2^3\,R^2 + (1 - 3\,c_1 \, - 3\,c_2\,b_1)\,R + 3\,a_0, \\ p_5 &=& c_1\,{c_2}^2\,R^2 + (b_1 - c_2\,a_1 - c_0 - c_1\,b_1 - c_2\,b_0)\,R + a_1^2, \\ p_4 &=& (c_0\,c_2^2 + c_1^2\,c_2)\,R^2 + (b_0 + b_1^2 - c_1\,a_1 - c_2\,b_1\,a_1 - c_2\,a_0 - c_0\,b_1 - c_1\,b_0)\,R + 2\,a_0\,a_1, \\ p_3 &=& (6\,c_0\,c_1\,c_2 + c_1^3)\,R^2 + (6\,b_0\,b_1 + b_1^3 - 3\,c_0\,a_1 - 3\,c_1\,b_1\,a_1 \\ && -3\,c_2\,b_0\,a_1 - 3\,c_1\,a_0 - 3\,c_2\,b_1\,a_0 - 3\,c_0\,b_0)\,R + a_1^3 + 3\,a_0^2, \\ p_2 &=& (c_0^2\,c_2 + c_0\,c_1^2)\,R^2 + (b_0^2 + b_0\,b_1^2 - c_0\,b_1\,a_1 - c_1\,b_0\,a_1 - c_0\,a_0 - c_1\,b_1\,a_0 - c_2\,b_0\,a_0)\,R + a_0\,a_1^2, \\ p_1 &=& c_0^2\,c_1\,R^2 + (b_0^2\,b_1 - c_0\,b_0\,a_1 - c_0\,b_1\,a_0 - c_1\,b_0\,a_0)\,R + a_0^2\,a_1, \\ p_0 &=& c_0^3\,R^2 + (b_0^3 - 3\,c_0\,b_0\,a_0)\,R + a_0^3\,. \end{array}\right. \tag{62}$$

場合 2：$b_2 = c_2 = 0$ かつ $b_1 = 1$. この場合には変数は 7 つ a_1，a_0，b_0，c_2，c_1，c_0，R で，8 連立の方程式は式 (63) になる．パラメタは等式を 1 つ満たす必要がある．(この連立方程式は頑張れば手計算でも解けるかもしれない).

$$\left\{\begin{array}{l} p_7 = a_1, \;\; p_6 = c_2^3\,R^2 + 3\,a_0, \; p_5 = -c_1\,R + a_1^2, \; p_4 = -(c_0 + c_1\,b_0)\,R + 2\,a_0\,a_1, \\ p_3 = c_1^3\,R^2 + (1 - 3\,c_1\,a_1 - 3\,c_0\,b_0)\,R + a_1^3 + 3\,a_0^2, \\ p_2 = c_0\,c_1^2\,R^2 + (b_0 - c_0\,a_1 - c_1\,b_0\,a_1 - c_1\,a_0)\,R + a_0\,a_1^2, \\ p_1 = c_0^2\,c_1\,R^2 + (b_0^2 - c_0\,b_0\,a_1 - c_0\,a_0 - c_1\,b_0\,a_0)\,R + a_0^2\,a_1, \\ p_0 = c_0^3\,R^2 + (b_0^3 - 3\,c_0\,b_0\,a_0)\,R + a_0^3\,. \end{array}\right. \tag{63}$$

場合 3：$b_2 = c_2 = b_1 = c_1 = 0$ かつ $b_0 = 1$. この場合には残る変数は 4 つ a_1，a_0，c_0，R であり，連立方程式は 4 連立で式 (64) であり，パラメタは 4 つの等式条件を満たすことが必要である．

$$\left\{\begin{array}{l} p_7 = a_1, \; p_6 = 3\,a_0, \; p_5 = a_1^2, \; p_4 = 2\,a_0\,a_1, \; p_2 = a_0\,a_1^2, \\ p_3 = -3\,c_0\,R + a_1^3 + 3\,a_0^2, \; p_1 = -c_0\,a_1\,R + a_0^2\,a_1, \; p_0 = c_0^3\,R^2 + (1 - 3\,c_0\,a_0)\,R + a_0^3\,. \end{array}\right. \tag{64}$$

まずパラメタは $p_7^2 = p_5$，$2\,p_6\,p_7 = 3\,p_4$，$3p_2 = p_5\,p_6$ を満たすことが必要であり，$a_1 := p_7$，$a_0 := p_6/3$ となり，あとの c_0 と R については 3 連立の式 (65) が得られる．

$$p_3 = -3\,c_0\,R + p_7^3 + 3(p_6/3)^2,\ p_1 = -p_7\,c_0\,R + p_7\,(p_6/3)^2,\ p_0 = c_0^3\,R^2 + (1 - p_6 c_0)\,R + (p_6/3)^3. \quad (65)$$

関係 $c_0\,R = p_7^3 + 3(p_6/3)^2 - p_3$ を使うと，パラメタが満たすべき最後の必要条件は (66) となる．

$$p_1 = -p_7\{p_7^3 + 2(p_6/3)^2 - p_3\}. \quad (66)$$

そうして R は式 (67) の 2 次方程式の解である．

$$R^2 + \left[(p_6/3)^3 - p_6\{p_7^3 + 3(p_6/3)^2 - p_3\} - p_0\right] R + \{p_7^3 + 3(p_6/3)^2 - p_3\}^3 = 0\,. \quad (67)$$

それから $c_0 := \{p_7^3 + 3(p_6/3)^2 - p_3\}/R$ となる．よって，この場合には，巾根拡大で元の 9 次方程式を 3 つの 3 次因子に分解できて，それぞれの 3 次の方程式を巾根で解けば 9 つの根が得られる．

9.1 9 次方程式を分解した実験例（Risa/Asir による）

- 例題 1：9 次方程式 $f = x^9 + 2 = 0$ の場合（これは $t = x^3$ の 3 次方程式である）．グレブナ基底の作成の時間は `CPU` が 98.83 秒, `Elapsed` が 100.9 秒で，R 単独の方程式の作成の時間は `CPU` が 0.50 秒，`Elapsed` が 0.51 秒であった．(なおグレブナ基底から求まる R 単独の方程式の多項式は次数が 111 であったが，R^3 の多項式としては 37 次であった．) R についての 111 次式の既約分解は `CPU` が 0.31 秒で，`Elapsed` が 0.31 秒であった．分解で得られた既約因子は 3 次のもの 1 つ，9 次のものが 6 つ，18 次のものが 2 つであった．3 次の因子は $R^3 - 2$ であった．
- 例題 2：9 次方程式 $f = x^9 + 3\,x^7 + 1 = 0$ の場合．グレブナ基底の作成の時間は `CPU` が 22.3 分，`Elapsed` が 22.9 分であった．R 単独の方程式の作成時間は `CPU` が 3.71 分，`Elapsed` が 3.78 分であった．R 単独の方程式の次数は 560 で，その Q 上での既約分解はどれだけ待っても計算が終わらずに中止にした．
- 例題 3：9 次方程式 $f = x^9 + 3\,x^7 + 5 = 0$ の場合．グレブナ基底の作成には 3.46 時間で，基底から R 単独の方程式の作成は 4.29 分で，R 単独の方程式の多項式の次数は 560 で，その Q 上での既約分解はどれだけ待っても計算が終わらずに中止した．

10 まとめ

低次の 1 変数代数方程式の巾根解法を，巾根を添加された体上での多項式の因数分解の観点で扱うことを試みた．因数分解が成立するための条件から多変数の連立代数方程式が生じる．その求解計算は元の方程式の次数の増加に伴って次第に困難になる．

5 次方程式の場合には，単独変数 R の 24 次方程式が生じる．今回の方法では元の 5 次方程式の係数がごく少ない桁数の整数であっても，この R についての方程式は係数が長大な桁数の整数になり手計算で求めることは到底無理であるし，その 24 次多項式の既約分解も手計算では無理である．連立方程式の数式解法は，多くの演算量とメモリ容量を必要とする．Risa/Asir のグレブナ基底計算は maxima のものに比べて極めて速いが，その理由は多変数の多項式の内部表現の違いによるものであろう．

連立方程式から消去により R 単独の高次代数方程式が生じるが，それがたとえば巾根解法で解けるような低次の既約因子を持つならば元の方程式の解は巾根による表示を持つ．しかしどの既約因子の次数も高い場合には今回の簡単な議論だけでは再びそれら因子に対応する多項式の根が巾根で表示できるかを調べることになる．例えば体 K 上の monic な既約 5 次方程式 $f = 0$ の K 上のガロア群が対称群 S_5 や交代群 A_5 であって巾根による解の表現が不可能な場合でも，今回の簡単な議論だけからではそのことは分からない．