

数学コンサルタントシステムGALOISにおける 根号による1の原始 n 乗根の解法

元吉 文男
(電子技術総合研究所)

1. はじめに

近年、計算機による知識情報処理の研究が盛んに行われるようになり、筆者等も数学についての知識を処理する数学コンサルタントシステムGALOISの開発に着手したが、そこでは数学の様々な概念を扱う予定である。なかでも数は重要な概念であり、これをきちんと扱えるようにする必要がある。整数や有理数については従来からきちんとした処理が行われているが、代数的数については数として扱うのではなく式として扱っている処理系が多い(たとえば逆数を求める場合の処理において)。

GALOISにおいては代数的数も数として扱うように設計したが、その応用として1の原始 n 乗根を根号を使って求めるプログラムを作成した。また、そのアルゴリズムも従来のものは複数の根号がある場合に、それらの間の分岐のとりかたに制限があるために正しい答えを示すには分岐のとりかたを指定しなければならなかった。ここで紹介する方法は、同じ式が中に表われる根号については同じ分岐をとるという制限だけで、あとは自由な分岐をとることができる。

2. GALOIS

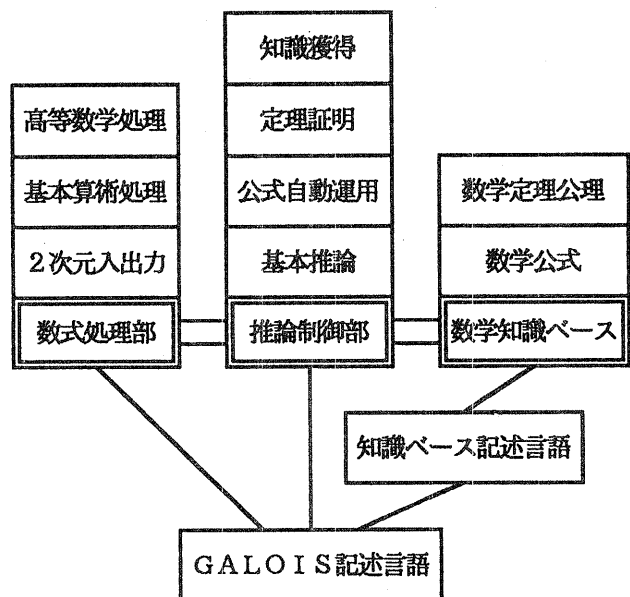
ここで簡単にGALOISの紹介をしておく。GALOISは、数学に関する知識を持ち、式に対する演算も行うことのできる数学コンサルタントシステムとなることを目標に、筆者等が作成中のシステムである。全体の構成を右図に示しておく。

この図で数式処理部は従来の数式処理システムが行ってきたことに加えて、集合や演算子などという概念も扱えるようにする。集合も要素を数えあげる直接的なものだけでなく、論理式による間接的なものまで含める。そのためには論理式の処理も行える必要がある。またユーザとのインターフェースにはビットマップディスプレイによる2次元表示を使用する。

数学知識ベース部には、各種の

GALOIS

General ALgebra-Oriented
Inference System



公理・定義・定理や公式を持ち、ユーザからの要求に応じて、あるいは推論制御部における自動運用のために使用される。

推論制御部は与えられた問題を解くために、知識ベース部や数式処理部を呼び出して実際の推論を行う部分である。この際の基本的な推論機構としてはP r o l o gに似た形をとる。ただし式のマッチングは同じ構造かどうかという構文的なものではなく、数学的に同じ式かどうかという意味までを考えた方法で行う。もう1つの重要な相違点はP r o l o gは式が証明されない場合には、否定されたものと考えているが、それでは不十分なので肯定が証明される、否定が証明される、両方とも証明されないという3通りの状態による推論を行うようにする。

3. GALOISにおける根号の意味

x の n 乗根 $a = \sqrt[n]{x}$ というのは n 乗して x になる数のことであるが、このような数は n 個あり、 a によってそのうちのどれを表わすかが問題となる。 x が正の実数のときは普通 a は正の実数になるようにしている。しかし x が複素数のときにはどれにするかが明らかではない。偏角を最小にするようにする方法もあるが、これでも問題が生じることがあ

$$x^3 + p x + q = 0 \quad \dots\dots\dots (1)$$

$$t_1 = -\frac{q}{2} + \sqrt{\left(\frac{p}{2}\right)^2 + \left(\frac{q}{3}\right)^3}, \quad t_2 = -\frac{q}{2} - \sqrt{\left(\frac{p}{2}\right)^2 + \left(\frac{q}{3}\right)^3} \quad \dots\dots\dots (2)$$

$$x = \sqrt[3]{t_1} + \sqrt[3]{t_2} \quad \dots\dots\dots (3)$$

る。たとえば3次方程式(1)が与えられたときに、よく $t_1 \cdot t_2$ を(2)のようにして、(3)で示される x が根であるとするが、このときには t_1 の3乗根と t_2 の3乗根のとりかたは独立ではなく、その積が $-p/3$ であるという関係がある。そこでいつも偏角が最小になるようにしていたのでは不都合が生じる。

GALOISでは根号で示される式は、そのどの分岐をとってもよいようにする。ただしいったん分岐を定めたならば、以後根号の中に入る式が同じものについては前と同じ分岐をとることにする。この条件はもうすこし緩めることが可能で、実際、同じところで根号にしたもののだけを同じ分岐にするようにしても以後の計算に不都合は生じない。しかし、これでは出力のときにどの根号どうしが同じ分岐であるかをいちいち指定しなくてはならず不便であるので最初に述べた方策に従うことにした。ただし、こうすることによって上の例における(3)式のような書き方が許されなくなる。GALOISでは(3)の根は次のように表わすことになる。すなわち、分岐のとりかたが依存しているような根号は一

$$x = \sqrt[3]{t_1} - \frac{p}{3 \sqrt[3]{t_1}} \quad \dots\dots\dots (4)$$

つの根号で表わさなければならない。(4)式では分岐のとりかたによって自動的に3つの根が表現されている。

4. “1”の原始n乗根の解法

1の原始n乗根を ω_n とする。原始n乗根というのは次の式を満たす数のことである。

$$\omega_n^n = 1 \quad \text{かつ} \quad \omega_n^m \neq 1 \quad 0 < m < n$$

まずnが素数の場合に帰着されることを示す。

I. $n = p^k$ のとき (pは素数)

$$\omega_n = \sqrt[k]{\omega_p} \text{ が1の原始n乗根となる (どの分岐をとっても) }。$$

II. $n = p \cdot q$ のとき (pとqは互いに素)

$x = \omega_p \omega_q$ を考える。このとき、 $\omega_p = \omega_{pq}^q = \omega_n^q$ 、 $\omega_q = \omega_{pq}^p = \omega_n^p$ と書ける。

すると $x = \omega_n^{p+q}$ となるが、 $\gcd(n, p+q) = 1$ なのでxが1の原始n乗根である。

nが素数でない場合は上の2つのどちらかになる。最後にnが素数の場合についての解法を説明するが、3節で述べたように、分岐のとりかたが相互に依存する根号が存在することのないようにしてある。

III. nが素数のとき

1) 次のような整数列 f_j を求める。

$$1 = f_m < \dots < f_1 < f_0 = n - 1$$

ただし、 f_j は f_{j-1} を割り切り、 $p_j = f_{j-1} / f_j$ は素数である。(1 ≤ j ≤ m)

$$e_j = (n - 1) / f_j \text{ としておく。}$$

2) nの原始根をrとし、 $\zeta_0 = \omega_n$ 、 $\zeta_{i+1} = \zeta_i^r$ ($0 \leq i < n - 1$) とする。

ここでの計算は ω_n を変数とみなして、 ω_n に関する多項式として計算を進める。ただし、n次以上の項は次の関係により消去することができる。

$$\omega_n^n - 1 = 0$$

以後の計算においても同様に行う。

3) 各jについて次のことを繰り返す ($1 \leq j \leq m$)。

3. 1) 1)における e_j 、 e_{j-1} 、 f_j を使用して

$$\eta_{j,i} = \zeta_{ie_{j-1}} + \zeta_{e_j + ie_{j-1}} + \dots + \zeta_{(f_j-1)e_j + ie_{j-1}} \quad (0 \leq i < p_j)$$

を計算する (ガウスのf項周期)。

なおj=0については次のようにしておく。

$$\eta_{0,0} = \zeta_0 + \zeta_1 + \dots + \zeta_{n-2} = \omega + \omega^2 + \dots + \omega^{n-1} = -1$$

3. 2) $\eta_{j,0}$ を次の手順に従って求める。

i) I I I の手続きを再帰的に使用して 1 の原始 p_j 乗根 ω_{p_j} を求める。

i i) ラグランジュの分解式を次のように求める。

$$\langle \omega_{p_j}^k, \eta_j \rangle = \sum_{i=0}^{p_j-1} \omega_{p_j}^{ik} \eta_{j,i} \quad \text{と定義する。} \quad \dots \dots \dots (*)$$

このとき $\langle \omega_{p_j}^0, \eta_j \rangle = \sum_{i=0}^{p_j-1} \eta_{j,i} = \eta_{j-1,0}$ である。

また $u_{j,k} = \langle \omega_{p_j}^k, \eta_j \rangle \langle \omega_{p_j}, \eta_j \rangle^{p_j-k}$ は ω_n の多項式であるが、これ

は $\eta_{j-1,0}$ を表わす ω_n の式を使用して ω_n を消去できることが知られている。

($1 \leq k < p_j$)

$\eta_{j-1,0}$ はすでに根号で表わされているので $u_{j,k}$ も根号で表わしている。

この $u_{j,k}$ を使用して

$$\langle \omega_{p_j}, \eta_j \rangle = \sqrt[p_j]{u_{j,1}} \quad \text{がまず求まり、} \quad 2 \leq k < p \quad \text{については}$$

$$\langle \omega_{p_j}^k, \eta_j \rangle = u_{j,k} \langle \omega_{p_j}, \eta_j \rangle^{k-p_j} = u_{j,k} \langle \omega_{p_j}, \eta_j^k \rangle / u_{j,1}$$

によって求まる。ここで (*) 式の k について 0 から $p_j - 1$ まで加えると、

$$p_j \eta_{j,0} = \sum_{k=0}^{p_j-1} \langle \omega_{p_j}^k, \eta_j \rangle \quad \text{となり、} \quad \eta_{j,0} \quad \text{が根号によって表わされる。}$$

4) 3) によって求めた $\eta_{m,0}$ が 1 の原始 n 乗根 ω_n である。

5. 例——“1”の原始14乗根

前節のアルゴリズムを n が 14 の場合に当てはめて、1 の原始 14 乗根を実際に求めてみる。

$n = 2 \cdot 7$ であり、2 と 7 は互いに素であるので前節の I I の場合に当たる。そこで

$$\omega_{14} = \omega_7 \omega_2 = -\omega_7$$

となり ($\omega_2 = -1$ である)、結局 ω_7 を求めればよい。

$n = 7$ として前節の I I I の手続きを行う。

1) 各 f_j を求める

$f_0 = n - 1 = 6$ であり、これより $f_1 = 2$ 、 $f_2 = 1$ が求まり、 $m = 2$ であることがわかる。そこで、 $e_0 = (n - 1) / f_0 = 1$ 、 $p_1 = f_0 / f_1 = 3$ 、

$$e_1 = (n - 1) / f_1 = 3, \quad p_2 = f_1 / f_2 = 3, \quad e_2 = (n - 1) / f_2 = 1.$$

2) 各 η_i を求める ($0 \leq i < 6$)

3 は 7 の原始根であるので $r = 3$ とする。すると、 $\zeta_0 = \omega_7$ 、 $\zeta_1 = \omega_7^3$ 、
 $\zeta_2 = (\omega_7^3)^3 = \omega_7^2$ 、 $\zeta_3 = (\omega_7^2)^3 = \omega_7^6$ 、 $\zeta_4 = (\omega_7^6)^3 = \omega_7^4$ 、
 $\zeta_5 = (\omega_7^4)^3 = \omega_7^5$ となる。

3) $j = 1$ 、2 についての繰り返し

$j = 1$ の場合

$$\eta_{1,0} = \zeta_0 + \zeta_3 = \omega_7 + \omega_7^6, \quad \eta_{1,1} = \zeta_1 + \zeta_4 = \omega_7^3 + \omega_7^4,$$

$$\eta_{1,2} = \zeta_2 + \zeta_5 = \omega_7^2 + \omega_7^5 \quad \text{となる。また、1 の原始 3 乗根を } \omega_3 \text{ とすると、}$$

$$\langle \omega_3^k, \eta_1 \rangle = \eta_{1,0} + \omega_3^k \eta_{1,1} + \omega_3^{2k} \eta_{1,2} \quad \text{である。}$$

$$\text{このとき、} \langle \omega_3^0, \eta_1 \rangle = \eta_{0,0} = -1 \text{ である。次に各 } u_k \text{ を求める。}$$

$$\langle \omega_3, \eta_1 \rangle^3 \text{ を計算して } u_{1,1} = -7(3\omega_3 + 1) \quad \text{となり、}$$

$$\langle \omega_3^2, \eta_1 \rangle \langle \omega_3, \eta_1 \rangle \text{ を計算して、} u_{1,2} = 7 \text{ となる。}$$

$$\text{よって、} \langle \omega_3, \eta_1 \rangle = \sqrt[3]{-7(3\omega_3 + 1)} \quad \text{が求まり、これを使用して}$$

$$\langle \omega_3^2, \eta_1 \rangle = 7 \cdot \sqrt[3]{-7(3\omega_3 + 1)^2} / (-7(3\omega_3 + 1))$$

$$= (3\omega_3 + 2) \sqrt[3]{-7(3\omega_3 + 1)^2} / 7 \quad \text{となる。}$$

$$\begin{aligned} \therefore \eta_{1,0} &= (-7 + 7 \sqrt[3]{-7(3\omega_3 + 1)} \\ &\quad + (3\omega_3 + 2) \sqrt[3]{-7(3\omega_3 + 1)^2}) / 21 \end{aligned}$$

$j = 2$ の場合

$$\eta_{2,0} = \zeta_0 = \omega_7, \quad \eta_{2,1} = \zeta_3 = \omega_7^6 \quad \text{となる。}$$

$$\langle \omega_2^k, \eta_2 \rangle = \eta_{2,0} + \omega_2^k \eta_{2,1} \quad \text{であるが、} \omega_2 \text{ は 1 の原始 2 乗根、すなわち } -1 \text{ である。このとき、}$$

$$\langle \omega_2^0, \eta_2 \rangle = \omega_7 + \omega_7^6 = \eta_{1,0} \quad \text{で、これは } j = 1 \text{ の場合に求めてある。}$$

$$\text{また、} u_{2,1} = \langle \omega_2, \eta_2 \rangle^2 = (\omega_7 - \omega_7^6)^2 = \omega_7^2 + \omega_7^5 - 2$$

$$= (\omega_7 + \omega_7^6)^2 - 4 = \eta_{1,0}^2 - 4 \quad \text{となって、} \eta_{1,0} \text{ で表わせた。}$$

$$\text{そこで、} \langle \omega_2, \eta_2 \rangle = \sqrt{\eta_{1,0}^2 - 4} \quad \text{となる。}$$

$$\therefore \eta_{2,0} = (\eta_{1,0} + \sqrt{\eta_{1,0}^2 - 4}) / 2$$

4) 3) で求めた $\eta_{2,0}$ が 1 の原始 7 乗根 ω_7 である (正確には ω_3 に 1 の原始 3 乗根 $(-1 + \sqrt{-3}) / 2$ を代入したものが)。

この最後の $j = 2$ の場合にもアルゴリズムを確かめるために方法に忠実に従ったが、実は一般的に次のことがいえる。最後のステップは $j = m$ であるが、このとき $f_{m-1} = 2$ とすることができる (n は 2 と異なる素数としてよいので、 $n - 1$ は偶数となる)。

$\eta_{m-1,0} = \zeta_0 + \zeta_{(n-1)/2} = \omega_n + \omega_n^{r^{(n-1)/2}} = \omega_n + \omega_n^{-1}$
 となる ($r^{n-1} = 1 \pmod{n}$) から $r^{(n-1)/2} = -1 \pmod{n}$ がいえる)。この式を変形すると次の式になる。

$$\omega_n^2 - \eta_{m-1,0} \omega_n + 1 = 0$$

これを解くことによって直ちに次の式が得られる。

$$\omega_n = (\eta_{m-1,0} + \sqrt{\eta_{m-1,0}^2 - 4}) / 2$$

以上のことより、 $f_{m-1} = 2$ とすることによって $\eta_{j,0}$ ($1 \leq j < m$) は実数であることがわかる。

上のようにして ω_7 が求まったので、1 の 14 乗根が次のように求まった。

$$\omega_{14} = -(\eta_{1,0} + \sqrt{\eta_{1,0}^2 - 4}) / 2,$$

$$\begin{aligned} \text{ただし } \eta_{1,0} = & (-7 + 7 \sqrt[3]{-7(3\omega_3 + 1)}) \\ & + (3\omega_3 + 2) \sqrt[3]{-7(3\omega_3 + 1)^2} / 21, \end{aligned}$$

$$\omega_3 = (-1 + \sqrt{-3}) / 2$$

6. インプリメンテーション

4 節のアルゴリズムは実際に GALOIS にインプリメントされているが、内部表現等について説明する。

GALOIS では、 n 乗根を表わす根号だけでなく、 $\alpha^5 + \alpha + 1 = 0$ を満たす数 α というような一般的な代数的数も整数・有理数と対等なコンスタントとして扱うように設計してある。そこで n 乗根を表わす根号は代数的数の特別な場合、すなわち $\sqrt[n]{x}$ は $\alpha^n = x$ を満たす α のことである、として扱っている。また 4 節で述べたような根号の意味をとることにすれば、簡単化の規則は単に定義多項式を法とする計算を行うだけになる。

代数的数を GALOIS において表現するには GAL におけると同様の方法を用いているが、簡単にそれを紹介する。代数的数を表現するには、その数を変数とする多項式が考えられる。この方法は加減乗算については十分であるが、除算のときに手数のかかる分母の有理化を行わなければならない。さらに、分母を有理化しないほうが式が簡単になる場合もあり、一律に有理化を行うのも考えものである。GALOIS では、代数的数を有理式として表現しておき、必要に応じ、あるいはユーザの求めに応じて分母の有理化を行うようにしている。このとき、根号だけを含む式の分母の有理化は一般的な代数的数の場合より簡単にできるが、いまのところ一般的な場合についてしかインプリメントしていないので効率が少し悪くなっている。なお、この表現における有理式の分母・分子は多変数の多項式であるが、その係数は整数になるようにしておく。

また根号の中に入る式は整数係数の多項式となるようにしてある。そこで、与えられた式が有理式の場合は分母の $n-1$ 乗を分母・分子に掛けて、分母の有理化を行っておく。これを、分母・分子別々に根号をとることにすると、同じ数でも GALOIS における代数的数の表現では異なった表現となることがあるので、3 節で述べたような根号の自由な分岐がとれなくなってしまう。

図 1 に実際に GALOIS によって解かれた 1 の原始 7 乗根と原始 13 乗根の結果を示す。この図の値は 5 節で求めたものと見掛け上異なっているが、図の計算では 1 の 3 乗根を代入したあとで計算を行っているために、5 節で計算した根号の中が有理式になる为上で述べた理由によって根号の中を整数係数の多項式にしているためである。

7. 問題点と今後の予定

根号を含む式の簡単化については、根号はどの分岐をとってもよいという条件のもとでは n 乗したものが根号の中の式になるという規則で行うものだけであるが、上の条件を緩

$$W(7) = (4 \sqrt[3]{2} + 3 \sqrt[3]{3} i \sqrt[3]{2} + 3 \sqrt[3]{2} + 28 \sqrt[3]{2} - 56) / 336$$

$$\sqrt[3]{2} = 28 (-3 \sqrt[3]{3} i + 1)$$

$$\sqrt[3]{3} = 21 (-\sqrt[3]{3} i \sqrt[3]{2} + 2 \sqrt[3]{2} + 7 \sqrt[3]{3} i \sqrt[3]{2} - 7 \sqrt[3]{2} - 196)$$

$$W(13) = (2 \sqrt[5]{5} + 4 \sqrt[5]{4} + 3 \sqrt[5]{3} i \sqrt[5]{3}^2 - 5 \sqrt[5]{3}^2 + 52 \sqrt[5]{3} - 104) / 1248$$

$$\sqrt[5]{3} = 52 (-3 \sqrt[5]{3} i - 5)$$

$$\sqrt[5]{4} = 39 (-3 \sqrt[5]{3} i \sqrt[5]{3}^2 - 8 \sqrt[5]{3}^2 - 39 \sqrt[5]{3} i \sqrt[5]{3} + 13 \sqrt[5]{3} + 676)$$

$$\sqrt[5]{5} = 2 (3 \sqrt[5]{3} i \sqrt[5]{3}^2 \sqrt[5]{4} - 5 \sqrt[5]{3}^2 \sqrt[5]{4} + 52 \sqrt[5]{3} \sqrt[5]{4} - 104 \sqrt[5]{4} - 312 \sqrt[5]{3} i \sqrt[5]{3}^2 - 156 \sqrt[5]{3}^2 - 20 \sqrt[5]{3} i \sqrt[5]{3} - 2028 \sqrt[5]{3} - 105456)$$

記号の意味：

$$x^n \text{ は } x^n,$$

$$\sqrt[n]{x} \text{ は } \sqrt[n]{x}, n \mid x \text{ は } \sqrt[n]{x} \text{ を表わす}$$

図 1. GALOIS による 1 の原始 7 乗根と原始 13 乗根

めて、根号の中の数が正の実数の場合には正の実数の分岐をとるようにすることも可能である。また、このようにしないと実数の計算をしているのに、複素数が表われたり、2数の大きさが較べられなくなったりしてしまう。ただし、この場合には根号を含む式の単純化が複雑になる。たとえば次のような単純化がそうである。

$$\sqrt{1+\sqrt{3}} + \sqrt{3+3\sqrt{3}} = \sqrt{10+6\sqrt{3}}$$

根号をとるときにも今までに存在する根号との代数的関係を調べる必要が生じる。このように処理が複雑になるにもかかわらず、上に述べたようなことは必要であるのでGALLOISにおいても実現する予定である。

GALLOISにおいて代数的数の処理プログラムを作成し、その応用として1の原始n乗根を根号によって表わす方法をインプリメントしたが、これを使用して5次以上の代数方程式が根号によって解かれる場合にはそれを求めるプログラムを作成することが次の課題である。またGALLOIS自身も作成中のシステムであり、ユーザとのインターフェースを重視した入出力を中心として開発を行っていく予定である。

8. 参考文献

1. 元吉、佐々木、“数学コンサルタントシステムGALLOISの構想”、情報処理学会第31回全国大会。
2. 元吉、佐々木、“GALにおける代数的数の取り扱いについて”、情報処理学会第28回全国大会。
3. 日野 訳、“ガロアの理論”、東京図書、1964。
4. Gaal、“Classical Galois Theory with Examples”、Chelsea Publishing Company、N. Y.、1971。
5. Borodin他、“Decreasing the Nesting Depth of Expressions Involving Square Roots”、J. Symbolic Computation (1985) 1、169-188。
6. Zippel、“Simplification of Expressions Involving Radicals”、J. Symbolic Computation (1985) 1、189-210。