5次方程式の代数解の不可能性 by Abel

能美武功

平成 12 年 5 月 28 日

1　多項式の変数に置換を施す

「3 次方程式の解法」において、対称式を (，，) として扱った。
対称式とは、変数をどのように入れ換えても元の式と同じものになる式をいう、のであるが、その扱いを行儀正しくすると、以下のようにかなり面倒である。

問 1. 3 変数の時、$(1,0,0) = x_1 + x_2 + x_3$
が対称式であることを示せ。
解
1. x_1と x_2を入れ換える。$x_2 + x_1 + x_3 = (1,0,0)$ となり変らない。
2. x_1と x_3を入れ換える。$x_3 + x_2 + x_1 = (1,0,0)$ となり変らない。
3. x_2と x_3を入れ換える。$x_1 + x_3 + x_2 = (1,0,0)$ となり変らない。
4. x_1と x_2を、x_2と x_3を、x_3と x_1を入れ換える。$x_2 + x_3 + x_1 = (1,0,0)$ となり変らない。
5. x_1と x_3を、x_3と x_2を、x_2と x_1を入れ換える。$x_3 + x_1 + x_2 = (1,0,0)$ となり変らない。（解おわり）

定義 1. 上において、
1 の入れ換えを *(1,2)* と書き、
2 の入れ換えを *(1,3)* と書き、
3 の入れ換えを *(2,3)* と書き、
4 の入れ換えを *(1,2,3)* と書き、
5 の入れ換えを *(1,3,2)* と書くことにする。
またついでに入れ換えなしにも記号 *(1)* を定義しておく。
上記 *6* 個の「入れ換え」を *(3* 次の*)* 置換という。

問 2. *4* 次の置換を全て作れ。
解　*4* 個のものの順列は *24* 通りあるから、*24* 個ある筈。

1. 1234 をこの順序に *1234* にする。つまり入れ換えないということ。これは *(1)* 。
2. 1234 をこの順序に *1243* にする。つまり *3* を *4* に、*4* を *3* に。これは *(3,4)* 。
3. 1234 をこの順序に *1324* にする。つまり *2* を *3* に、*3* を *2* に。これは *(2,3)* 。
4. 1234 をこの順序に *1342* にする。つまり *2* を *3* に、*3* を *4* に、*4* を *2* に。これは *(2,3,4)* 。
5. 1234 をこの順序に *1423* にする。つまり *2* を *4* に、*4* を *3* に、*3* を *2* に。これは *(2,4,3)* 。
6. 1234 をこの順序に *1432* にする。つまり *2* を *4* に、*4* を *2* に。これは *(2,4)* 。
7. 1234 をこの順序に *2134* にする。これは *(1,2)* 。
8. 1234 をこの順序に *2143* にする。これは *(1,2)(3,4)* 。
9. 1234 をこの順序に *2314* にする。これは *(1,2,3)* 。
10. 1234 をこの順序に *2341* にする。これは *(1,2,3,4)* 。
11. 1234 をこの順序に *2413* にする。これは *(1,2,4,3)* 。
12. 1234 をこの順序に *2431* にする。これは *(1,2,4)* 。
13. 1234 をこの順序に *3124* にする。これは *(1,3,2)* 。
14. 1234 をこの順序に *3142* にする。これは *(1,3,4,2)* 。
15. 1234 をこの順序に *3214* にする。これは *(1,3)* 。
16. 1234 をこの順序に *3241* にする。これは *(1,3,4)* 。
17. 1234 をこの順序に *3412* にする。これは *(1,3)(2,4)* 。
18. 1234 をこの順序に *3421* にする。これは *(1,3,2,4)* 。
19. 1234 をこの順序に *4123* にする。これは *(1,4,3,2)* 。
20. 1234 をこの順序に *4132* にする。これは *(1,4,2)* 。
21. 1234 をこの順序に *4213* にする。これは *(1,4,3)* 。
22. 1234 をこの順序に *4231* にする。これは *(1,4)* 。
23. 1234 をこの順序に *4312* にする。これは *(1,4,2,3)* 。
24. 1234 をこの順序に *4321* にする。これは *(1,4)(2,3)* 。
の *24* 個。　（解おわり）

多項式の変数に置換を施すとき、その多項式の左側に置換を書くことにする。例えば、
$(1,2)(x_1^2+x_2)=x_2^2+x_1$
或いは、$x_1^2+x_2=f(x_1,x_2)$ とおいて、
$(1,2)f=x_2^2+x_1$
と書いたりする。

問 3. $f=x_1^2+x_2-x_3$に $(1,2)$ を施したあと、$(1,3)$ を施したものは、
f に $(1,2,3)$ を施したものに等しいことを説明せよ。

解　$(1,2)f = x_2^2 + x_1 - x_3$
　　$(1,3)[(1,2)f] = x_2^2 + x_3 - x_1$
一方 $(1,2,3)f = x_2^2 + x_3 - x_1$　より。（解おわり）

　上の問から置換同志のかけ算が定義される。即ち上の例を使えば、
　(1,3)(1,2)=(1,2,3)
となる。（計算のやり方は常に右から左と考えること。）

問 4.　*(1,3)(1,2)* が *(1,2,3)* になることを f を使わずに説明せよ。
解
まず、*1* はどこに行くか。
　(1,2) により、*1* は *2* に行く。次に *2* は *(1,3)* によって動かない。
　故に *1* は *2* に行く。
次に、*2* はどこに行くか。
　(1,2) により、*2* は *1* に行く。次に *1* は *(1,3)* によって *3* に行く。
　故に *2* は *3* に行く。
次に、*3* はどこに行くか。
　(1,2) により、*3* は動かない。次に *3* は *(1,3)* によって *1* に行く。
　故に *3* は *1* に行く。
従って、答は *(1,2,3)*　（解おわり）

問 5. 2 変数の時、単項式、$f = x_1^2 x_2$から、$(2,1)$ 型の対称式を作れ。
解　$(1)f + (1,2)f$ を作ると、これは対称式。かつ求めるものとなる。
この式が 2 次の全ての置換によ っ て変らないことを言えばよい。
2 次の置換は (1) と $(1,2)$。(1) によ っ て変らないことは自明。
$(1,2)$ によ っ て変らないことを言う。
$\because$　$(1,2)[(1)f + (1,2)f] = (1,2)f + (1)f = (1)f + (1,2)f$ より。
実際にこれを作ると、
$(1)f + (1,2)f = x_1^2 x_2 + x_2^2 x_1$　（解おわり）

問 6. 3 変数の時、単項式、$f = x_1^2 x_2$から、$(2,1,0)$ 型の対称式を作れ。
解　$(1)f + (1,2)f + (1,3)f + (2,3)f + (1,2,3)f + (1,3,2)f$　を作ると、これは対称式。
かつ求めるものとなる。
この式が 3 次の全ての置換によ っ て変らないことを言えばよい。
3 次の置換は $(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)$ の 6 個。(1) によ っ て変らないことは自明。
$(1,2)$ によ っ て変らないことを言う。

$\because \quad (1,2)[(1)f+(1,2)f+(1,3)f+(2,3)f+(1,2,3)f+(1,3,2)f] = (1,2)f+(1)f+(1,3,2)f+(1,2,3)f+(2,3)f+(1,3)f$ より。
$(1,3)$ によって変らないことを言う。
$\because \quad (1,3)[(1)f+(1,2)f+(1,3)f+(2,3)f+(1,2,3)f+(1,3,2)f] = (1,3)f+(1,2,3)f+(1)f+(1,3,2)f+(1,2)f+(2,3)f$ より。
$(2,3)$ によって変らないことを言う。
$\because \quad (2,3)[(1)f+(1,2)f+(1,3)f+(2,3)f+(1,2,3)f+(1,3,2)f] = (2,3)f+(1,3,2)f+(1,2,3)f+(1)f+(1,3)f+(1,2)f$ より。
$(1,2,3)$ によって変らないことを言う。
$\because \quad (1,2,3)[(1)f+(1,2)f+(1,3)f+(2,3)f+(1,2,3)f+(1,3,2)f] = (1,2,3)f+(1,3)f+(2,3)f+(1,2)f+(1,3,2)f+(1)f$ より。
$(1,3,2)$ によって変らないことを言う。
$\because \quad (1,3,2)[(1)f+(1,2)f+(1,3)f+(2,3)f+(1,2,3)f+(1,3,2)f] = (1,3,2)f+(2,3)f+(1,2)f+(1,3)f+(1)f+(1,2,3)f$ より。実際にこれを作ると、
$x_1^2x_2+x_2^2x_1+x_3^2x_2+x_1^2x_3+x_2^2x_3+x_3^2x_1$ （解おわり）

問 7. 3 変数の時、単項式、$f = x_1x_2x_3$から、$(1,1,1)$ 型の対称式を作れ。
解　f は既に対称式であるが、前問のやり方でも出来ることを見てみる。
$(1)f+(1,2)f+(1,3)f+(2,3)f+(1,2,3)f+(1,3,2)f$ を作ると、これは前問でや っ たように対称式。
実際にこれを作ると、
$x_1x_2x_3+x_2x_1x_3+x_3x_2x_1+x_1x_3x_2+x_2x_3x_1+x_3x_1x_2 = 6x_1x_2x_3$
6 は無駄なので係数を 1 として、$x_1x_2x_3$ （解おわり）

多項式の集合と置換に関する次の定義をしておく。

定義 2. ある多項式の集合 F が与えられている。このとき、その集合に属するどの多項式も変化させない置換の集合 S を「F に対応する置換の集合」という。

問 8. 2 変数の時、
$F_1^2 = \{-b/a = x_1+x_2, c/a = x_1x_2\}$ が与えられているとき、
F_1^2に対応する置換の集合 S_1^2を求めよ。
解　$S_1^2 = \{(1),(1,2)\}$ （解おわり）

2 次方程式を解くとき、どんなに $-b/a$ と a/c に 4 則 $(+,-,\times,\div)$ を施しても根は作れない。そこで、$\sqrt{(-b/a)^2-4(a/c)} = x_1-x_2$を作るのであ っ た

。

問 9. 2 変数の時、
$F_2^2 = \{-b/a = x_1 + x_2, c/a = x_1x_2, x_1 - x_2\}$ が与えられているとき、
F_2^2に対応する置換の集合 S_2^2を求めよ。
解　今度は $x_1 - x_2$があり、$(1,2)$ はこれを変えてしまうから駄目。
$\therefore \quad S_2^2 = \{(1)\}$　（解おわり）

問 10. 3 変数の時、
$F_1^3 = \{-a_1 = x_1 + x_2 + x_3, a_2 = x_1x_2 + x_1x_3 + x_2x_3, -a_3 = x_1x_2x_3\}$ が与えられているとき、F_1^3に対応する置換の集合 S_1^3を求めよ。
解　$S_1^3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$　（解おわり）

3 次方程式を解くとき、どんなに a_1, a_2, a_3に 4 則 $(+, -, \times, \div)$ を施しても根は作れない。そこで、$\sqrt{-27D} = \sqrt{-27}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ を作るのであ っ た。

問 11. 3 変数の時、
$F_2^3 = \{-a_1 = x_1+x_2+x_3, a_2 = x_1x_2+x_1x_3+x_2x_3, -a_3 = x_1x_2x_3, \sqrt{-27D} = \sqrt{-27}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\}$ が与えられているとき、F_2^3に対応する置換の集合 S_2^3を求めよ。
解　$(1,2)\sqrt{-27D} = \sqrt{-27}(x_2 - x_1)(x_2 - x_3)(x_1 - x_3)\}$
$= -\sqrt{-27}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\} = -\sqrt{-27D}$　で、$(1,2)$ は駄目。
$(1,3)\sqrt{-27D} = \sqrt{-27}(x_3 - x_2)(x_3 - x_1)(x_2 - x_1)\}$
$= -\sqrt{-27}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\} = -\sqrt{-27D}$　で、$(1,3)$ は駄目。
$(2,3)\sqrt{-27D} = \sqrt{-27}(x_1 - x_3)(x_1 - x_2)(x_1 - x_2)\}$
$= -\sqrt{-27}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\} = -\sqrt{-27D}$　で、$(2,3)$ は駄目。
$(1,2,3)\sqrt{-27D} = \sqrt{-27}(x_2 - x_3)(x_2 - x_1)(x_3 - x_1)\}$
$= \sqrt{-27}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\} = \sqrt{-27D}$　で、$(1,2,3)$ は大丈夫。
$(1,3,2)\sqrt{-27D} = \sqrt{-27}(x_3 - x_1)(x_3 - x_2)(x_1 - x_2)\}$
$= \sqrt{-27}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\} = \sqrt{-27D}$　で、$(1,3,2)$ は大丈夫。
$\therefore \quad S_2^3 = \{(1), (1,2,3), (1,3,2)\}$　（解おわり）

上と同じ問題であるが、次の観点から見てみる。何故$\sqrt{-27D}$を作 っ たかというと、
$u = x_1 + \omega x_2 + \omega^2 x_3$
$v = x_1 + \omega^2 x_2 + \omega x_3$

と置いて、u^3+v^3が幸運にも a_1,a_2,a_3で表され、u^3-v^3が a_1,a_2,a_3を 4 則だけで計算することは出来なか っ たが、2 乗根を使えば$\sqrt{-27D}$として表されるのであ っ た。
そこで上の問題を次のように変形して解いてみる。

問 12. 3 変数の時、
$F_2^3=\{-a_1=x_1+x_2+x_3, a_2=x_1x_2+x_1x_3+x_2x_3, -a_3=x_1x_2x_3,$
$u^3+v^3, u^3-v^3\}$ が与えられているとき、F_2^3に対応する置換の集合 S_2^3を求めよ。
解　u^3+v^3は a_1,a_2,a_3で表されているのだから、どの 3 次の置換によ っ ても変らない。
1)　さて、$(1,2)[u^3-v^3]$ を計算する。最初に $(1,2)u^3$を計算する。
$(x_1+\omega x_2+\omega^2x_3)^3$を計算してから x_1と x_2を交換するのは、最初からこれを交換しておいて $(x_2+\omega x_1+\omega^2x_3)^3$を計算するのと同じことだから、
$(1,2)u^3=(x_2+\omega x_1+\omega^2x_3)^3$
$=(\omega^3x_2+\omega x_1+\omega^2x_3)^3$
$=[\omega((x_1+\omega^2x_2+\omega x_3)]^3=v^3$
次に $(1,2)v^3$を計算する。
$(1,2)v^3=(x_2+\omega^2x_1+\omega x_3)^3$
$=(\omega^3x_2+\omega^2x_1+\omega^4x_3)^3$
$=[\omega^2((x_1+\omega x_2+\omega^2x_3)]^3=u^3$
$\therefore\quad (1,2)[u^3-v^3]=v^3-u^3=-[u^3-v^3]$
即ち $(1,2)$ は $[u^3-v^3]$ を変える。
2)　次に、$(1,3)[u^3-v^3]$ を計算する。最初に $(1,3)u^3$を計算する。
$(1,3)u^3=(x_3+\omega x_2+\omega^2x_1)^3$
$=(\omega^3x_3+\omega^4x_2+\omega^2x_1)^3$
$=[\omega^2((x_1+\omega^2x_2+\omega x_3)]^3=v^3$
次に $(1,3)v^3$を計算する。
$(1,3)v^3=(x_3+\omega^2x_2+\omega x_1)^3$
$=(\omega^3x_3+\omega^2x_2+\omega x_1)^3$
$=[\omega((x_1+\omega x_2+\omega^2x_3)]^3=u^3$
$\therefore\quad (1,3)[u^3-v^3]=v^3-u^3=-[u^3-v^3]$
即ち $(1,3)$ は $[u^3-v^3]$ を変える。
3)　次に、$(2,3)[u^3-v^3]$ を計算する。最初に $(2,3)u^3$を計算する。
$(2,3)u^3=(x_1+\omega x_3+\omega^2x_2)^3=v^3$
次に $(2,3)v^3$を計算する。
$(2,3)v^3=(x_1+\omega^2x_3+\omega x_2)^3=u^3$
$\therefore\quad (2,3)[u^3-v^3]=v^3-u^3=-[u^3-v^3]$
即ち $(2,3)$ は $[u^3-v^3]$ を変える。

4)　次に、$(1,2,3)[u^3-v^3]$ を計算する。最初に $(1,2,3)u^3$を計算する。

$(1,2,3)u^3 = (x_2+\omega x_3+\omega^2 x_1)^3$

$= (\omega^3 x_2+\omega^4 x_3+\omega^2 x_1)^3$

$= [\omega^2((x_1+\omega x_2+\omega^2 x_3)]^3 = u^3$

次に $(1,2,3)v^3$を計算する。

$(1,2,3)v^3 = (x_2+\omega^2 x_3+\omega x_1)^3$

$= (\omega^3 x_2+\omega^2 x_3+\omega x_1)^3$

$= [\omega((x_1+\omega^2 x_2+\omega x_3)]^3 = v^3$

$\therefore \quad (1,2,3)[u^3-v^3] = [u^3-v^3]$

即ち $(1,2,3)$ は $[u^3-v^3]$ を変えない。

5)　次に、$(1,3,2)[u^3-v^3]$ を計算する。最初に $(1,3,2)u^3$を計算する。

$(1,3,2)u^3 = (x_3+\omega x_1+\omega^2 x_2)^3$

$= (\omega^3 x_2+\omega^4 x_3+\omega^2 x_1)^3$

$= [\omega^2((x_1+\omega x_2+\omega^2 x_3)]^3 = u^3$

次に $(1,3,2)v^3$を計算する。

$(1,3,2)v^3 = (x_3+\omega^2 x_1+\omega x_2)^3$

$= (\omega^3 x_3+\omega^2 x_1+\omega^4 x_2)^3$

$= [\omega^2((x_1+\omega^2 x_2+\omega x_3)]^3 = v^3$

$\therefore \quad (1,3,2)[u^3-v^3] = [u^3-v^3]$

即ち $(1,3,2)$ は $[u^3-v^3]$ を変えない。

$\therefore \quad S_2^3 = \{(1),(1,2,3),(1,3,2)\}$　（解おわり）

さて、次に u^3の 3 乗根 u を求めるのであ っ た。数値計算ではここで v^3 の 3 乗根も求めるのであるが、数学的には 3 乗根の計算は 1 回だけ行えば足りる。何故なら、uv が a_1,a_2,a_3で表されるから、$v=(uv)/u$ として 4 則を用いて計算できるからである。

実際に uv を a_1,a_2,a_3で表してみる。それは簡単で、

$uv = x_1^2+x_2^2+x_3^2-x_1x_2-x_1x_3-x_2x_3$

$= (x_1+x_2+x_3)^2-3(x_1x_2+x_1x_3+x_2x_3) = a_1^2-3a_2$

従 っ て F_2^3に u を付け加えて、4 則演算を許したものを F_3^3とすれば、F_3^3は、

$-a_1 = x_1+x_2+x_3$

$u = x_1+\omega x_2+\omega^2 x_3$

$v = x_1+\omega^2 x_2+\omega x_3$

を含むことになり、x_1,x_2,x_3を含むことになる。即ち、次の問題は、

問 13. 3 変数の時、

$F_3^3 = \{-a_1 = x_1+x_2+x_3, a_2 = x_1x_2+x_1x_3+x_2x_3, -a_3 = x_1x_2x_3,$

$u^3+v^3, u^3-v^3, u, v, x_1, x_2, x_3\}$ が与えられているとき、

F_3^3に対応する置換の集合 S_3^3を求めよ。

解　x_1があり、$(1,2,3)$ はこれを x_2に変えてしまうから駄目。また $(1,3,2)$ もこれを x_3に変えてしまうから駄目。
$\therefore \quad S_3^3 = \{(1)\}$　（解おわり）

上の議論の中で、「どんなに a_1, a_2, a_3に 4 則（$+, -, \times, \div$) を施しても」という言葉が出てきた。体という概念があって、これを次に定義する。

定義 3.（数または記号の）集合 R が与えられたとき、
その Rが体であるとは、Rの任意の二つの元に 4 則を施してもRの元になっている、ことを言う。

問 14. $\sqrt{2}$を含む（最小の）体 $R(\sqrt{2})$ とはどういうものか。説明せよ。
解　$\sqrt{2} - \sqrt{2} = 0$　だから、$R(\sqrt{2})$ は 0 を含む。
$\sqrt{2}/\sqrt{2} = 1$　だから、$R(\sqrt{2})$ は 1 を含む。
足し算、引き算を実行して、全ての整数を含む。
割り算を実行して、全ての有理数を含む。
任意の 2 つの有理数を p, q (正、負あり）として、$p + q\sqrt{2}$を含む。
r, s を有理数として、割り算$\dfrac{p + q\sqrt{2}}{r + s\sqrt{2}}$を実行しても再び $p + q\sqrt{2}$の形になることは既知。
また、p, q がどんな有理数であっても 1 から出発して 4 則を繰り返して、作ることが出来るから、結局、
$R(\sqrt{2})$ とは (p, q を任意の有理数として) $p + q\sqrt{2}$の集まりである。集合の記号を使えば、
$$R(\sqrt{2}) = \{p + q\sqrt{2}; \quad (p, q : \text{有理数})\}$$　（解おわり）

問 15. 記号 x を含む（最小の）体 $R(x)$ とはどういうものか。説明せよ。
解　$x - x = 0$　だから、$R(x)$ は 0 を含む。
$x/x = 1$　だから、$R(x)$ は 1 を含む。
足し算、引き算を実行して、全ての整数を含む。
割り算を実行して、全ての有理数を含む。
任意の $(n+1)$ 個の有理数を $p_0, p_1, p_2 ... p_{n+1}$として、$p_0 + p_1 x + p_2 x^2 + ... + p_n x^n$ を含む。
$q_0, q_1, q_2 ... q_{m+1}$を有理数として、割り算による商$\dfrac{p_0 + p_1 x + p_2 x^2 + ... + p_{n+1} x^n}{q_0 + q_1 x + q_2 x^2 + ... + q_{m+1} x^m}$ も含む。
結局、
$R(x)$ とは有理数を係数とする x の有理式全体である。
集合の記号を使えば、
$$R(x) = \left\{ \frac{p_0 + p_1 x + p_2 x^2 + ... + p_{n+1} x^n}{q_0 + q_1 x + q_2 x^2 + ... + q_{m+1} x^m}; \quad (p_i, q_j : \text{有理数}) \right\}$$

（解おわり）

（註　x, y から出来る体、$R(x, y)$ が有理数を係数とする x と y の有理式全体である、ことも分かる。）

この体という言葉を使 っ て、2 次方程式の解法を振り返 っ てみると、
まず原方程式$\big(ax^2 + bx + c = 0$ を a で割 っ て$\big)x^2 + (b/a)x + (c/a) = 0$ の係数、$(b/a), (c/a)$ から出来る体 $R\big((b/a), (c/a)\big)$の中に根がないかと捜す。ない。それで、
これに$\sqrt{(b/a)^2 - 4(c/a)}$を添加した体 $R\big((b/a), (c/a), \sqrt{(b/a)^2 - 4(c/a)}\big)$を作る。
(この操作を「体の拡大」という)
この中には x_1, x_2が含まれている。即ち、「根号によって解けた」ことになる。
記号、$(b/a), (c/a)$ を使わずに、x_1, x_2を使うと、次のようになる。
まず原方程式 $(ax^2+bx+c = 0$ を a で割って、$x^2-(x_1, +x_2)x+(x_1x_2) = 0)$ の係数、$-(x_1, +x_2), (x_1x_2)$ から出来る体 $R(-(x_1 + x_2), (x_1x_2))$ の中に根がないかと捜す。ない。それで、
これに $(x_1 - x_2)$ を添加した体 $R(-(x_1 + x_2), (x_1x_2), (x_1 - x_2))$ を作る。
この中には x_1, x_2が含まれている。即ち、「根号によって解けた」ことになる。
定義（**??**）は、
ある多項式の集合 F が与えられている。このとき、その集合に属するどの多項式も変化させない置換の集合 S を「F に対応する置換の集合」という。
であったが、体を定義したので、この定義を次のように変える。

定義 4. 体 R が与えられている。このとき、R に属するどの有理式も変化させない置換の集合 S を「体 R に対応する置換の集合」という。

すると、2 次方程式の解法は次のように書ける。
体 $R_1 = R(-(x_1 + x_2), (x_1x_2))$ の中に根がないかと捜す。ない。
体 R_1に対応する置換の集合 S_1^2は、$\{(1), (1, 2)\}$

体 R_1を拡大した体 $R_2 = R_1((x_1 - x_2)) = R_1(\sqrt{(b/a)^2 - 4(c/a)})$ の中に根がないかと捜す。ある。
体 R_2に対応する置換の集合 S_2^2は、$\{(1)\}$

また、3 次方程式の解法は次のように書ける。
体 $R_1 = R(-(x_1 + x_2 + x_3), (x_1x_2 + x_1x_3 + x_2x_3), (x_1x_2x_3))$ の中に根がないかと捜す。ない。

体 R_1に対応する置換の集合 S_1^3は、$\{(1),(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}$

体 R_1を拡大した体 $R_2 = R_1((u^3 - v^3)) = R_1(\sqrt{-27D})$
$= R_1(\sqrt{-27}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3))$ の中に根がないかと捜す。ない。
体 R_2に対応する置換の集合 S_2^3は、$\{(1),(1,2,3),(1,3,2)\}$

体 R_2を拡大した体 $R_3 = R_2(u) = R_2(x_1 + \omega x_2 + \omega^2 x_3)$
$= R_2(\sqrt[3]{u^3})$ の中に根がないかと捜す。ある。
体 R_3に対応する置換の集合 S_3^3は、$\{(1)\}$

次に 4 次方程式の解法を振り返 っ てみる。
$u_1 = x_1 + x_2 - x_3 - x_4$
$u_2 = x_1 - x_2 + x_3 - x_4$
$u_3 = x_1 - x_2 - x_3 + x_4$
とおいて、分解方程式
$y^3 - Ay^2 + By - C^2 = 0$ （A, B, C は原方程式の係数でかけている。）
の根は u_1^2, u_2^2, u_1^2となる。
これらを開平すると、u_1, u_2, u_3が出て、次に x_1, x_2, x_3, x_4が解ける。
これを体の拡大により解釈すると、
最初は、$R_1 = R(-a, b, -c, d)$
ここで、$-a, b, -c, d$ は原方程式の係数。
$-a = x_1 + x_2 + x_3 + x_4$
$b = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$
$-c = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$
$d = x_1x_2x_3x_4$
$\therefore$ $(R_1$に対応する $S_1^4) = 4$ 次の置換全部。
最初の拡大は、まず 3 次の分解方程式を解くのだから 3 根、u_1^2, u_2^2, u_1^2の判別式を添加。即ち、
$R_2 = R_1(\sqrt{-27}(u_1^2 - u_2^2)(u_1^2 - u_3^2)(u_2^2 - u_3^2))$
$= R_1(\sqrt{-27}(u_1 - u_2)(u_1 + u_2)(u_1 - u_3)(u_1 + u_3)(u_2 - u_3)(u_2 + u_3))$
$= R_1(\sqrt{-27})2^6(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4))$
体 R_2に対応する置換の集合 S_2^4は、$\{(1),(1,2,3),(1,2,4),(1,3,4),(2,3,4),$
$(1,3,2),(1,4,2),(1,4,3),(2,4,3),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$
次の拡大は 3 次方程式を解くための u の添加。即ちこの場合は、
$u = u_1^2 + \omega u_2^2 + \omega^2 u_3^2$
であるから、
$R_3 = R_2(u_1^2 + \omega u_2^2 + \omega^2 u_3^2)$
体 R_3に対応する置換の集合 S_3^4を求める。
まず $(1,2,3)(u_1^2 + \omega u_2^2 + \omega^2 u_3^2)$ を計算する。

$(1,2,3)(u_1^2) = ((1,2,3)u_1)^2 = (x_2+x_3-x_1-x_4)^2 = u_3^2$
$(1,2,3)(u_2^2) = ((1,2,3)u_2)^2 = (x_2-x_3+x_1-x_4)^2 = u_1^2$
$(1,2,3)(u_3^2) = ((1,2,3)u_3)^2 = (x_2-x_3-x_1+x_4)^2 = u_2^2$
$\therefore \quad (1,2,3)(u_1^2+\omega u_2^2+\omega^2 u_3^2) = u_3^2+\omega u_1^2+\omega^2 u_2^2 = \omega(u_1^2+\omega u_2^2+\omega^2 u_3^2) = \omega u$
即ち、変 っ てしまう。$(1,2,3)$ は、体 R_3に対応する置換の集合 S_3^4の元ではない。
同様の計算により、
$(1,2,4)u = \omega^2 u$
$(1,3,4)u = \omega u$
$(2,3,4)u = \omega^2 u$
$(1,3,2)u = \omega^2 u$
$(1,4,2)u = \omega u$
$(1,4,3)u = \omega^2 u$
$(2,4,3)u = \omega u$
より、3 個の数字からなる巡回置換は S_3^4の元ではない。
次に $(1,2)(3,4)(u_1^2+\omega u_2^2+\omega^2 u_3^2)$ を計算する。
$(1,2)(3,4)u_1^2 = (x_2+x_1-x_4-x_3)^2 = u_1^2$
$(1,2)(3,4)u_2^2 = (x_2-x_1+x_4-x_3)^2 = u_2^2$
$(1,2)(3,4)u_3^2 = (x_2-x_1-x_4+x_3)^2 = u_3^2$
即ち、変らない。$(1,2)(3,4)$ は、体 R_3に対応する置換の集合 S_3^4の元である。
同様の計算により、$(1,3)(2,4), (1,4)(2,3)$ も S_3の元である。
$\therefore$ 体 R_3に対応する置換の集合 $S_3 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$
次の拡大は u_1^2を開いたものを添加すること。即ち、
$R_4 = R_3(u_1) = R((x_1+x_2-x_3-x_4))$
体 R_4に対応する置換の集合 S_4を求める。
$(1,2)(3,4)u_1 = x_2+x_1-x_4-x_3 = u_1$ 即ち $(1,2)(3,4)$ は S_4^4の元。
$(1,3)(2,4)u_1 = x_3+x_4-x_1-x_2 = -u_1$ 即ち $(1,3)(2,4)$ は S_4^4の元ではない。
$(1,4)(2,3)u_1 = x_4+x_3-x_2-x_1 = -u_1$ 即ち $(1,4)(2,3)$ は S_4^4の元ではない。
$\therefore$ 体 R_4に対応する置換の集合 $S_4^4 = \{(1), (1,2)(3,4)\}$
次の拡大は u_2を開いたものを添加すること。即ち、
$R_5 = R_4(u_2) = R((x_1-x_2+x_3-x_4))$
体 R_5に対応する置換の集合 S_5^4を求める。
$(1,2)(3,4)u_2 = x_2-x_1+x_4-x_3 = -u_2$ 即ち $(1,2)(3,4)$ は S_5^4の元ではない。
$\therefore$ 体 R_5に対応する置換の集合 $S_5^4 = \{(1)\}$
註 一見、u_3^2をも開平する必要があるように思われるが、これは不要。
何故なら、$C = u_1u_2u_3$は既に R_1に入っていて、u_1と u_2が R_5に入ってい

るのだから、$u_3 = C/(u_1u_2)$ は R_5に入っている。

2 「重要な仮定」以降の証明

2 次方程式の体の拡大と、それに対応する置換の集合の縮小を図にすると、

$R \subset R(\sqrt{D})$

$S_2 \supset \{(1)\}$

3 次方程式の体の拡大とそれに対応する置換の集合の縮小を図にすると、

$$R \subset R(\sqrt{-27D}) \subset R\left(\sqrt{-27D}, \sqrt[3]{\frac{A+\sqrt{-27D}}{2}}\right)$$

$S_3 \supset \{(1),(1,2,3),(1,3,2)\} \supset \{(1)\}$

4 次方程式の体の拡大とそれに対応する置換の集合の縮小を図にすると、

$$R \subset R(\sqrt{-27D'}) \subset R\left(\sqrt{-27D'}, \sqrt[3]{\frac{A+\sqrt{-27D'}}{2}}\right)$$

$$\subset R\left(\sqrt{-27D'}, \sqrt[3]{\frac{A+\sqrt{-27D'}}{2}}, u_1\right) \subset R\left(\sqrt{-27D'}, \sqrt[3]{\frac{A+\sqrt{-27D'}}{2}}, u_1, u_2\right)$$

$S_4 \supset \{(1),(1,2,3),(1,3,2),(1,2,4),(1,4,2),(1,3,4),(1,4,3),(2,3,4),$
$(2,4,3),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$
$\supset \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$
$\supset \{(1),(1,2)(3,4)\} \supset \{(1)\}$ とな っ ている。

ここで、添加する根号を調べると、

2 次方程式のとき、$\sqrt{D} = x_1 - x_2$

3 次方程式のとき、$\sqrt{-27D} = \sqrt{-27}(x_1-x_2)(x_1-x_3)(x_2-x_3)$

$$\sqrt[3]{\frac{A+\sqrt{-27D}}{2}} = x_1 + \omega x_2 + \omega^2 x_3$$

4 次方程式のとき、$\sqrt{-27D'} = \sqrt{-27}(x_1-x_2)(x_1-x_3)(x_1-x_4)$
$\times (x_2-x_3)(x_2-x_4)(x_3-x_4)$

$$\sqrt[3]{\frac{A+\sqrt{-27D'}}{2}} = u_1 + \omega u_2 + \omega^2 u_3$$

$$= (x_1+x_2-x_3-x_4)^2 + \omega(x_1-x_2+x_3-x_4)^2 + \omega^2(x_1-x_2-x_3+x_4)^2$$

$u_1 = x_1 + x_2 - x_3 - x_4$

$u_2 = x_1 - x_2 + x_3 - x_4$

といずれも根の有理式（実際は多項式）で書けている。

そこで、次の「重要な仮定」をおく。（これは第 3 節で証明する。）

定理 1. （重要な仮定）方程式が根号によって解けたと仮定すると、各段階の体の拡大において添加すべき根号は、根の有理式になっている。

次のことは当然のことであるが、念のため書いておく。

「根号内の式は、その一つ前の体の元からなる有理式である。」

この仮定が証明されたものとすると、後は比較的容易に 5 次方程式が根号によって解けないことが示される。

まず、上の 3 例で、いずれも最初は平方根の添加、次の 2 例から、2 番目に添加するものは 3 乗根であることが見てとれる。実はこれは証明出来る事柄なのである。まずこれを示す。

定理 2. 体の拡大はまず平方根から始まる。

証明　与えられた方程式を 5 次方程式とし、簡単のために、符号を次のようにする。

$$x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 = 0$$

根と係数の関係から、$a_i(i = 1, 2, 3, 4, 5)$ が基本対称式、$(1, 0, 0, 0, 0), (1, 1, 0, 0, 0), (1, 1, 1, 0, 0), (1, 1, 1, 1, 0), (1, 1, 1, 1, 1)$, になることは分かるであろう。

a_1, a_2, a_3, a_4, a_5からなる体を R_1とおく。

さて、R_1に添加すべき冪根を $\sqrt[p]{r}$とすれば、（$p = 2$ であることを示すのが目標である。）

「重要な仮定」により、

$\sqrt[p]{r}$は、根、x_1, x_2, x_3, x_4, x_5の有理式。これを、$\phi(x_1, x_2, x_3, x_4, x_5)$ とおく。即ち、

$$\sqrt[p]{r} = \phi(x_1, x_2, x_3, x_4, x_5)$$

根号内の式 r は勿論、その一つ前の体の元からなる有理式である。即ち、対称式である。

$$r = \phi^p(x_1, x_2, x_3, x_4, x_5)$$

体を拡大させるために $\sqrt[p]{r}$を作ったのだから、勿論 $\sqrt[p]{r}$は対称式ではない。

従って、何か置換σがあって、これに作用すると変化する。即ち、

$$\sigma\phi(x_1, x_2, x_3, x_4, x_5) \neq \phi(x_1, x_2, x_3, x_4, x_5)$$

置換σは、互換（2 個の数字の置換）の積に書ける。即ち、

$$\sigma = (i_m, j_m)(i_{m-1}, j_{m-1}) \dots (i_2, j_2)(i_1, j_1)$$

このことは証明していないが、例えば、

$(1, 2, 3, 4, 5) = (1, 2)(2, 3)(3, 4)(4, 5)$

となることから明らかであろう。

右から順に作用させていって、初めて$\phi(x_1, x_2, x_3, x_4, x_5)$ でなくなった (i_k, j_k) を改めて (i, j) とおく。

このような (i_k, j_k) は必ず存在する。

$\because$ もし存在しなければ、最後の (i_m, j_m) まで行って、

$\sigma\phi(x_1, x_2, x_3, x_4, x_5) = \phi(x_1, x_2, x_3, x_4, x_5)$ となり、矛盾。

$(i, j)\phi(x_1, x_2, x_3, x_4, x_5)$ を$\phi'(x_1, x_2, x_3, x_4, x_5)$ とおく。即ち、

$(i, j)\phi(x_1, x_2, x_3, x_4, x_5) = \phi'(x_1, x_2, x_3, x_4, x_5)$

仮定より勿論、

$\phi'(x_1,x_2,x_3,x_4,x_5) \neq \phi(x_1,x_2,x_3,x_4,x_5)$

さて、上の式、$(i,j)\phi = \phi'$を p 乗する。（変数を書くのは省略。）

$((i,j)\phi)^p = (\phi')^p$

この左辺はϕに変数 x_i, x_jの入れ換えを行った後、p 乗したもの。従って、これを逆の順序つまり、p 乗した後、変数の入れ換えを行ったものに等しい。故に次の式が成り立つ。

$(i,j)\phi^p = (\phi')^p$

ところが左辺のϕ^pは R の元であるから対称式。故に (i,j) を作用させても変化なし。従って、

$\phi^p = (\phi')^p$

$\therefore \phi' = \epsilon\phi$　　（ϵ は、1 の虚 p 乗根、又は -1。）

さて、$(i,j)(i,j) = (1)$ であるから、

$(i,j)(i,j)\phi = \phi$

この左辺は、$(i,j)\big((i,j)\phi\big) = (i,j)\phi' = (i,j)\epsilon\phi = \epsilon(i,j)\phi = \epsilon^2\phi$

即ち、

$\epsilon^2\phi = \phi$

$\therefore \quad \epsilon^2 = 1$

$\epsilon = 1$ とすると、$\phi' = \phi$となり矛盾。従って、$\epsilon = -1$

$\therefore \quad \phi' = -\phi$

一方、$\phi^p = (\phi')^p$ より、$\phi^p = (-\phi)^p$

$\therefore \quad p$ は 2 の倍数。

p が $4, 6, 8, \ldots$ のときは、次々に 2 乗根を添加して体を拡大することにすれば、最初に拡大すべき p は 2。即ち、2 乗根。そして、根 x_1, x_2, x_3, x_4, x_5はいずれも特別扱いをしていないから、(i,j) で言えたことはすべての他の組み合わせで言えなければならない。即ちϕは、

$(1,2)\phi = -\phi$　　$(1,3)\phi = -\phi$　　$(1,4)\phi = -\phi$　　$(1,5)\phi = -\phi$

$(2,3)\phi = -\phi$　　$(2,4)\phi = -\phi$　　$(2,5)\phi = -\phi$　　$(3,4)\phi = -\phi$

$(3,5)\phi = -\phi$　　$(4,5)\phi = -\phi$

を満たさねばならない。上の 10 の関係を満たす多項式を 5 次の交代式という。

ここで一般に「交代式」の定義を書いておく。

定義 5. *2* 個の置換 *(i,j)*（これを互換という）によって符号を変える多項式を交代式という。

（註　この定義に矛盾が生じないかどうかを示す必要があるが、ここでは省略する。）

以上から分かっ たことは、「最初の拡大は 2 乗根によるものであり、添加すべき式は交代式」ということである。

交代式の例は簡単に作れて、

$$p=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_1-x_5)(x_2-x_3)(x_2-x_4)(x_2-x_5)$$
$$\times(x_3-x_4)(x_3-x_5)(x_4-x_5)$$
この p を最簡交代式というが、これを用いると、任意の交代式 ϕ は h を対称式として、
$$\phi=hp$$
と書けることが証明される。
証明には、因数定理「多項式の変数 x に p を代入して 0 になれば、その多項式は $x-p$ で割り切れる」を用いる。
まず交代式 $\phi(x_1,x_2,x_3,x_4,x_5)$ が (x_1-x_2) で割り切れることを言う。
$\because\quad (1,2)\phi(x_1,x_2,x_3,x_4,x_5)=-\phi(x_1,x_2,x_3,x_4,x_5)$
この左辺は$\phi(x_2,x_1,x_3,x_4,x_5)$ である。故に、
$\phi(x_1,x_2,x_3,x_4,x_5)=-\phi(x_2,x_1,x_3,x_4,x_5)$
このϕの x_1に x_2を代入すると、
$\phi(x_2,x_2,x_3,x_4,x_5)=-\phi(x_2,x_2,x_3,x_4,x_5)$
右の式を左辺に移項して、
$$2\phi(x_2,x_2,x_3,x_4,x_5)=0$$
$\therefore\quad \phi(x_2,x_2,x_3,x_4,x_5)=0$
即ち、ϕは (x_1-x_2) で割り切れる。
同様にして、$(x_1-x_3)\dots(x_4-x_5)$ で割り切れるから、ϕ は p で割り切れる。その商を h とすると、
$\phi=hp$
ここで h が対称式であることを言う。
両辺に $(1,2)$ を施して、
$$(1,2)\phi=(1,2)(hp)$$
この左辺は $-\phi$。故に $-hp$。
右辺は、$[(1,2)h][(1,2)p]$ に等しい。またこれは $(1,2)h(-p)$ であるから、
$(1,2)h(-p)=-hp$
両辺を $-p$ で割って、
$(1,2)h=h$
同様にしてどんな (i,j) に対しても、$(i,j)h=h$
即ち h は対称式。
以上から分かったことは、「最初の拡大は 2 乗根によるものであり、添加すべき式は hp（対称式 × 最簡交代式）」ということである。ところが、対称式はもともと R_1の元であるから、添加の必要はない。
即ち、「最初の拡大は 2 乗根によるものであり、添加すべき式は最簡交代式である」ことが分かった。（証明終わり）

R_2は、R_1に最簡交代式 P を添加して作られた。
最簡交代式は互換を施すと変化するが、互換を偶数回施しても変化しない。つまり、R_2の元を変化させない置換は、偶数回の互換によって出来る置換

である。そこで次の定義を設ける。

定義 6. 偶数個の互換の積で出来る置換を偶置換という。それ以外の置換を奇置換という。*(1)* は *0* 回の互換を行って出来る置換だから偶置換に入れる。

例　(1,2,3)=(1,2)(2,3)　　偶置換
(1,2,3,4)=(1,2)(2,3)(3,4)　　奇置換
(1,2)(2,3,4)=(1,2)(2,3)(3,4)　　奇置換
（註　「ある置換が偶数個の互換で表され、かつ奇数個の互換でも表される」ということはおこらない。このことは証明を要することであるが、ここでは省略する。）

次に証明する定理は、「平方根の次の体の拡大は立方根」であるが、準備のためまず次の定理を示す。

定理 3. 任意の偶置換によ っ て変化しない多項式 ϕ は $S+S'P$（ここで S、S' は対称式、P は最簡交代式）と表される。
証明　最初に、任意の偶置換は 3 個の数字の置換 (i,j,k) の積によって表されることを示す。
そのためにまず、任意の互換 (i,j) は $(1,l)$ の形の互換の積によって表されることを言う。それは、

$$(i,j)=(1,i)(1,j)(1,i)\quad \text{だからである。}$$

従って、2 個の $(1,l)$ の形の互換の積が (i,j,k) と書けることを言えばよい。それは, ただ計算すれば出てくる。つまり、

$$(1,i)(1,j)=(1,j,i)$$

となるから。これで示された。

$$\text{例}\quad (1,2)(3,4)=(1,2)(1,3)(1,4)(1,3)=(1,3,2)(1,3,4)$$

$$(2,3)(4,5)=(1,2)(1,3)(1,2)(1,4)(1,5)(1,4)=(1,3,2)(1,4,2)(1,4,5)$$

従って、上に掲げた定理は、「任意の (i,j,k) によって変化しない多項式は $S+S'P$ と表される」を示せばよいことになった。これを示す。
もし与えられた多項式 ϕ が任意の (i,j) によって変化しないならば ϕ は対称式だから、$S'=0$ とおけばよい、からこの場合はすみ。
ある (i,j) が存在して、$(i,j)\phi=\phi'\quad(\phi'\neq\phi)$ とする。
するとϕは、任意の互換 (k,l) を（1 回）施されてϕ'となる。

$\because$　$(k,l)(i,j)$ が偶置換だから変化せず、$(k,l)(i,j)\phi=\phi$
両辺に (k,l) を施して、$(i,j)\phi=(k,l)\phi$
$\therefore\quad (k,l)\phi=\phi'$
これで示された。

即ち、ϕは、任意の奇置換に対してϕ'となる。

また、ϕ'は、任意の偶置換に対してϕ'となり、任意の奇置換に対してϕとなる。

($\because$　置換を互換の積になおして考えればよい。)

すると、$\dfrac{\phi+\phi'}{2}$は対称式、$\dfrac{\phi-\phi'}{2}$は交代式になる。

$\left(\because\quad \tau$を奇置換とすれば、$\tau\left(\dfrac{\phi-\phi'}{2}\right)=\dfrac{\phi'-\phi}{2}$より。$\right)$

ϕは上の二つの式をつかって、

$$\phi=\frac{\phi+\phi'}{2}+\frac{\phi-\phi'}{2}=\text{対称式}+\text{交代式}$$

と表すことが出来、また、任意の交代式は$S'P$(S'は対称式、Pは最簡交代式)と書けるから、

$$\phi=S+S'P$$

と表すことが出来た。(証明終わり)

上の定理により、「最初の拡大によって出来た体R_1の元は任意の偶置換によって変化しない多項式」であることが分かった。

ここで次の定理を示す。

定理 4. 2番目の体の拡大は立方根による。

証明　R_1に$\psi(x_1,x_2,x_3,x_4,x_5)$を添加して体を拡大する。

$$\psi(x_1,x_2,x_3,x_4,x_5)=\sqrt[q]{r_1}\quad(r_1\text{は}R_1\text{の元})$$

としてqを求める。($q=3$が予告していた数である。)

ψは、R_1の元ではないから、ある(i,j,k)があって、

$(i,j,k)\psi=\psi'\quad(\psi'\neq\psi)$

ψをq乗するとR_1の元だから、これに(i,j,k)を施しても不変。

$(i,j,k)\{\psi^q\}=(\psi)^q$

q乗してから変数を入れ換えても、変数を入れ換えてからq乗しても同じだから、

$\{(i,j,k)\psi\}^q=(\psi)^q$

$\therefore\quad(\psi')^q=\psi^q$

$\therefore\quad\psi'=\omega\psi\quad$($\omega$は1の虚$q$乗根)

さて、$(1,2,3)(1,2,3)(1,2,3)=(1)$だから、

$\psi=(1,2,3)(1,2,3)(1,2,3)\psi=\omega^3\psi$

故に、　ωは1の虚3乗根。

$(\omega\psi)^q=\psi^q\quad$より、$q$は3の倍数。

qが$6,9,12,\ldots$のときは、3乗根を次々と添加することにして、(2乗根の次に)最初に添加すべき根は3乗根。即ち$R_2=R_1(\sqrt[3]{r_1})$であることが分かった。(証明終わり)

さて、5 次方程式のときに、2 回目の拡大が出来るであろうか。実はこの拡大が不可能であることが証明されるのである。(1 回目の拡大は最簡交代式の添加であるから、これは可能。)

ここですぐその証明をしても気分が出ないと思われるので、3 次、4 次方程式の場合を振り返 っ てみることにする。

3 次方程式のとき。

$u = x_1 + \omega x_2 + \omega^2 x_3$

とおくと、u は R_1の元ではない。なぜなら、

$(1,2,3)u = x_2 + \omega x_3 + \omega^2 x_1 = \omega^2(x_1 + \omega x_2 + \omega^2 x_3) = \omega^2 u \neq u$

即ち、偶置換で変化してしまうから。ところが、u^3は R_1の元である。なぜなら、S_3には偶置換は (1) を除いて 2 個、つまり $(1,2,3)$ と $(1,3,2)$ しかなくて、

$(1,2,3)u^3 = \{(1,2,3)u\}^3 = \{\omega^2 u\} = \omega^6 u^3 = u^3$

$(1,3,2)u^3 = \{(1,3,2)u\}^3 = \{\omega u\} = \omega^3 u^3 = u^3$

であるから。

即ち、変数が 3 個のときは、「それ自身は偶置換で変化するが、その 3 乗は偶置換では変化しない多項式」を捜すことが出来ている。

4 次方程式のとき。

$u_1 = x_1 + x_2 - x_3 - x_4$

$u_2 = x_1 - x_2 + x_3 - x_4$

$u_3 = x_1 - x_2 - x_3 + x_4$

とし、

$u = u_1^2 + \omega u_2^2 + \omega^2 u_3^2$

とおくと、u は R_1の元ではない。なぜなら、

$(1,2,3)u = u_3^2 + \omega u_1^2 + \omega^2 u_2^2 = \omega u \neq u$

(ここでの $(1,2,3)$ は、変数 x についてであ っ て、u に対するものでないことに注意。)

であ っ た。

しかし u^3は R_1の元。なぜなら、

$(1,2,3)u^3 = \{(1,2,3)u\}^3 = (\omega u)^3 = u^3 \quad etc$

だからである。即ち、「それ自身は偶置換で変化するが、その 3 乗は偶置換では変化しない多項式」を捜すことが出来ている。

5 次方程式でこれを捜そうとしても、うまくいかないのである。少し努力してみる。例えば、

3 乗で R_1に入るのだから、$\psi = u_1^2 + \omega u_2^2 + \omega^2 u_3^2$として、$u_1, u_2, u_3$にうまい x_1, x_2, x_3, x_4, x_5の多項式を考えつけばよい。しかしこれは難しい。例え

ば u_1として、
$u_1 = x_1 + x_2 - x_3 - x_4 - x_5$
とおき、$(1,2,3)$ を作用させると、
$(1,2,3)u_1 = x_2, +x_3 - x_1 - x_4 - x_5$
これは u_1とは違うので、$-u_2$とおいて、
$u_2 = x_1 - x_2 - x_3 + x_4 + x_5$
$(1,2,3)u_2 = x_2 - x_3 - x_1 + x_4 + x_5$
これは u_1とも、u_2とも違うので、$-u_3$とおいて、
$(1,2,3)u_3 = x_2 - x_3 + x_1 - x_4 - x_5 = u_1$
即ち、
$(1,2,3)u_1^2 = u_2^2$
$(1,2,3)u_2^2 = u_3^2$
$(1,2,3)u_3^2 = u_1^2$
で、
$(1,2,3)\psi = \omega^2\psi$
一方、3 乗の方は、$(1,2,3)\psi^3 = \{(1,2,3)\psi\}^3 = \{\omega^2\psi\} = \psi^3$
つまり、「$(1,2,3)$ で 3 乗は変らないが元の式は変る」ものが出来た。
しかしψ^3が R_1の元であるためには、「どんな偶置換に対してもψ^3が変らない」ことが必要なのである。そこで、偶置換 $(1,2,3,4,5)$ でやってみると、
$(1,2,3,4,5)u_1^2 = (x_2 + x_3 - x_4 - x_5 - x_1)^2 = u_2^2$
である。が、
$(1,2,3,4,5)u_2^2 = (x_2 - x_3 - x_4 + x_5 + x_1)^2 = (x_1 + x_2 - x_3 - x_4 + x_5)^2$
となり、u_1でも u_2でもない。つまり、$(1,2,3,4,5)\psi^3$はψ^3ではないのである。
　さて、実は次のことが言えるのである。

定理 5. ψを 5 変数 x_1, x_2, x_3, x_4, x_5の多項式とする。すると、
ψ^3が任意の偶置換によ っ て変化しないならば、ψは任意の偶置換によ っ て変化しない。
証明　$(1,3,2,4,5)$ は偶置換。
$\therefore \quad (1,3,2,4,5)\psi^3 = \psi^3$
$\therefore \quad \{(1,3,2,4,5)\psi\}^3 = \psi^3$
$\therefore \quad (1,3,2,4,5)\psi = \omega\psi \quad (\omega^3 = 1)$
(注意　ここで、$\omega^3 = 1$ であ っ て、「ωは 1 の虚 3 乗根」でないことに注意。即ち、$(1,3,2,4,5)\psi = \psi$かもしれない。)
一方、$(1,3,2,4,5)(1,3,2,4,5)(1,3,2,4,5)(1,3,2,4,5)(1,3,2,4,5) = (1)$ だから、
$\psi = (1,3,2,4,5)(1,3,2,4,5)(1,3,2,4,5)(1,3,2,4,5)(1,3,2,4,5)\psi = \omega^5\psi$
$\therefore \quad \omega^5 = 1$
$\omega^3 = 1$ でもあ っ たから、

$$\omega = 1$$
$\therefore \quad (1,3,2,4,5)\psi = \psi$
同様の計算によ っ て、
$$(3,2,1,4,5)\psi = \psi$$
$\therefore \quad (3,2,1,4,5)(1,3,2,4,5)\psi = \psi$
$\therefore \quad (1,2,3)\psi = \psi$
同様の計算により、任意の (i,j,k) に対し、
$$(i,j,k)\psi = \psi$$
即ちψは R_1の元。　（証明終わり）

即ち、変数が 5 個あると、3 次の根号を添加することによ っ て体を拡大することは出来ないのである。
すると 5 次方程式は $R(\sqrt{D})$ までの拡大で根を含まねばならないが、これは、
$x_1 = S_1 + S_2 P$　（S_1, S_2は対称式、P は最簡交代式）
が恒等式になり得ないので無理。
以上から「5 次方程式は根号を用いて根を求めることは出来ない」ことが示された。

3　「重要な仮定」の証明

さて、残 っ た「重要な仮定」、即ち、定理**??**(重要な仮定)「体を拡大するときに添加する根号は与えられた方程式の根の有理式で書ける」を示すことが、この節の目的である。
これが 2 次、3 次、4 次方程式のときに成立していたことを、諄（くど）いようであるがもう一度見てみる。

1　2 次方程式のとき。 $\sqrt{D} = x_1 - x_2$　で大丈夫。
2　3 次方程式のとき。 $\sqrt{-27D} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
　　次に u を添加。 $u = x_1 + \omega x_2 + \omega^2 x_3$
　で大丈夫。
3　4 次方程式のとき。 $\sqrt{-27D'} = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)$
　　$(x_2 - x_4)(x_3 - x_4)$
　次に u を添加するが、これは、$u = (x_1 + x_2 - x_3 - x_4)^2$
　　$+ \omega(x_1 - x_2 + x_3 - x_4)^2 + \omega^2(x_1 + x_2 - x_3 - x_4)^2$
　次に u_1を添加するが、これは、$u_1 = x_1 + x_2 - x_3 - x_4$
　次に u_2を添加するが、これは、$u_2 = x_1 - x_2 + x_3 - x_4$
　で大丈夫。
以下定理**??**を示すが、途中 4 個所で証明を飛ばす。これは証明の筋道を追

いやすいようにとの配慮であるが、この方法が成功しているかどうかは未知。勿論後に証明を定理、あるいは問題の形で説明する。また、「最後から２番目の拡大に関して成立」の部分はアーベルのもとの論文でも分かり難いので、後で解説をつける。

定理**??**の証明　５次方程式

$$x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$$

が与えられていて、a_1、a_2、a_3、a_4、a_5からなる体 R_1を拡大していって、

$$R_1 \subset R_2 \subset \cdots R_{k-1} \subset R_{k-1}(\sqrt[p]{r}) = R_k$$

のところで解けたとする。

$$\sqrt[p]{r} = \alpha$$

とおいて、

$$x_1 = r_0 + r_1\alpha + \cdots + r_{p-1}\alpha^{p-1}$$

（$r_0, r_1, \cdots r_{p-1}$は R_{k-1}の元。）

が根だとする。（このように、分母を有理化できることは証明を要すが、後に問題**??**において説明する。）

このとき、Rに添加すべき元を少し変更することによって、αの１乗の係数 r_1を１にすることが出来、改めて根 x_1は、

$$x_1 = r_0 + \alpha + \cdots + r_{p-1}\alpha^{p-1}$$

としてよい。（このように、１にできることは証明を要すが、後に定理**??**において示す。）

この x_1を原方程式に代入して、αの冪で整頓すると、

$$T_0 + T_1\alpha + +T_1\alpha^2 + \cdots + +T_{p-1}\alpha^{p-1} = 0$$

（$T_i(i = 0, 1, \cdots p-1)$ は R_{k_1}の元。）

となる。（$\because$　αが根だから。）

表現の一意性により、（「表現の一意性」は証明を要すが、後に定理**??**において示す。）

$$T_0 = T_1 = T_2 = \cdots = T_{p-1} = 0$$

となる。故に、ϵを１の虚 p 乗根として、

$$x_2 = r_0 + (\epsilon\alpha) + r_2 + (\epsilon\alpha)^2 \cdots + r_{p-1}(\epsilon\alpha)^{p-1}$$
$$x_3 = r_0 + (\epsilon^2\alpha) + r_2 + (\epsilon^2\alpha)^2 \cdots + r_{p-1}(\epsilon^2\alpha)^{p-1}$$
$$\cdots\cdots\cdots$$
$$x_p = r_0 + (\epsilon^{p-1}\alpha) + r_2 + (\epsilon^{p-1}\alpha)^2 \cdots + r_{p-1}(\epsilon^{p-1}\alpha)^{p-1}$$

とおき、これらを原方程式に代入すると、

x_2を代入　$T_0 + T_1(\epsilon\alpha) + T_2(\epsilon\alpha)^2 + \cdots + T_{p-1}(\epsilon\alpha)^{p-1} = 0$

x_3を代入　$T_0 + T_1(\epsilon^2\alpha) + T_2(\epsilon^2\alpha)^2 + \cdots + T_{p-1}(\epsilon^2\alpha)^{p-1} = 0$

$\cdots\cdots\cdots$

x_pを代入　$T_0 + T_1(\epsilon^{p-1}\alpha) + T_2(\epsilon^{p-1}\alpha)^2 + \cdots + T_{p-1}(\epsilon^{p-1}\alpha)^{p-1} = 0$

（このことはちょっと分かり難いので、後に練習問題**??**として解説する。）

となるから、$x_1, x_2, \cdots x_p$, は原方程式の根。
ϵは 1 の虚 p 乗根だから、

$$\epsilon^{p-1} + \epsilon^{p-2} + \cdots + \epsilon^2 + \epsilon^1 + 1 = 0$$

に気をつければ、αは $x_1, x_2, \cdots x_p$で次のように表される。

$$\alpha = \frac{1}{p}(x_1 + \epsilon^{-1}x_2 + \epsilon^{-2}x_3 + \cdots + \epsilon^{-(p-1)}x_p)$$

これで、「最後に添加すべき根号は原方程式の根の有理式で表される」は示された。
次に「最後から二番目に添加すべき根号も原方程式の根の有理式で表される」を示す。
（これが示されれば、この証明が次々に前に適用出来て、証明終りとなる。）
そのときに使うので、上の式から、$r_0, r_2, r_3, \cdots, r_{p-1}$も原方程式の根の有理式で表されることを言っておく。

$$r_0 = \frac{1}{p}(x_1 + x_2 + x_3 + \cdots + x_p)$$

$$r_2\alpha^2 = \frac{1}{p}(x_1 + \epsilon^{2(-1)}x_2 + \epsilon^{2(-2)}x_3 + \cdots + \epsilon^{-2(p-1)}x_p)$$

$$\cdots\cdots\cdots$$

$$r_{p-1}\alpha^{p-1} = \frac{1}{p}(x_1 + \epsilon^{(p-1)(-1)}x_2 + \epsilon^{(p-1)(-2)}x_3 + \cdots + \epsilon^{-(p-1)(p-1)}x_p)$$

ここでαは既に原方程式の根で表されているから、$r_0, r_2, r_3, \cdots, r_{p-1}$も原方程式の根の有理式で表されている。
さて、最後から二番目の拡大を $R(\sqrt[q]{r})$ とする。即ち、拡大が次のようになっているとする。

$$R \subset \cdots \subset R_{k-2} \subset R_{k-2}(\sqrt[q]{r}) \subset R_{k-2}(\sqrt[q]{r}, \sqrt[p]{r'})$$

最後から二番目の拡大のときの添加する $\sqrt[q]{r}$が、原方程式の根、$x_1, x_2, \cdots x_p$で表されることを言う。
（以下の証明はひどくさっぱりしている。しかし分かり難いので、後に練習問題**??**として解説する。）
すぐ前にやった結果から、$r_0, r_2, r_3, \cdots, r_{p-1}$も原方程式の根の有理式で表されている。
この中で、$R_{k-2}(\sqrt[q]{r})$ に拡大して初めて含まれたものがある筈。（もしそうでなければ、$r_0, r_2, r_3, \cdots, r_{p-1}$は全て R_{k-2}までの元であり、R_{k-1}まで拡大することなく $\sqrt[p]{r'}$を添加することによって $x_1, x_2, \cdots x_p$, が解けたことになる。これは矛盾。）
その r_iを y_0とおく。y_0は $x_1, x_2, \cdots x_p$の有理式である。今、S_5を 5 次の置換全部の集合として、（その数は 5 の階乗個ある。従って、120 個の置換となる。）次の方程式 $F(y) = 0$ を考える

$$F(y) = \prod_{\sigma \in S_5} (y - \sigma y_o) = 0 \tag{1}$$

と、これは 120 次の方程式だが、係数は $x_1, x_2, \cdots x_5$の対称式。従 っ て、原

方程式の係数で書けている。

このことを次の様に解釈する。即ち、

最初に方程式 $F(y)=0$ が与えられていて、これを解こうとする。係数の体（これは原方程式の係数のなす体と同じ）を拡大していっ て、$R_{k-1}=R_{k-2}(\sqrt[q]{r})$ まで来たとき、y_0が初めて解けた。

即ち、最後に添加した$\sqrt[q]{r}$は、$\sigma y_0(\sigma\in S_5)$ で表される。

$\sigma y_0(\sigma\in S_5)$ は $x_1,x_2,\cdots x_5$の有理式だから、$\sqrt[q]{r}$は $x_1,x_2,\cdots x_5$の有理式である。　（証明終わり）

さて、残されたものをやる。

問 16. 1) 次のξを有理化せよ。但し$\alpha=\sqrt[3]{2}$である。

$$\xi=\frac{1}{g(\alpha)}=\frac{1}{1+2\alpha+3\alpha^2}$$

2)　次のξを有理化せよ。但し$\alpha=\sqrt[5]{2}$である。

$$\xi=\frac{1}{g(\alpha)}=\frac{1}{1+2\alpha+3\alpha^2+4\alpha^3+5\alpha^4}$$

（解 -1）分子、分母に

$g(\omega\alpha)g(\omega^2\alpha)$　(ω は 1 の虚 3 乗根)

をかける。

$g(\omega\alpha)g(\omega^2\alpha)=(1+2\omega\alpha+3\omega^2\alpha^2)(1+2\omega^2\alpha+3\omega\alpha^2)$

$=1+2\omega\alpha+3\omega^2\alpha^2$

$\quad 2\omega\alpha+4\alpha^2+12\omega^2$

$\quad\quad 3\omega^2\alpha^2+12\omega+18\alpha$

$=(1+12\omega+12\omega^2)+(2\omega^2+2\omega+18)\alpha+(3\omega+4+3\omega^2)\alpha^2$

$=-11+16\alpha+\alpha^2$

$$\therefore\quad \xi=\frac{-11+16\alpha+\alpha^2}{(1+2\alpha+3\alpha^2)(-11+16\alpha+\alpha^2)}$$

$$=\frac{-11+16\alpha+\alpha^2}{89}$$　（解 1　終わり）

1) の解説。

何故 $g(\omega\alpha)g(\omega^2\alpha)$ にはωがなくなるかというと、この式は$\omega\alpha$と$\omega^2\alpha$の対称式。従っ て、変数 2 の基本対称式で書ける。実際にその基本対称式を作っ てみると、

$\sigma_1=\omega\alpha+\omega^2\alpha=-\alpha$

$\sigma_2=(\omega\alpha)(\omega^2\alpha)=\alpha^2$

確かにωは含まれていない。この 2 個と、元の式の係数で表されるのだから、ωは含まれない。

次に、何故分母が有理化されるかというと、

$g(\alpha)g(\omega\alpha)g(\omega^2\alpha)$ は$\alpha,\omega\alpha$と$\omega^2\alpha$の対称式。従っ て、変数 3 の基本対称式で書ける。実際にその基本対称式を作っ てみると、

$\sigma_1=\alpha+\omega\alpha+\omega^2\alpha=0$

$\sigma_2 = (\alpha)(\omega\alpha) + (\alpha)(\omega^2\alpha) + (\omega\alpha)(\omega^2\alpha) = 0$
$\sigma_3 = (\alpha)(\omega\alpha)(\omega^2\alpha) = 2$
$0, 0, 2$ と、元の式の係数で表されるのだからα は含まれない。（解説終わり）

（解 -2）分子、分母に
$g(\epsilon\alpha)g(\epsilon^2\alpha)g(\epsilon^3\alpha)g(\epsilon^4\alpha)$　(ϵ は 1 の虚 5 乗根)
をかける。
　すると、分母は有理化され、分子には ϵ は含まれず、
$\xi = \dfrac{-3359 + 4028\alpha + 121\alpha^2 + 110\alpha^3 + 100\alpha^4}{38949}$
（解 2　終わり）

定理 6. $R_(\sqrt[p]{r})$ まで拡大して、方程式の根 x_1が、($\sqrt[p]{r} = \alpha$とおいて)
$x_1 = r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{p-1}\alpha^{p-1}$
として解けたとする。このとき、拡大のとき添加すべき$\sqrt[p]{r}$を少し変えることにより、
$x_1 = r_0 + \alpha + r_2\alpha^2 + \cdots + r_{p-1}\alpha^{p-1}$
と、αの係数を 1 にすることが出来る。
証明　$case$　1)　$r_1 \neq 0$,　$case$　2)　$r_1 = 0$, の二つの場合に分けて示す。
$case$　1) のとき。
R に$\sqrt[p]{r}$ を添加する代わりに、$r_1\sqrt[p]{r}$を添加すればよい。
$r_1\sqrt[p]{r}$を改めてβとおく。即ち、
$\beta = r_1\alpha$
$\alpha = \dfrac{\beta}{r_1}$
であるから、
$x_1 = r_0 + \beta + r_2\left(\dfrac{1}{r_1}\right)^2\beta^2 + \cdots + r_{p-1}\left(\dfrac{1}{r_1}\right)^{p-1}\beta^{p-1}$
ここで $r_i\left(\dfrac{1}{r_1}\right)^i$ は R の元であるから、改めて r_iとおけば、体 $R(\beta)$ において、
$x_1 = r_0 + \beta + r_2\beta^2 + \cdots + r_{p-1}\beta^{p-1}$
と書けた。これで $case$ 1) の証明は終わり。
$case$ 2) 即ち $r_1 = 0$　のとき。
　r_i $(i = 2, 3, \cdots p-1)$ の中で、0 に等しくない最初のものを $r_m\alpha^m$とする。（これは必ず存在する。そうでなければ、$x_1 = r_0$、即ち、x_1がその前の体 R の元となり、拡大する必要がなかったことになる。）
そして、$\beta = r_m\alpha^m$ とおいて、R にβを添加して体 $R(\beta)$ を作ればよい。
あと示さねばならないことは、「αを R の元とβで表すことが出来る」である。
以下、その証明。
　p は素数、m はそれより小さい自然数だから、p と m は互いに素。従って最

大公約数は 1。故にうまい整数 h と k を捜してくれば、

$$mh = pk + 1$$

と出来る。（具体的にはユークリッドの互除法を使えばよい。この解説も後でする。）

$\therefore \quad \alpha^{mh} = \alpha^{pk}\alpha$

$\alpha^p = r, \alpha^m = \dfrac{\beta}{r_m}$だから、$\left(\dfrac{\beta}{r_m}\right)^h = r^k\alpha$

$\therefore \quad \alpha = \dfrac{\beta^h}{r_m^h r^k}$

即ち、αは $R(\beta)$ の元。

なおまた、x_1は、

$x_1 = r'_0 + \beta + r'_2\beta^2 + \cdots + r'_{p-1}\beta^{p-1}$

と表される。　（証明終わり）

数に関するユークリッド互除法を忘れた人のために、次の練習問題を解いておく。

問 17. 問　$p = 87$ と $q = 67$ は互いに素である。$hp = kq + 1$ を満たす整数 h と k を求めよ。

解　87 を 67 で割 っ て余りを求める。

$87 = 67 \times 1 + 20 \quad \therefore \quad 20 = p - q$

その余り 20 で 67 を割 っ て余りを求める。

$67 = 20 \times 3 + 7 \quad \therefore \quad 7 = q - 3 \times 20 = q - 3(p - q) = 4q - 3p$

その余り 7 で 20 を割 っ て余りを求める。

$20 = 7\times3+(-1) \quad \therefore \quad -1 = 20-3\times7 = (p-q)-3(4q-3p) = 10p-13q$

即ち、

$h = -10, k = -13$

が、求める整数解（の一つ）であ っ て、

$-10p = -13q + 1$　（解終わり）

次の「一意性」の定理を示す前に多項式の最大公約数を見つけるときの、ユークリッド互除法を復習しておく。

問 18. $x^4 + 5x^3 + 10x^2 + 11x + 3$ と $x^4 + 4x^3 + 7x^2 + 10x + 3$ の最大公約数（多項式）を求めよ。

解　$x^4 + 5x^3 + 10x^2 + 11x + 3$ を $x^4 + 4x^3 + 7x^2 + 10x + 3$ で割 っ て、余りを求める。

$x^4+5x^3+10x^2+11x+3 = (x^4+4x^3+7x^2+10x+3)1 + x^3+3x^2+x$

この余り、$x^3 + 3x^2 + x$ で $x^4 + 4x^3 + 7x^2 + 10x + 3$ を割り、余りを求める。

$$x^4+4x^3+7x^2+10x+3=(x^3+3x^2+x)(x+1)+3x^2+9x^+3$$
この余り、$3x^2+9x^+3$ で x^3+3x^2+x を割り、余りを求める。
$$x^3+3x^2+x=(3x^2+9x^+3)(1/3)x+0$$
余りは 0。即ち $(3x^2+9x^+3)$ あるいは、3 で割った x^2+3x+1 が最大公約数。（解終わり）

定理 7. p が素数で、$\alpha=\sqrt[p]{r}$のとき、ある数ξが
$$\xi=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{p-1}\alpha^{p-1}$$
（ここで a_i $(i=1,2,\cdots p-1)$ は、αを添加する前の体の元。）
と表されたとすると、この表し仕方はこれしかない。（このことを、「表現の一意性」という。）
証明　次のように二通りに表されたと仮定する。
$$\xi=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{p-1}\alpha^{p-1}=b_0+b_1\alpha+b_2\alpha^2+\cdots+b_{p-1}\alpha^{p-1}$$
（ここで a_i,b_i $(i=1,2,\cdots p-1)$ は、αを添加する前の体の元。）
$a_i-b_i=r_i$とおいて、$r_i=0$ $(i=1,2,\cdots p-1)$ を示す。即ち、右辺を左に移項して、
$$r_0+r_1\alpha+r_2\alpha^2+\cdots+r_{p-1}\alpha^{p-1}$$
降冪の順になおして、αを x に変えた方程式を作ると、
$$r_{p-1}x^(p-1)+r_{p-1}x^(p-1)+\cdots+r_2x^2+r_1x+r_0=0$$
ここで「全ての r_iが 0 であること」を示せばよい。これを示す。
この方程式はαを根にもつ。即ち $x-\alpha$を因数に持つ。また、αは、方程式
$$x^p-r=0$$
の根。故にこの方程式も $x-\alpha$を因数に持つ。故に、上の二つの式の最大公約数は 1 ではなく、ある多項式である。これをユークリッドの互除法によって求めると、係数が添加する前の体の元 q_i である多項式、
$$q_mx^m+q_{m-1}x^{q-1}+\cdots+q_1x+q_0$$
が出来、最大公約数である。最大係数を 1 にするため q_mで割って作った式、
$$x^m+s_{m-1}x^{q-1}+\cdots+s_1x+s_0$$
（ここで s_i $(i=1,2,\cdots m)$ は、αを添加する前の体の元。）
も両多項式の最大公約数である。ところがこれは、x^p-r を 1 次因数に分解したものの、m 個の積でなければならない。即ちϵを 1 の虚 p 乗根として、
$$x^p-r=(x-\alpha)(x-\epsilon\alpha)(x-\epsilon^2\alpha)\cdots(x-\epsilon^{p-1}\alpha)$$
の右辺の 1 次因数の m 個の積。積を作って上の式の定数項とを較べると、
$$s_0=(-1)^m\epsilon'\alpha^m$$
となる。ところが、m は $p-1$ 以下の数であるから、α^mは「αを添加する前の体の元」ではありえない。s_0は「αを添加する前の体の元」であるから、これは矛盾。
（$\because$　m と p は互いに素。故に、$hp=km+1$ をみたす h,k がある。
$\therefore$　$(\alpha^p)^h=(\alpha^m)^k\alpha$

ここでもし、α^mが「αを添加する前の体の元」ならば、
αも「αを添加する前の体の元」となり、矛盾。）
これは、r_iの中に 0 でないものがあるとを仮定したことから生じた矛盾。従って、全ての r_iは 0 である。　（証明終わり）

問 19. 本来は、
「問　$x_1 = r_0 + \alpha + r_2\alpha^2 + r_3\alpha^3 + \cdots + r_{p-1}\alpha^{p-1}$
が、方程式、
$x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$
の根であるならば、ϵを 1 の虚 p 乗根として、

$$x_2 = r_0 + (\epsilon\alpha) + r_2 + (\epsilon\alpha)^2 \cdots + r_{p-1}(\epsilon\alpha)^{p-1}$$
$$x_3 = r_0 + (\epsilon^2\alpha) + r_2 + (\epsilon^2\alpha)^2 \cdots + r_{p-1}(\epsilon^2\alpha)^{p-1}$$
$$\cdots\cdots\cdots$$
$$x_p = r_0 + (\epsilon^{p-1}\alpha) + r_2 + (\epsilon^{p-1}\alpha)^2 \cdots + r_{p-1}(\epsilon^{p-1}\alpha)^{p-1}$$

も上の方程式の根である」
ことを示さねばならないのであるが、次数が低いところで具体的にや っ た方が分かり易いと考え、$p = 3$、方程式の次数が 4、のときを例示することにした。
問 1)　多項式 x^2に

$$x_1 = r_0 + r_1\alpha + r_2\alpha^2$$

を代入し、定数項 $T_0^{(2)}, \alpha$の係数 $T_1^{(2)}, \alpha^2$の係数 $T_2^{(2)}$を計算せよ。
また、同じく x^2 に、

$$x_2 = r_0 + r_1\omega\alpha + r_2\omega^2\alpha^2$$
$$x_3 = r_0 + r_1\omega^2\alpha + r_2\omega\alpha^2$$

を代入せよ。
問 2)　多項式 x^3に

$$x_1 = r_0 + r_1\alpha + r_2\alpha^2$$

を代入し、定数項 $T_0^{(3)}, \alpha$の係数 $T_1^{(3)}, \alpha^2$の係数 $T_2^{(3)}$を計算せよ。
また、同じく x^3 に、

$$x_2 = r_0 + r_1\omega\alpha + r_2\omega^2\alpha^2$$
$$x_3 = r_0 + r_1\omega^2\alpha + r_2\omega\alpha^2$$

を代入せよ。
問 3)　多項式 x^4に

$$x_1 = r_0 + r_1\alpha + r_2\alpha^2$$

を代入し、定数項 $T_0^{(4)}, \alpha$の係数 $T_1^{(4)}, \alpha^2$の係数 $T_2^{(4)}$を計算せよ。
また、同じく x^4 に、

$$x_2 = r_0 + r_1\omega\alpha + r_2\omega^2\alpha^2$$
$$x_3 = r_0 + r_1\omega^2\alpha + r_2\omega\alpha^2$$

を代入せよ。

問 4) 多項式

$$f(x) = ax^4 + bx^3 + cx^2 + dx + g$$

に

$$x_1 = r_0 + r_1\alpha + r_2\alpha^2$$

を代入し、定数項 T_0, αの係数 T_1, α^2の係数 T_2を計算せよ。

また、同じく x^3 に、

$$x_2 = r_0 + r_1\omega\alpha + r_2\omega^2\alpha^2$$
$$x_3 = r_0 + r_1\omega^2\alpha + r_2\omega\alpha^2$$

を代入せよ。

解　1)　$x_1^2 = (r_0 + r_1\alpha + r_2\alpha^2)^2$

$= r_0^2 + r_1^2\alpha^2 + r_2^2\alpha^4 + 2r_0r_1\alpha + 2r_0r_2\alpha^2 + 2r_1\alpha r_2\alpha^2$

$= (r_0^2 + 2r_1r_2r) + (r_2^2r + 2r_0r_1)\alpha + (r_1^2 + 2r_0r_2)\alpha^2$

$\therefore \quad T_0^{(2)} = r_0^2 + 2r_1r_2r$

$T_1^{(2)} = r_2^2r + 2r_0r_1$

$T_2^{(2)} = r_1^2 + 2r_0r_2$

x_2 を代入。

$x_2^2 = (r_0 + r_1\omega\alpha + r_2\omega^2\alpha^2)^2$

$= r_0^2 + \omega^2r_1^2\alpha^2 + \omega r_2^2\alpha^4 + \omega 2r_0r_1\alpha + \omega^2 2r_0r_2\alpha^2 + 2r_1\alpha r_2\alpha^2$

$= (r_0^2 + 2r_1r_2r) + (r_2^2r + 2r_0r_1)\omega\alpha + (r_1^2 + 2r_0r_2)\omega^2\alpha^2$

$= T_0^{(2)} + T_1^{(2)}\omega\alpha + T_2^{(2)}\omega^2\alpha^2$

x_3 を代入。

$x_3^2 = (r_0 + r_1\omega^2\alpha + r_2\omega\alpha^2)^2$

$= r_0^2 + \omega r_1^2\alpha^2 + \omega^2 r_2^2\alpha^4 + \omega^2 2r_0r_1\alpha + \omega 2r_0r_2\alpha^2 + 2r_1\alpha r_2\alpha^2$

$= (r_0^2 + 2r_1r_2r) + (r_2^2r + 2r_0r_1)\omega^2\alpha + (r_1^2 + 2r_0r_2)\omega\alpha^2$

$= T_0^{(2)} + T_1^{(2)}\omega^2\alpha + T_2^{(2)}\omega\alpha^2$

解　2)　$x_1^3 = (r_0 + r_1\alpha + r_2\alpha^2)^3$　を求める。

$(a+b+c)^3 = (a)^3+(b)^3+(c)^3+3(a)^2(b)+3(a)^2(c)+3(b)^2(a)+3(b)^2(c)+3(c)^2(a)+3(c)^2(b)+6(a)(b)(c)$　より

$(r_0+r_1\alpha+r_2\alpha^2)^3 = (r_0)^3+(r_1\alpha)^3+(r_2\alpha^2)^3+3(r_0)^2(r_1\alpha)+3(r_0)^2(r_2\alpha^2)+3(r_1\alpha)^2(r_0)+3(r_1\alpha)^2(r_2\alpha^2)+3(r_2\alpha^2)^2(r_0)+3(r_2\alpha^2)^2(r_1\alpha)+6(r_0)(r_1\alpha)(r_2\alpha^2)$

$= (r_0^3 + r_1^3r + r_2^3r^2 + 6r_0r_1r_2r)$

$+ (3r_0^2r_1 + 3r_1^2r_2r + 3r_2^2r_0r)\alpha$

$+ (3r_0^2r_2 + 3r_1^2r_0 + 3r_2^2r_1r)\alpha^2$

$\therefore \quad T_0^{(3)} = r_0^3 + r_1^3r + r_2^3r^2 + 6r_0r_1r_2r$

$T_1^{(3)} = 3r_0^2r_1 + 3r_1^2r_2r + 3r_2^2r_0r$

$T_2^{(3)} = 3r_0^2r_2 + 3r_1^2r_0 + 3r_2^2r_1r$

x_2 を代入。

$x_2^3 = T_0^{(3)} + T_1^{(3)}\omega\alpha + T_2^{(3)}\omega^2\alpha^2$

x_3 を代入。

$x_3^3 = T_0^{(3)} + T_1^{(3)}\omega^2\alpha + T_2^{(3)}\omega\alpha^2$

解　3)　$x_1^4 = (r_0 + r_1\alpha + r_2\alpha^2)^4$　を求める。

$(a+b+c)^4 = (a)^4 + (b)^4 + (c)^3) + 4(a)^3(b) + 4(a)^3(c) + 4(b)^3(a) + 4(b)^3(c) + 4(c)^3(a) + 4(c)^3(b) + 6(a)^2(b)^2 + 6(a)^2(c)^2 + 6(b)^2(c)^2 + 12(a)^2(b)(c) + 12(b)^2(a)(c) + 12(c)^2(a)(b)$　より

$(r_0 + r_1\alpha + r_2\alpha^2)^4 = (r_0)^4 + (r_1\alpha)^4 + (r_2\alpha^2)^3) + 4(r_0)^3(r_1\alpha) + 4(r_0)^3(r_2\alpha^2) + 4(r_1\alpha)^3(r_0) + 4(r_1\alpha)^3(r_2\alpha^2) + 4(r_2\alpha^2)^3(r_0) + 4(r_2\alpha^2)^3(r_1\alpha) + 6(r_0)^2(r_1\alpha)^2 + 6(r_0)^2(r_2\alpha^2)^2 + 6(r_1\alpha)^2(r_2\alpha^2)^2 + 12(r_0)^2(r_1\alpha)(r_2\alpha^2) + 12(r_1\alpha)^2(r_0)(r_2\alpha^2) + 12(r_2\alpha^2)^2(r_0)(r_1\alpha)$

$= (r_0^4 + 4r_1r_0r + 4r_2^2r_0r^2 + 4r_2r_1r + 6r_1^2r_2^2r^2 + 12r_0^2r_1r_2r)$

$+ (r_1^4r + 4r_0^3r_1 + 6r_0^2r_2^2r + 12r_1^2r_0r_2r)\alpha$

$+ (r_2^4r^2 + 4r_0^3r_2 + 4r_1^3r_2r + 6r_0^2r_1^2 + 12r_2^2r_0r_1r)\alpha^2$

$\therefore \quad T_0^{(4)} = r_0^4 + 4r_1r_0r + 4r_2^2r_0r^2 + 4r_2r_1r + 6r_1^2r_2^2r^2 + 12r_0^2r_1r_2r$

$T_1^{(4)} = r_1^4r + 4r_0^3r_1 + 6r_0^2r_2^2r + 12r_1^2r_0r_2r$

$T_2^{(4)} = r_2^4r^2 + 4r_0^3r_2 + 4r_1^3r_2r + 6r_0^2r_1^2 + 12r_2^2r_0r_1r$

x_2 を代入。

$x_2^4 = T_0^{(4)} + T_1^{(4)}\omega\alpha + T_2^{(4)}\omega^2\alpha^2$

x_3 を代入。

$x_3^4 = T_0^{(4)} + T_1^{(4)}\omega^2\alpha + T_2^{(4)}\omega\alpha^2$

解　4)　$f(x_1)$　を求める。

$f(x_1) = a(T_0^{(4)} + T_1^{(4)}\alpha + T_2^{(4)}\alpha^2)$

$+ b(T_0^{(3)} + T_1^{(3)}\alpha + T_2^{(3)}\alpha^2)$

$+ c(T_0^{(2)} + T_1^{(2)}\alpha + T_2^{(2)}\alpha^2)$

$+ d(r_0 + r_1\alpha + r_2\alpha^2)$

$+ g$

$= (aT_0^{(4)} + bT_0^{(3)} + cT_0^{(2)} + dr_0 + g)$

$+ (aT_1^{(4)} + bT_1^{(3)} + cT_1^{(2)} + dr_1)\alpha$

$+ (aT_2^{(4)} + bT_2^{(3)} + cT_2^{(2)} + dr_2)\alpha^2$

$= T_0 + T_1\alpha + T_2\alpha^2$

とおくと、

$f(x_2) = T_0 + T_1\omega\alpha + T_2\omega^2\alpha^2$

$f(x_3) = T_0 + T_1\omega^2\alpha + T_2\omega\alpha^2$

以上の計算から、本来の問題、

$f(x) = ax^4 + bx^3 + cx^2 + dx + g = 0$

の一つの根が、

$x_1 = r_0 + r_1\alpha + r_2\alpha^2$　（α^3は $f(x)$ の係数のなす体の元。）

ならば、

$f(x_1) = T_0 + T_1\alpha + T_2\alpha^2 = 0$

一意性により、

$$T_0 = T_1 = T_2 = 0$$

である。この結果から、

$$x_2 = r_0 + r_1\omega\alpha + r_2\omega^2\alpha^2$$

を $f(x)$ に代入しても、

$$f(x_2) = T_0 + T_1\omega\alpha + T_2\omega^2\alpha^2 = 0$$

となり、T_iが全て 0 なのであるから、x_2は $f(x) = 0$ の根である。
x_3についても同様である。　（解終わり）

問 20.　順次、問 1 から問 3 まで問題を出しては解いてゆくことにする。
問 1）「最後から 2 番目に添加すべき根号も原方程式の根の有理式で表される」の証明は分かり難いものであ っ た。4 次方程式は実際に解けるのであるから、この定理の証明を 4 次方程式を使 っ てなぞることが出来る筈である。定理の証明中にある式 (**??**) (即ち、$F(y) = \prod_{\sigma\in S_4}(y - \sigma y_o)$ を作り、最後から 2 番目に添加する u_1が根、x_1, x_2, x_3, x_4の有理式になることを説明せよ。
解　$R_5 = R_3(u_1, u_2) = R_4(u_2)$　まで拡大して、はじめて根 x_1が含まれた。すると、u_2は x_1, x_2, x_3, x_4の有理式で書ける。
$\because$　u_2は 2 乗根であるから、

$$x_1 = r_0 + r_1u_2$$

と表される。ここで $r_1 = 1$ と出来るから、（u_2を添加する代わりに、r_1u_2を添加すればよい。）

$$x_1 = r_0 + u_2$$

$r_0 - u_2$も根であるから、これを x_2とする。

$$x_2 = r_0 - u_2$$

r_0, u_2を解いて、

$$r_0 = \frac{1}{2}(x_1 + x_2)$$
$$u_2 = \frac{1}{2}(x_1 - x_2)$$

R_4に拡大して初めて r_0を含んだ筈である。（さもなければ、R_4への拡大が不要となる。定理の証明参照。）この r_0を y_0とおき、

$$F(y) = \prod_{\sigma\in S_4}(y - \sigma y_o) = 0$$

を求める。
$\sigma \in S_4$は 24 個ある。これを全部求める。

$$(1,2)(x_1 + x_2) = x_2 + x_1$$
$$(1,3)(x_1 + x_2) = x_3 + x_2$$
$$(1,4)(x_1 + x_2) = x_4 + x_2$$
$$(2,3)(x_1 + x_2) = x_1 + x_3$$
$$(2,4)(x_1 + x_2) = x_1 + x_4$$
$$(3,4)(x_1 + x_2) = x_1 + x_2$$

$(1,2,3)(x_1+x_2)=x_2+x_3$
$(1,2,4)(x_1+x_2)=x_2+x_4$
$(1,3,4)(x_1+x_2)=x_3+x_2$
$(2,3,4)(x_1+x_2)=x_1+x_3$
$(1,3,2)(x_1+x_2)=x_3+x_1$
$(1,4,2)(x_1+x_2)=x_4+x_1$
$(1,4,3)(x_1+x_2)=x_4+x_3$
$(2,4,3)(x_1+x_2)=x_1+x_4$
$(1,2,3,4)(x_1+x_2)=x_2+x_3$
$(1,2,4,3)(x_1+x_2)=x_2+x_4$
$(1,3,2,4)(x_1+x_2)=x_3+x_4$
$(1,3,4,2)(x_1+x_2)=x_3+x_1$
$(1,4,2,3)(x_1+x_2)=x_4+x_3$
$(1,4,3,2)(x_1+x_2)=x_4+x_1$
$(1,2)(3,4)(x_1+x_2)=x_2+x_1$
$(1,3)(2,4)(x_1+x_2)=x_3+x_4$
$(1,4)(2,3)(x_1+x_2)=x_4+x_3$

結局、次の 6 個しかない。

x_1+x_2
x_1+x_3
x_1+x_4
x_2+x_3
x_2+x_4
x_3+x_4

つまり、$F(y)$ は 24 次式であるが、実質的な部分は 6 次式。

$-a=x_1+x_2+x_3+x_4$
$u_1=x_1+x_2-x_3-x_4$
$u_2=x_1-x_2+x_3-x_4$
$u_3=x_1-x_2-x_3+x_4$

とおくと、上の 6 式は、

$x_1+x_2=(1/2)(-a+u_1)$
$x_1+x_3=(1/2)(-a+u_2)$
$x_1+x_4=(1/2)(-a+u_3)$
$x_2+x_3=(1/2)(-a-u_3)$
$x_2+x_4=(1/2)(-a-u_2)$
$x_3+x_4=(1/2)(-a-u_1)$

と表される。これを $F(y)$ の式に代入すると、

$F(y)=(y-\frac{1}{4}(-a+u_1))(y-\frac{1}{4}(-a+u_2))(y-\frac{1}{4}(-a+u_3))(y-\frac{1}{4}(-a-u_3))(y-\frac{1}{4}(-a-u_2))(y-\frac{1}{4}(-a+u_1))$

$y+\frac{1}{4}a=t$ とおいて、

$F(y)=(t-\frac{1}{4}u_1)(t-\frac{1}{4}u_2)(t-\frac{1}{4}u_3)(t+\frac{1}{4}u_3)(t+\frac{1}{4}u_2)(t+\frac{1}{4}u_1)$

$=(t^2-\frac{1}{16}u_1^2)(t^2-\frac{1}{16}u_2^2)(t^2-\frac{1}{16}u_3^2)$

$=t^6-\frac{1}{16}(u_1^2+u_2^2+u_3^2)t^4+\frac{1}{16^2}(u_1^2u_2^2+u_1^2u_3^2+u_2^2u_3^2)t^2-\frac{1}{16^3}u_1^2u_2^2u_3^2$

$u_1^2+u_2^2+u_3^2=A$

$u_1^2u_2^2+u_1^2u_3^2+u_2^2u_3^2=B$

$u_1^2u_2^2u_3^2=C^2$

とおいて、

$F(y)=t^6-\frac{1}{16}At^4+\frac{1}{16^2}Bt^2-\frac{1}{16^3}C^2$

$t=y+\frac{1}{4}a$ に戻して、

$F(y)=\big(y+\frac{1}{4}a\big)^6-\frac{1}{16}A\big(y+\frac{1}{4}a\big)^4+\frac{1}{16^2}B\big(y+\frac{1}{4}a\big)^2-\frac{1}{16^3}C^2$

計算に気を取られて最初の問題を忘れていてはいけないので、再び説明をつける。即ち、

方程式、

$F(y)=\big(y+\frac{1}{4}a\big)^6-\frac{1}{16}A\big(y+\frac{1}{4}a\big)^4+\frac{1}{16^2}B\big(y+\frac{1}{4}a\big)^2-\frac{1}{16^3}C^2$

を解くために、$F(y)$ の係数からなる体 R_1（これは原 4 次方程式の係数のなす体と同じ。）を拡大して、

$$R_1\subset R_2\subset R_3\subset R_3(u_1)=R_4$$

まで来て初めて $r_0=(1/2)(x_1+x_2)$ を含む。即ち、最後に添加した u_1は方程式 $F(y)=0$ の根の有理式。

即ち、u_1は、$x_1+x_2, x_1+x_3, x_1+x_4, x_2+x_3, x_2+x_4, x_3+x_4$の有理式。

即ち、u_1は、x_1, x_2, x_3, x_4の有理式。　（問 1 の解終わり）

問 2）再び 4 次方程式を使い、また $R_3(u_1)=R_4$から出発してもう一つ遡ってみよ。

解　u_1は 2 乗根。故に、

$F(y)=(y+\frac{1}{4}a)^6-\frac{1}{16}A(y+\frac{1}{4}a)^4+\frac{1}{16^2}B(y+\frac{1}{4}a)^2-\frac{1}{16^3}C^2$

の根、$(1/2)(x_1+x_2)$ は、

$$(1/2)(x_1+x_2)=s_0+u_1\quad（s_0\text{は }R_3\text{の元。}）$$

また、s_0-u_1も根。これを、$F(y)=0$ の他の適当な根、といっても、この根は R_4 に含まれていなければならない。従って、$(1/2)(x_1+x_2)$ の他には $(1/2)(x_3+x_4)$ しかない。従って、$(1/2)(x_3+x_4)$ とおく。即ち、

$$(1/2)(x_3+x_4)=s_0-u_1\quad（s_0\text{は }R_3\text{の元。}）$$

すると、

$$s_0=(1/4)(x_1+x_2+x_3+x_4)$$

となり、s_0が R_1に属してしまう。また、この他には s_iは存在しない。定理の証明には、「もし全ての r_iがその一つ前の体に属さないならば、その拡大は無

意味となるから、必ず $r_i(i=0,2,\cdots,p-1)$ の中に一つ前の体に属すものがある。」と説明しているが、ここではこれが適用出来ない。この例の場合、R_3の拡大が不要かというと、とんでもないことで、R_3の拡大がなければ u_1^2 がない。従って、R_4で u_1^2を開平することも出来ない。故にここでは、y_0として、u_1^2を採用するのが適切であるし、また他には証明の方法がない。（従って、定理の証明は少し変更せねばならない。即ち、「$r_i(i=0,2,\cdots,p-1)$ のいずれも R_{k-1}に属さない場合は、α^pを y_0とする」と。）即ち、

$$y_0 = u_1^2 = (1/4)^2(x_1+x_2-x_3-x_4)^2$$

とする。さて、σy_0を計算する。

$$(1,2)y_0 = (1/4)^2(x_2+x_1-x_3-x_4)^2 = (1/4)^2u_1^2$$
$$(1,3)y_0 = (1/4)^2(x_3+x_2-x_1-x_4)^2 = (1/4)^2u_3^2$$
$$(1,4)y_0 = (1/4)^2(x_4+x_2-x_3-x_1)^2 = (1/4)^2u_2^2$$
$$(2,3)y_0 = (1/4)^2(x_1+x_3-x_2-x_4)^2 = (1/4)^2u_2^2$$
$$(2,4)y_0 = (1/4)^2(x_1+x_4-x_3-x_2)^2 = (1/4)^2u_3^2$$
$$(3,4)y_0 = (1/4)^2(x_1+x_2-x_4-x_3)^2 = (1/4)^2u_1^2$$

etc　で、$F(y)$ の因子で異なるものは 3 個。従って $F(y)=0$ は、

$$F(y) = (y-\frac{1}{16}u_1^2)(y-\frac{1}{16}u_2^2)(y-\frac{1}{16}u_3^2)$$
$$= y^3 - \frac{1}{16}Ay^2 + \frac{1}{16^2}By - \frac{1}{16^3}C^2 = 0$$

諄いが、説明を繰り返す。
方程式、

$$F(y) = (y-\frac{1}{16}u_1^2)(y-\frac{1}{16}u_2^2)(y-\frac{1}{16}u_3^2)$$
$$= y^3 - \frac{1}{16}Ay^2 + \frac{1}{16^2}By - \frac{1}{16^3}C^2 = 0$$

を解くために、$F(y)$ の係数からなる体 R_1（これは原 4 次方程式の係数のなす体と同じ。）を拡大して、

$$R_1 \subset R_2 \subset R_2(u)$$

まで来て初めて $(1/4)^2u_1^2 = (1/4)^2(x_1+x_2-x_3-x_4)^2$を含む。即ち、最後に添加した u は方程式 $F(y)=0$ の根の有理式。
即ち、u は、$(1/4)^2u_1^2, (1/4)^2u_1^2, (1/4)^2u_1^2$の有理式。
即ち、u は、x_1,x_2,x_3,x_4の有理式。　(問 2 の解おわり)

次にその前の段階であるが、4 次方程式でやると変数が煩雑になるだけなので、3 次方程式で実行する。即ち、問 3）は、

問 3）　3 次方程式、

$$x^3 + ax^2 + bx + c = 0$$

は、その係数のなす体 R_1を拡大して、

$$R_1 \subset R_1(\sqrt{-27D}) \subset R_1(\sqrt{-27D}, u)$$

となって初めて、根 x_1を含む。その一つ前の拡大で添加した$\sqrt{-27D}$が、根 x_1,x_2,x_3 の有理式になることを説明せよ。

解　u は 3 乗根だから、x_1は、

$$x_1 = r_0 + u + r_2u^2$$

とかける。$r_0+\omega u+r_2\omega^2u^2$も $r_0+\omega^2u+r_2\omega u^2$も根となるから、これを x_3, x_2 とおく。（後の計算が見慣れたものとなるので、この順にする。）即ち、

$$x_2 = r_0 + \omega^2u + r_2\omega u^2$$
$$x_3 = r_0 + \omega u + r_2\omega^2u^2$$

r_iを逆に解いて、

$$r_0 = \frac{1}{3}(x_1 + x_2 + x_3)$$
$$u = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3)$$
$$r_2u^2 = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$$

$x_1 + \omega^2x_2 + \omega x_3$を v とおく。即ち、

$$v = x_1 + \omega^2x_2 + \omega x_3$$

すると、

$$r_2 = \frac{v}{3u^2}$$

r_0は R_1の元。残りの r_iは r_2しかない。従って r_2は、R_2の元。これを y_0とおいて、$F(y)$ を作る。

「uv は対称式、u^3は偶置換では変化しない」ことを利用して、

$$y_0 = r_2 = \frac{uv}{3u^3}$$

と変形してσy_0を計算する。

$$(1,2)y_0 = \frac{uv}{3v^3}$$
$$(1,3)y_0 = \frac{uv}{3v^3}$$
$$(2,3)y_0 = \frac{uv}{3v^3}$$

であるから、$F(y)$ は実質 2 次式で、

$$F(y) = \left(y - \frac{uv}{3u^3}\right)\left(y - \frac{uv}{3v^3}\right)$$
$$= y^2 - \frac{A}{3C^2}y + \frac{1}{C}$$

諄いが、再び説明を繰り返す。

方程式、

$$F(y) = y^2 - \frac{A}{3C^2}y + \frac{1}{C}$$

を解くために、$F(y)$ の係数からなる体 R_1（これは原 3 次方程式の係数のなす体と同じ。）を拡大して、

$$R_1 \subset R_2(\sqrt{-27D})$$

まで来て初めて$\frac{v}{3u^2}$を含む。即ち、最後に添加した$\sqrt{-27D}$は方程式 $F(y) = 0$ の根の有理式。

即ち、$\sqrt{-27D}$は、$\frac{v}{3u^2}, \frac{u}{3v^2}$の有理式。

即ち、u は、x_1, x_2, x_3の有理式。（問 2 の解終わり）

蛇足　以下、老婆心のため付け加えておく。

4 次方程式の根 x_1は、

$x_1 = r_0 + r_1 u_2$(r_0, r_1は、R_4の元)

と表される、と書いたが、これが無理ではないかと疑問を持つ人に。

$$\begin{aligned} x_1 &= (1/4)(x_1 + x_2 + x_3 + x_4) + (1/4)(x_1 + x_2 - x_3 - x_4) \\ &\quad + (1/4)(x_1 - x_2 + x_3 - x_4) + (1/4)(x_1 - x_2 - x_3 + x_4) \\ &= (1/4)(-a + u_1) + (1/4)(u_2 + u_3) \\ &= (1/4)(-a + u_1) + (1/4)(1 + \frac{u_3}{u_2})u_2 \\ &= (1/4)(-a + u_1) + (1/4)(1 + \frac{u_1 u_3^2}{u_1 u_2 u_3})u_2 \end{aligned}$$

右辺の第 1 項が R_4に属すことは自明。第 2 項の u_2の係数は、u_3^2が R_3に属し、$u_1 u_2 u_3$が R_1に属すから大丈夫。

これで *Abel* による「5 次方程式の代数解の不可能性の証明」を全て終った。