数理解析研究所講究録
第722巻 1990年 17-20

巡回群をガロア群に持つ5次方程式の判別とその解法

元吉文男 (Fumio Motoyoshi)
(電子技術総合研究所)

表題は正確には、「Q上の5次既約多項式$f \in \mathrm{Q}[x]$のQ上のガロア群が巡回群であることの判定と、その場合にfを代数的に解く方法の数式処理による実現」である。以下の方法は5次に限らず素数次の場合に適用できるが、実際に計算できるかどうかでは、せいぜい7次までであると考える。

§1. ガロア群が巡回群かどうかの判定

fのQ上の最小多項式はfであるのでfの1根をαとしたときにfを$\mathrm{Q}(\alpha)$で因数分解して、根がすべて分離できれば巡回群である。

$f \in \mathrm{Q}[x]$の$\mathrm{Q}(\alpha)$上での因数分解法

1. αの定義多項式をgとする。($g(\alpha) = 0$)
2. $f(x-s\alpha)$と$g(\alpha)$のαに関する終結式$r(x)$を求めるが、このとき$r(x)$が無平方になるようにsを決める。
3. $r(x)$をQ上で因数分解する。
$$r(x) = r_1(x)\ r_2(x)\ \cdots\ r_k(x)$$
4. 各$r_i(x)$と$f(x-s\alpha)$とのGCDをとる。
$$f_i(x) = \mathrm{GCD}(r_i(x), f(x-s\alpha))$$
すると
$$f(x) = f_1(x+s\alpha)\ f_2(x+s\alpha)\ \cdots\ f_k(x+s\alpha)$$
となって因数分解ができる。

ここで$g(\alpha) = f(\alpha)$としたときの各f_iがxについての1次式ならばfのQ上のガロア群は巡回群である。さらにfの$\mathrm{Q}(\omega_5)$上でのガロア群も同じ巡回群になっている。このときαはfの任意の1根であり、他の根$\alpha_i (1 \leq i \leq 4)$は$\alpha$のQ係数多項式として表される。
$$\alpha_i = \theta_i(\alpha)$$

§2. ガロア群が巡回群である5次方程式の解法

上の因数分解によってfの根が任意の1根の多項式として表せたとする。このとき$\alpha_2, \alpha_3, \alpha_4$と$\theta_1^2(\alpha), \theta_1^3(\alpha), \theta_1^4(\alpha)$は全体として一致するので、あらためて$\alpha_i = \theta_1^i(\alpha), (1 \leq i \leq 4)$とし、 $\theta = \theta_1$と書くことにする。このようにするとfの根は$\theta^i(\alpha), (0 \leq i \leq 4)$である。

ここでfを代数的に解くためにラグランジェの方法を使用する。ラグランジェの分解式を次のように定義する:

$$u(\alpha, k) = \alpha+\omega_5^k\theta(\alpha)+\omega_5^{2k}\theta^2(\alpha)+\omega_5^{3k}\theta^3(\alpha)+\omega_5^{4k}\theta^4(\alpha)$$

このときに

$$\theta(u(\alpha, k)) = \omega_5^{-k}u(\alpha, k)$$

である。そこで

$$\theta(u(\alpha, k)\ u(\alpha, 1)^{5-k}) = u(\alpha, k)\ u(\alpha, 1)^{5-k} \qquad (1\leq k\leq 4)$$

となり,$u(\alpha, k)\ u(\alpha, 1)^{5-k} \in \mathrm{Q}(\omega_5)$ であるので、$\sigma_i(\omega_5)$ $(1\leq i\leq 4)$をω_5の多項式として

$$u(\alpha, k)\ u(\alpha, 1)^{5-k} = \sigma_k(\omega_5)$$

と書くことができる。そこで実際に各σ_iを計算して具体的な形を求める。すると各$u(\alpha,k)$は次のように求めることができる:

$$u(\alpha,1) = \sqrt[5]{\sigma_1(\omega_5)}$$

$$u(\alpha,k) = \frac{\sigma_k(\omega_5)\ u(\alpha,1)^k}{\sigma_1(\omega_5)}$$

また

$$u(\alpha,0) = \alpha+\theta(\alpha)+\theta^2(\alpha)+\theta^3(\alpha)+\theta^4(\alpha)$$

であり、これは

$$f(x) = a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$$

としたときの $-a_4/a_5$である。

さらに

$$5\alpha = u(\alpha,0)+u(\alpha,1)+u(\alpha,2)+u(\alpha,3)+u(\alpha,4)$$

という関係を利用すればαの具体的な形が得られる。

§3. 例

$$f(x) = x^5+x^4-4x^3-3x^2+3x+1$$

を解くことにする。αを$f(x) = 0$の根とする。

$f(x)$のQ(α)上での因数分解

αの定義多項式は$f(\alpha)$であり、$f(x)$は$x-\alpha$で割ることができるので次数を1つ落すことができる。

$$h(x,\alpha) = \frac{f(x)}{x-\alpha} = x^4+(\alpha+1)x^3+(\alpha^2+\alpha-4)x^2+(\alpha^3+\alpha^2-4\alpha-3)x+(\alpha^4+\alpha^3-4\alpha^2-3\alpha+3)$$

ここで$h(x+\alpha,\alpha)$と$f(\alpha)$のαに関する終結式を求めると

$$r(x) = x^{20}-44x^{18}+792x^{16}-7623x^{14}+43076x^{12}-147983x^{10}+310123x^8-388652x^6$$
$$+278179x^4-102487x^2+14641$$

となり、これをQで因数分解すると

$$r(x) = (x^5-11x^3+22x+11)(x^5-11x^3+22x-11)(x^5-11x^3-11x^2+11x+11)(x^5-11x^3-11x^2+11x-11)$$

となる。この各因子と$h(x+\alpha,\alpha)$とのGCDを求めることになるが、最初の因子で行なうと、

$$\mathrm{GCD}(h(x+\alpha,\alpha),(x^5-11x^3+22x+11))$$
$$=(105\alpha^4-170\alpha^3-285\alpha^2+216\alpha+80)x+(-404\alpha^4+165\alpha^3+753\alpha^2-314\alpha-144)$$

が得られるがxの係数を1にするためにxの係数の逆数を求めると

$$\frac{1}{(105\alpha^4-170\alpha^3-285\alpha^2+216\alpha+80)}=\frac{143261\alpha^4+96331\alpha^3-599144\alpha^2-237458\alpha+488688}{20339}$$

となり、これを定数項に掛けて次の式を得る。

$$\mathrm{GCD}=x+(-\alpha^4+4\alpha^2+\alpha-2)$$

同様にして各項のGCDを計算して

$$h(x+\alpha,\alpha)=(x-(\alpha^4-4\alpha^2-\alpha+2))(x-(\alpha^3-4\alpha))(x-(\alpha^2-\alpha-2))(x-(-\alpha^4-\alpha^3+3\alpha^2+\alpha-1))$$

となるので

$$f(x)=(x-\alpha)h(x,\alpha)$$
$$=(x-\alpha)(x-(\alpha^4-4\alpha^2+2))(x-(\alpha^3-3\alpha))(x-(\alpha^2-2))(x-(-\alpha^4-\alpha^3+3\alpha^2+2\alpha-1))$$

となって因数分解ができ、fのQでのガロア群が巡回群であることがわかる。

$f(x)$の代数的解法

上の因数分解から

$$\theta(\alpha)=\alpha^2-2$$

とする。これより

$$\theta^2(\alpha)=\alpha^4-4\alpha^2+2$$
$$\theta^3(\alpha)=\alpha^3-3\alpha$$
$$\theta^4(\alpha)=-\alpha^5-\alpha^4+3\alpha^3+2\alpha-1$$

となる。そこで

$$u(\alpha,k)=\alpha+\omega_5^k\theta(\alpha)+\omega_5^{2k}\theta^2(\alpha)+\omega_5^{3k}\theta^3(\alpha)+\omega_5^{4k}\theta^4(\alpha)$$

に代入して各$u(\alpha,k)$を計算すると

$$u(\alpha,0)=-1$$
$$u(\alpha,1)=(\omega_5^3+2\omega_5^2+\omega_5+1)\alpha^4+(2\omega_5^3+\omega_5^2+\omega_5+1)\alpha^3+(-3\omega_5^3-7\omega_5^2-2\omega_5-3)\alpha^2$$
$$+(-5\omega_5^3-2\omega_5^2-2\omega_5-1)\alpha+(\omega_5^3+3\omega_5^2-\omega_5+1)$$
$$u(\alpha,2)=(-2\omega_5^3-\omega_5^2-\omega_5-1)\alpha^4+(-\omega_5^3+\omega_5)\alpha^3+(7\omega_5^3+5\omega_5^2+4\omega_5+4)\alpha^2+(2\omega_5^3-3\omega_5+1)\alpha$$
$$+(-3\omega_5^3-4\omega_5^2-2\omega_5-2)$$
$$u(\alpha,3)=(-\omega_5^2+\omega_5)\alpha^4+(-\omega_5^3-2\omega_5^2-\omega_5-1)\alpha^3+(\omega_5^3+3\omega_5^2-4\omega_5)\alpha^2+(3\omega_5^3+5\omega_5^2+3\omega_5+4)\alpha$$
$$+(-2\omega_5^3-\omega_5^2+2\omega_5)$$
$$u(\alpha,4)=(-\omega_5^3-\omega_5)\alpha^4+(\omega_5^2-\omega_5)\alpha^3+(-5\omega_5^3-\omega_5^2+2\omega_5-1)\alpha^2+(-3\omega_5^2+2\omega_5+1)\alpha+(4\omega_5^3+2\omega_5^2+\omega_5+2)$$

これより各$\sigma_k(\omega_5)=u(\alpha,k)u(\alpha,1)^{5-k}$を計算すると以下のようになる。

$$\sigma_1(\omega_5)=-110\omega_5^3+165\omega_5^2-220\omega_5-286$$
$$\sigma_2(\omega_5)=99\omega_5^3+33\omega_5^2+77-33$$
$$\sigma_3(\omega_5)=-11\omega_5^3-22\omega_5^2+22\omega_5$$

$$\sigma_4(\omega_5) = 11$$

ここで

$$\beta = \sqrt[5]{\sigma_1(\omega_5)} = \sqrt[5]{-110\omega_5^3+165\omega_5^2-220\omega_5-286}$$

と書くことにすると、上の$\sigma_k(\omega_5)$を用いて

$$5\alpha = -1+\beta+\frac{\sigma_2(\omega_5)\beta^2+\sigma_3(\omega_5)\beta^3+\sigma_4(\omega_5)\beta^4}{\sigma_1(\omega_5)}$$

$$= -1+\beta+\frac{(-4\omega_5^3-3\omega_5^2-2\omega_5-2)}{11}\beta^2+\frac{(-4\omega_5^3+2\omega_5^2-7\omega_5-10)}{121}\beta^3+\frac{(35\omega_5^3+10\omega_5^2+20\omega_5-6)}{1331}\beta^4$$

となって根が求まる。なおω_5は1の原始5乗根であり、

$$\omega_5^4+\omega_5^3+\omega_5^2+\omega_5+1 = 0$$

を満たすのでこれより、

$$\omega_5 = -\frac{\sqrt{2\sqrt{5}-10}+\sqrt{5}+1}{4}$$

である。(実はαはω_{11}を1の原始n乗根として

$$\alpha = \omega_{11}+\omega_{11}^{10}$$

と表すことができる。)

§4．5次既約方程式の代数的可解性の判定

素数次既約方程式が代数的に可解であることの必要十分条件は、その任意の2根によって根が分離できることであるので、これを利用して可解性の判定を行なうことができる。

§1において因数分解を行なった際に、$r_i(x)$のうちに次数が5次より大きいものがあるときには、ガロア群が巡回群ではなかったが、その式は $Q(\alpha)$にfのα以外の根を添加した体の最小多項式になっている。そこで、fの因数分解で分離できなかった式を、この新しい体で因数分解してみて、すべての根が分離できれば、fは代数的に可解であることがわかる。

この計算は最悪の場合には、60次の整数係数多項式の整数上での因数分解になるが、計算機で実行可能かどうかはまだ試していない。ガロア群がZ_5を核とするZ_2の群拡大の場合には、20次の式の因数分解なので十分に計算可能であるので現在プログラム中である。