数学入門公開講座

昭和63年８月２日（火）から８月11日（木）まで

京都大学数理解析研究所

昭和63年度(第11回)数学入門公開講座テキスト(京都大学数理解析研究所, 昭和63年8月8日～8月11日開催)

数学入門公開講座

講師及び内容

1. 演算子法の話（7時間）　京都大学数理解析研究所・教授　松　浦　重　武

微分・積分などの解析的な計算を、たんに記号の掛け算や割り算として取扱い、微分方程式の解法などを記号の形式的代数計算ですませるのが演算子法である。その歴史は19世紀のはじめ頃までさかのぼるらしいが、イギリスの電気工学者ヘビサイドが組織的に使用してから普及したので、ヘビサイド算法ともいわれる。

ヘビサイド算法は、正しい答を素早く求める便利な方法であったが、数学的基礎づけを持たなかった。

今世紀になってから、ラプラス変換による基礎づけが行われたが、簡明さが失われ、適用範囲にも制限がついた。ところで1950年頃、ポーランドの数学者ミクシンスキーは、ヘビサイドの簡明さをそのまま保つ基礎づけに成功した。

今回は、ミクシンスキーの方法によって演算子法の入門的な部分を解説する。

2. 無限大の自由度と対称性（7時間）　京都大学数理解析研究所・助教授　三　輪　哲　二

可解格子模型とモジュラー函数、無限次元リー環の関係について基本的な例を中心に解説する。

3. 結び目の話（7時間）　京都大学数理解析研究所・教授　島　田　信　夫

3次元空間における閉曲線である結び目の同位型分類は、直感的に捉え易いものとして、恐らく昔から考えられた問題であろう。そしてこの問題は、オイラーの曲面定理などとともに、位相幾何と呼ばれる数学分野が創られる要因になった。ここでは、関連する絡み輪、組み紐群の話をまじえて、この方面における最近の進展にも触れたい。

4. 代数方程式について（7時間）　京都大学数理解析研究所・教授　一　松　　信

代数方程式は古くて新しい問題である。古典的な代数的解法を見直すとともに、数値解法と合せて考察してみたい。

時　間　割

日 / 時間	8月2日(火)	3日(水)	4日(木)	5日(金)	6日(土)	7日(日)	8日(月)	9日(火)	10日(水)	11日(木)
13:15～15:00	松浦	松浦	松浦	松浦	休		島田	島田	島田	島田
15:00～15:15	休憩						休憩			
15:15～17:00	三輪	三輪	三輪	三輪	講		一松	一松	一松	一松

4. 代数方程式について（7時間）

京都大学数理解析研究所・教授 一 松 信

1988, AUGUST 8, 9, 10, 11 15:15 - 17:00

代数方程式について

京都大学数理解析研究所／一松　信

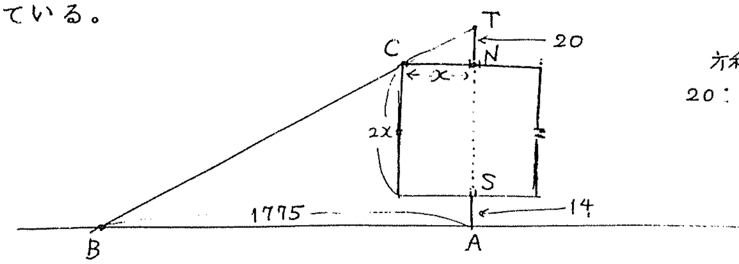
要旨：　代数方程式を解くことは、古くて新しい問題である。　古代から扱われているが、代数的解法は限られた場合にしか使えない。　数値解法も、計算機が発展した今日でさえ（あるいは今日かえって）容易でない。　その辺の事情と、近年の研究を解説する。

目次

I　特別な方程式

1．1　2次方程式

2次方程式は、古代バビロニヤの粘土板にもあるし、古代中国の『九章算術』にも出ている。



方程式：
$20 : x = (34+2x) : 1775$

「図のように、正方形の城壁で囲まれた都市がある。　各辺の中央に門がある。北門から北20歩に木がある。　南門から14歩南の地点を通る東西一直線の道路に沿って、南門の正面から西へ1775歩進んだ所で、城壁の北西の角に北の木が見えた。　城壁の大きさはいくらか？」

一辺を$2x$とすると、2次方程式 $x^2+17x-17750=0$ 　になり、正の解として

$$x=125,\ 2x=250$$

をうる。　今では簡単だが、これは恐らく戦国時代に、城の大きさを遠隔測定する高度のスパイ技術(?) だったのだろう。

2次方程式の解の公式は有名だが、IIにおいて、対称式の立場から再考する。

1．2　3次方程式

3次方程式の問題も、2つの2次曲線の交点として、あるいはアナログ的な方法により、古代ギリシャ時代から扱われている。　中世アラビア科学圏において、かなりの研究があったが、当時は負の数がなかったので、係数の正負に応じて細かく分類して扱っている。

15世紀になって、タルタリヤ・カルダノの解法が知られた。　それはIIで述べるラグランジュの解法と、本質的に同じものである。

ここではわざと趣を変えて、三角関数の倍角定理を基礎にして扱ってみる。

3次方程式 $a_3x^3+a_2x^2+a_1x+a_0=0$ において、未知数を $x+a_2/3a_3$ に置換えると、x^2の係数を0にすることができる。それで以下3次方程式の標準形として

$$x^3+3px+2q=0$$

を採用する。

三角関数の加法定理から、次の3倍角の公式がでる。

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

p>0 の場合には、左辺が単調増加なので、実解は一つしかない。そこでまず3実解を持つ可能性のある場合として、p<0 のときを扱う。

このとき $\rho=2\sqrt{-p}$, $t=x/\rho$ と置くと、$4t^3-3t-a=0$, $a=q/(-p)^{3/2}$ となる。ここで $|a|\leq 1$ ならば3実解がある。逆三角関数の主値により、

$$\alpha = \arccos a \qquad (0\leqq\alpha\leqq\pi)$$

とおくと、$x=\rho\cos(\alpha/3), \rho\cos(\alpha/3+2\pi/3), \rho\cos(\alpha/3+4\pi/3)$ が3実解である。これは関数電卓で簡単に計算できる。

ここで $|a|>1$ のときには、自然に解析接続をして（$-x$ をとれば $a>1$ としてよい）

$$\arccos a = i\ \mathrm{arcosh}\ a = i\log(a+\sqrt{a^2-1})$$

と解釈できる。したがって $A=\mathrm{arcosh}\ a$ と置くと、$x_0=\rho\cosh(A/3)$ が唯一の実解であり、

$$-\frac{x_0}{2} \pm i\frac{\sqrt{3(px_0-2q)}}{2x_0}$$

が一対の共役複素解である。

p>0 の場合にも類似の解釈が可能だが、この場合には直接タルタリヤ・カルダノの解法を利用したほうが早い。このような解法を紹介したのは、楕円関数による5次方程式の解法の雛形であることを考慮したためである。

今一つ別の考え方がある。それはチルンハウス変換により、さらに xの係数をも0にして、$x^3+a=0$ の形に直す方法である。これについては、III (3.2)で 改めて解説する。

1．3　2元2次連立方程式

2元2次連立方程式を解くのは、2つの2次曲線の交点を求めることである。

一方が1次式ならば、1つの変数について解いて代入すればよい。　また一方の2次式が2つの一次式の積に因数分解できれば、そのおのおのの1次式と連立させればよい。

一般のときには、両者の一次結合をとり、それが2つの1次式の積に因数分解できるようにする。　そのためには、つぎの定理が基本的である。

定理　2元2次式　$ax^2+2hxy+by^2+2gx+2fy+c$　が2つの1次式の積

$$(Ax+By+C)(Dx+Ey+F)$$

に因数分解できるための必要十分条件は、2次形式の係数行列式

$$\begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix} = 0$$

である。

証明　係数の間の関係は、次の通りである。

$$a=AD,\ 2h=AE+BD,\ b=BE,\ 2g=AF+CD,\ 2f=BF+CE,\ c=CF$$

必要なことは、これらを行列式に代入して計算すればできる。

十分のほうは、まず2次式として　$ax^2+2hxy+by^2=(Ax+By)(Dx+Ey)$　と因数分解する。

(i) $A:B\neq D:E$ のとき。　g,f の関係式を、C,F に関する連立1次方程式と見て解く。　このとき最後の式　$c=CF$　は、行列式が0という条件から、自動的に満たされる（検算に利用できる）。

(ii)　$A:B=D:E$ のとき。　2次の項が完全平方式になるが、このときには条件から式全体が　$z=Ax+By$　の2次式に変形できるので、それを因数分解すればよい。

この証明は、単なる存在証明でなく、条件が満たされたとき具体的に因数分解の計算をする算法をも示している。

１．４　４次方程式

以下に述べるのは、本質的にはフェラーリの元の考え方に沿うものである。

４次方程式において、$y=x^2$ と置いて、x,y の２元２次式に直す。　但し x^2 の項にパラメタλを入れて、全体を次のように表し、これが２つの１次式の積に因数分解できるようにパラメタλを決める。

$$a_4x^4+a_3x^3+a_2x^2+a_1x+a_0=ax^4+bx^3+cx^2+dx+e$$
$$=ay^2+bxy+(c-\lambda)x^2+\lambda y+dx+e$$

前節の定理により、その条件は次の３次方程式で表される。

$$\lambda^3-c\lambda^2+(bd-4ae)\lambda+4ace-ad^2-eb^2=0$$

これを解き、その解λを代入して x,y に関する２つの１次式をうれば、それらは０とおいた xに関する２つの２次方程式を解けばよい。

ここでλは３つ出るが、そのどれを使っても、４つの解の組合せが変って現れるだけであって、全体としては同じ４個の解をうる。　もっとも実係数の場合に、うまいλを取らないと、複素数係数の２次方程式を解く羽目に陥ったりする。

(４つの解を x_1,x_2,x_3,x_4 とするとき，３つのλはそれぞれ $x_1x_2+x_3x_4$，$x_1x_3+x_2x_4$，$x_1x_4+x_2x_3$ に相当する。)

なおオイラーは、この方法を真似して一般に2^n次の多項式が2 個の2^{n-1}次多項式の積に因数分解できることを示して、方程式論の基本定理を証明しようとした。

その着想は面白いが、８次以上の場合には本質的な難点があることをラグランジュとガウスとが指摘している。　ガウスは最初はそれを修正しようと努力したらしいが、結局まったく新しい証明を考えた。

以上の解法は、それぞれの次数について、まったく「その場限り」の方法であるが、対称式の性質を使うと、ある程度統一的に扱うことができる。　ラグランジュによるその考えを次に述べる。

II　代数的解法を巡って

2．1　対称式の性質と応用

（i）対称式の基本定理　n変数 $x_1,\ldots,x_n$ の多項式で、変数をどのように入換ても全体として不変なものを対称式という。そのうち単項式

$$x_1^{e_1}\cdots x_n^{e_n}\text{（これを }[e_1,\ldots,e_n]\text{ と記す）}$$

を基にして、可能な限りの変数の置換を施し、その全部を加えてできる対称式を、それから生成された単純対称式といい、それにも上の記号を転用する。単純対称式を生成する単項式は、次数が減少する順序に並んだ式を代表としてよい。

単純対称式を表現する記号 $[e_1,\ldots,e_n]$ に、辞書式順序を入れる。すなわち e_1 が大きいものを大きいとし、それが同じならば e_2 で比べ、以下同様にする。この順序は次の性質を満たす。

1°.全順序である。　2°.積が順序を保存する。　3°.無限減少列はない。

この順序で最も小さい単純対称式は、順次

$$[1,0,\ldots,0],[1,1,0,\ldots,0],\ldots,[1,1,\ldots,1]$$

である。これらを基本対称式という。詳しくいうと、1がk 個のものは、

$S_k=\Sigma\{x_1,\ldots,x_n$ からk 個とって掛けた項$\}$ 可能な$\binom{n}{k}$個の組合せ全部に対し ── で表される。

基本定理　任意の対称式は、基本対称式の多項式として表される。

証明は下に述べる。

代数方程式の解と係数との関係は、

$$(t+x_1)\cdots(t+x_n)=t^n+S_1t^{n-1}+\cdots+S_{n-1}t+S_n$$

で表される。したがって解（根）の対称式は、元の方程式の係数で表現できる。

基本定理の証明　単純対称式 $[e_1,\ldots,e_n]$ について示せばよい。

$$e_1\geqq\cdots\geqq e_n \text{ とするとき } S_1^{e_1-e_2}S_2^{e_2-e_3}\cdots S_{n-1}^{e_{n-1}-e_n}S_n^{e_n}$$

を引けば、上の順序について前のよりも小さい項だけからなる対称式になる。それを単純多項式の和に分けて、同じ操作を反復すれば、有限回で残りがなくなる。

例　$[k,0,\ldots,0]=P_k$ と置くとき $P_2=S_1^2-2S_2$, $P_3=S_1^3-3S_1S_2+3S_3$.

(ii)ニュートンの公式　上記の累乗の和 P_k を基本対称式で表す（あるいはその逆）の公式を、ニュートンの公式という。　それには次のような母関数を利用する求め方がある。

前記の解と係数との関係式を対数微分すると

$$\frac{nt^{n-1}+(n-1)S_1t^{n-2}+\cdots+S_{n-1}}{t^n+S_1t^{n-1}+\cdots+S_{n-1}t+S_n}=\frac{1}{t+x_1}+\frac{1}{t+x_2}+\cdots+\frac{1}{t+x_n}$$

となるが、右辺の $1/(t+x_j)$ を展開してまとめると

$$\frac{1}{t}\left[n-\frac{P_1}{t}+\frac{P_2}{t^2}-\frac{P_3}{t^3}+\cdots\right]$$

となる。　分母を払って整理すると

$$S_1t^{n-1}+2S_2t^{n-2}+\cdots+(n-1)S_{n-1}t=(t^n+S_1t^{n-1}+\cdots+S_n)\left[\frac{P_1}{t}-\frac{P_2}{t^2}+\frac{P_3}{t^3}-\cdots\right]$$

となり、これから次の漸化式をうる。　それを順次 P_k または S_k について解けばよい。

$$S_1=P_1,\quad 2S_2=P_1S_1-P_2,\quad 3S_3=P_1S_2-P_2S_1+P_3,\ \cdots$$

P_k について解くと，$P_1=S_1$，$P_2=S_1^2-2S_2$，$P_3=S_1^3-3S_1S_2+3S_3$，$\cdots$

なお個々の式は有限項までで済むから、形式的展開の収束は問題にしなくてよい。

2．2　対称式によるラグランジュの解法

(i) 2次方程式　解 x_1, x_2 の和は基本対称式 S_1 である。　差 x_1-x_2 は対称式ではないが、2乗すれば対称式になり、$S_1^2-4S_2$ と表される。　後者の平方根をとり、前者との和と差を作ればよい。　結果はおなじみの解の公式そのものである。

(ii)　3次方程式　1の虚3乗根を　$\omega=(-1+i\sqrt{3})/2=\exp(2\pi i/3)$　と置き、

$$y_1=x_1+\omega x_2+\omega^2x_3,\quad y_2=x_1+\omega^2x_2+\omega x_3$$

と置く。　$\omega^2+\omega=-1$　に注意すると

$$x_1=(S_1+y_1+y_2)/3,\quad x_2=(S_1+\omega^2y_1+\omega y_2)/3,\quad x_3=(S_1+\omega y_1+\omega^2y_2)/3$$

である。 積 $y_1 y_2$ は対称式であり、 $S_1^2-3S_2$ と表される。 また

$$y_1^3=x_1^3+x_2^3+x_3^3+6x_1x_2x_3+3\omega(x_1^2x_2+x_2^2x_3+x_3^2x_1)+3\omega^2(x_2^2x_1+x_3^2x_2+x_1^2x_3)$$

は対称式ではないが、$y_1^3+y_2^3$ は対称式であり、

$$2S_1^3-9S_1S_2+27S_3$$

と表される。 ゆえに2次方程式を解いて y_1^3, y_2^3 がわかり、その3乗根から x_k が求められる。

3次方程式を $x^3+3px+2q=0$ と標準化すれば、$(y_1/3)^3, (y_2/3)^3 = t$ はともに

$$2次方程式\quad t^2+2qt-p^3=0$$

の解になり、タルタリア・カルダノの公式による解

$$x_1=u+v,\quad x_2=\omega^2u+\omega v,\quad x_3=\omega u+\omega^2v;\quad u=(-q+\sqrt{q^2+p^3})^{1/3},\quad v=(-q-\sqrt{q^2+p^3})^{1/3}$$

をうる。 ここで $q^2+p^3<0$ のときには3実解なのに、複素数の3乗根を計算しなければならない。 いわゆる「不還元の場合」であるが、このとき実数の3乗根のみで解くことはできない（次項参照）。

(iii) 4次方程式　4つの解 x_1, x_2, x_3, x_4 に対して、

$$y_1=x_1x_2+x_3x_4,\ y_2=x_1x_3+x_2x_4,\ y_3=x_1x_4+x_2x_3$$

と置くと、これらの基本対称式は、x_k に関する対称式になり、3次方程式を解いて求められる。 計算は略すが、その具体形はIで述べた式と同じになる。

y_1 がわかった後は、まず x_1x_2 と x_3x_4 とのS_4が既知なので、x_1x_2 と x_3x_4 とが求められる。 ゆえに

$u=x_1+x_2,\ v=x_3+x_4$ に対し　$u+v=S_1,\ x_3x_4u+x_1x_2v=S_3$ という関係式が成立し、これを u, v の連立1次方程式として解けば、x_1, x_2 と x_3, x_4 とをそれぞれ2次方程式の解として求めることができる。

重複解の場合など多少の修正がいるが、この解法はIで述べたものと結果的には同一になる。

以上のラグランジュの考えは巧妙だが、y_i の式などの置き方が天下り的であって、必然性がはっきりしない欠点がある。

2．3　3次方程式の不還元な場合

実係数の3次方程式が相異る3実解をもつとき、それを代数的に解くには複素数の3乗根を計算しなければならない。 そのことは前記の解の公式からわかる。

すなわち　x_1, x_2, x_3 がすべて相異る実数ならば、 y_1, y_2 は互いに共役な複素数でなければならず、それらの3乗も複素数である。

もちろんこれだけでは、厳密でないという異論があるだろう。 前の解法が悪かったのであり、もっとうまい公式を見附ければ、実数の3乗根だけで解けるのではないかという「ものいい」である。

これに完全に答えるのには、代数方程式のガロアの理論を論じなければならないが、大ざっぱにいうと次の通りである。 四則演算が普通にできる（0で割ることを除く）数の体系を体という。 代数的解法とは、基礎になる係数体（例えば有理数体）に次々に累乗根を添加して体を拡大し、有限回の後についに元の方程式の解が、拡大した体に含まれるようにする操作なのである。

前の公式からわかることは、3実解をもつ3次方程式の解が、それ自身は実数であるにもかかわらず、複素数の3乗根を添加した体に含まれているということである。 もしも実数の累乗根だけで解けるものならば、その解は実数の累乗根のみを添加してできる「実代数体」に含まれていなければならない。 しかし両者の構造が違うので、そのようなことはありえない。

もちろん実用的には、3実解をもつ3次方程式は、いまやⅠで述べたように三角関数を使って簡単に解くことができる。

2．4　5次以上の代数方程式について

ルネサンス期に3次・4次方程式の解法が見付かったあと、5次方程式が大問題になった。 多くの研究があったが、いずれも6次方程式に帰着してしまった。

19世紀になると、代数的解法がないのではないかという疑いが生じ、結局アーベル・ガロアの研究によってそれが証明されたことは、周知である。

「群論がガロアに始まる」という定説には、多少の注釈がいる。 確かに代数方程式に対するガロア群の発見は画期的であった。 それにより代数学の中心課題が、代数方程式から群（及び一般の代数系）に移ったのである。 しかし群の

考えは、前記ラグランジュの研究にはっきり現れているし、コーシーも積極的に活用して研究している。

一これは一般に、大発見の先駆になった研究者の業績をどう評価すべきかという課題であろう。

この講義の主題は、ガロアの理論や、5次代数方程式が代数的に解けないことの証明ではないので、この事実の証明にはこれ以上触れない。 ガロアの理論の解説書は多数あるし、アーベル・ガロアの論文の翻訳もある。 高木貞治『代数学講義』（共立出版）には、ほぼアーベルの最初の研究の線に沿う証明が載っている。

19世紀の中頃になって、エルミート・クロネッカー・ブリオスキ及びクラインらが、楕円関数を使って一般の5次方程式を解く公式を与えた。 それらは今ではほとんど忘れられてしまったが、楕円テータ関数を利用すると、数値計算にも有用な方法のようであり、今一度見直す必要がありそうである。

一これを話したかったのだが、楕円関数に関する準備が多量に必要なので諦めた。

ところで超越関数を使えば、6次方程式も解けるか？ 結論は否定的である。

5次方程式から導かれる「ヤコビの6次方程式」は楕円関数によって解けるが、これは5次方程式に帰着できるので、むしろ当然である。 それ以外の一般6次方程式は、1変数の解析関数だけでは解けない。

一般の7次方程式が2変数解析関数のみでは解けないだろうというのが、ヒルベルトの第13問題である。 この問題は、ソ連のアーノルドらによって「否定的」に解決されたことになっている。 しかしそれは「3変数の連続関数が、常に2変数連続関数の合成関数として表現できる」という一般的な定理であって、具体的な解の公式を与えているわけではない。 しかもヒルベルトの論文には「2変数の<u>連続</u>関数」と明記してあるが、これは「<u>解析</u>関数」のいいそこない(?)である可能性が強い。 アーノルドの使った関数は、いたる所微分できない連続関数であって、実用には程遠い。 そして7次方程式が本当に2変数<u>解析</u>関数だけで解けないかどうかについては、何等実質的な研究がない。 したがって「ヒルベルトの第13問題」は、一般的には否定的に解決されたといってよいが、実質的に

は手つかずの現状である。

III　代数方程式に関する話題

3．1　方程式論の基本定理

いわゆる方程式論(algebra) の基本定理とは、複素数体が代数的閉体という命題である。

フランスではダランベールの定理ということがあるが、これは正しくない。ダランベールが証明したことは、n次代数方程式は n個より多くの解をもちえないという定理であって、解の存在ではない。

オイラーがその証明を試みたのは事実だが、それは不完全であった。　現在の立場からいって、ほぼ完全といえる証明を初めて与えたのは、ガウスの学位論文である。　それを審査したのは、当時ドイツ一の数学者といわれたパフであり、彼は「このような素晴らしい論文を審査できた自分は幸である」といったお世辞(?) を述べている。

その証明は後述の通り構成的であり、その後近似解法として何度も再発見されている。　しかし現在の観点からみると、なお厳密性に欠けるところがあった。

ガウス自身もそれを気にしており、後年いくつかの別証明を試みている。

今日最も簡単な証明とされているのは、複素関数論のリュービルの定理を使うもの、あるいは回転指数の概念を利用するものである。　しかしこれらは「解が存在しないと仮定すると矛盾が起る」という形の、抽象的存在証明である。　このような証明法が許容されるようになってきたのは、いわゆる純粋数学が定着してきた19世紀後半以降である。　19世紀初め頃までの証明が難しかったのは、近似的にでも解を具体的に求める算法を与えたものだったからである。

一歴史は繰り返すというか、近年計算機の発展とともに、再び数学にも具体的な算法指向の傾向が強くなってきたように感ずる。

以下ガウスの最初の証明の要点を述べる。　代数方程式を

$$p(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=0,\ a_0\neq 0$$

と置く。　複素数平面上で $x=re^{i\theta}$ と置き、 rが十分大とすると、p(x)はほぼ x^n に支配される。　すなわち円周 r=c（定数）の上で、p(x)の実部・虚部は x^n のそれに近い。　したがってほぼ

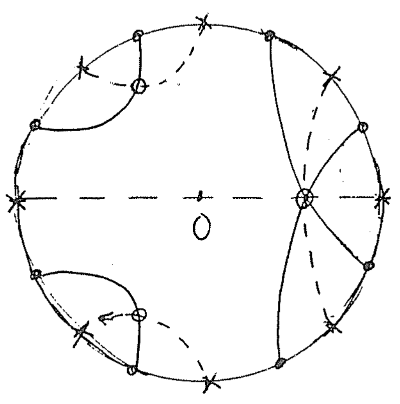
$$\theta=(2k+1)\pi/2n \text{ で実部が}0,\quad \theta=k\pi/n \text{ で虚部が}0$$

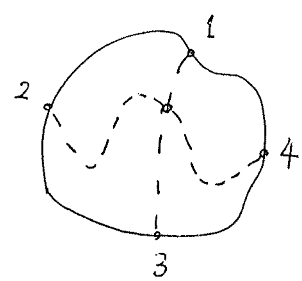
となる。　これらの点は、円周上に交互にある。 $(k=0,1,\cdots,2n-1)$

r を少し小さくすると、それらの零点も少し変るが、連続的に実部及び虚部が0になる軌跡を作る。　それらが途中で消滅することはない。　しかしr が0 に十分近ければ、$p(x)\fallingdotseq a_0\neq 0$ だから、どちらの軌跡も存在しない。　したがって大きい円周上の2n個の点から始まった軌跡は、途中で適当に融合して、離れた点同士を円内で結ぶ曲線族をなす。

ところで単純閉曲線上に４点があるとき、第１と第３の点、第２と第４の点とをその内部で結ぶ曲線同士は、必ず交わる。　ーこれはジョルダンの曲線定理から証明できる。　したがって、実部が０の曲線と虚部が０の曲線とは交わることになる。　その交点が初めの方程式の解に他ならない。

現在では、この操作によって解のごく粗い近似値を求めることは、マイコンによるグラフィックスを援用すれば、容易にできる。　数値解法に当って、解の大体の位置を調べ、粗い近似値をまず求めておくことはきわめて重要である。





3．2　チルンハウス変換

歴史は古く、16世紀にさかのぼる。

$$f(x)=a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

に対して、$y=c_0+c_1 x + c_2 x^2 + \ldots$(有限項)$=g(x)$と置き、$f(x)=0$と$g(x)-y=0$とが共有解をもつようにする。それには両者の終結式を0と置けばよい。あるいは互除法により、定数でない最大公約式を求めて0と置く。それはyについてのn次式になるが、$c_0, c_1, \cdots$をうまく選ぶと、$y^{n-1}, y^{n-2}, \ldots$の係数を0にすることができる。これがチルンハウス変換である。

1次式 $y=x+\alpha$としてy^{n-1}の係数を0にするのが、もっとも簡単な例であり、これは$\alpha=a_{n-1}/na_n$とした平行移動と同じ結果になる。次に簡単なのは、$a_n=1$, $a_{n-1}=0$と標準化した上で、

$$y=\alpha+\beta x+x^2,\ \alpha=2a_{n-2}/n$$

とすると、y^{n-1}の係数は0のままであり、y^{n-2}の係数はβの2次式になる。その2次方程式を解いてβを決めれば、y^{n-1}, y^{n-2}の係数が0である方程式に還元できる。

以下3次方程式について、具体的に述べよう。3次方程式を標準化して$x^3+3px+2q=0$とし、これと$x^2+\beta x+2p-y$との互除法を行う。但し2次式で割り切れるなどと欲張ると、元の方程式に戻ってしまうが、1次の剰余は

$$(y+p+\beta^2)x+2q+(2p-y)\beta$$

である。これを0と置いてxについて解き、2次式に代入して整理すると

$$y^3+3y(p\beta^2+2q\beta-p^2)-2(p^3+3p^2\beta^2+3pq\beta-q\beta^3+2q^2)=0$$

をうる。ここで$p\beta^2+2q\beta-p^2=0$, すなわち$\beta=(-q\pm\sqrt{q^2+p^3})/p$ととれば、

$$y^3=A,\ A=8(p^3+q^2)(1-q\beta/p^3)$$

の形になるので、Aの3乗根としてyが出る。それから上記の1次の剰余の式によりxを求めればよい。一般にβは2つでるが、どちらからも適切なyをとれば同一のxがでる。

但しp, q が実数でも $q^2+p^3<0$ のときにはx は３個とも実数だが、β もA も複素数となり、複素数の３乗根を計算しなければならない。

$n\geqq 4$ のとき、計算ははるかに複雑になるが、３次式にして３次方程式を解くことにより、y^{n-3} の係数をも0 にすることができる。 これは４次方程式の別の解法である。

ところでチルンハウス及びその後継者達は、最初は同様にして４次方程式を解くことにより、y^{n-4} の係数をも０にでき、それで５次方程式が解けると期待したらしい。 しかし実はy^{n-4} の係数を消すには、６次方程式を解かなければならないのであり、その期待は挫折した。 しかし５次方程式を扱うときには、チルンハウス変換により、少なくとも４乗と３乗の係数を０にして考えるのが標準である。

3．3 有限体上の代数方程式

近年有限体の上で、代数方程式を解くことが必要な場合が、しばしば生じてきた。

伝統的な数学の立場は「有限個なのだから、全部の値を代入してみて、０になるものを探せばよい」であった。 百個位ならばそれでよい。 しかし10^{50}個ともなれば、超超高速計算機を宇宙が出来てから今まで動か続けたとしても、完了しない。 ローマクラブ以後(?) 漸く数学界でも、人間の寿命も研究費も有限であり、限られた時間と手間の制約下で可能な算法が必要という雰囲気が現れている。

有限体がかえって難しいのは、その上に自然な位相(topology)がないせいだろうというのが、故高橋秀俊先生の御意見である。

４次までは代数的解法が使える。 また解に平方剰余と非剰余とが混じっていれば、

$$\mathbb{Z}_p \text{ において } \quad x^{\frac{p-1}{2}}-1 \quad , x^{\frac{p-1}{2}}+1$$

と、互除法による最大公約式を求めると、うまく次数を下げられることがある。

例えば Z_p における平方剰余は、$a^{(p-1)/2}\equiv 1$ で判定できるが、aの平方根を具体的に求めるには、次のようにする。

p が4n-1型のときには、a の奇数m=(p-1)/2 乗が1と合同になる。一般に a の奇数m 乗が1と合同ならば、

$$a^{m+1}\equiv a \pmod p) \quad \text{なので} \quad a^{(m+1)/2} \text{が平方根}$$

を与える。そうでないときには、次のRabin の算法による。

まず乱数c をとり、$x^{(p-1)/2}-1$ と $x^2-2cx+c^2-a$ との最大公約式を求める。実際には、前者を後者で割った剰余を求めればよい。それが定数になったら失敗であり、乱数を取り直して再度試みる。もし剰余が1次式 $ux+v$ になれば、Z_p での計算による $c-v/u$が平方根の一つを与える。立方根も、同様にして計算できる。

これは確率的な算法であるが、実際には最悪の場合でも、5,6 回の繰返で求められることが多く、有用な方法である。

3．4　部分終結式について

縦がm 行、横がn 列($m\leq n$) の横長行列Aがあるとする。Aをn 個のm 次元縦ベクトルa_1，．．．．，a_n と並びとみなす。そのときAに附随した多項式を

$$P(A)=\sum_{k=0}^{n-m}\det[a_1,\ldots,a_{m-1},a_{m+k}]x^{n-m-k}$$

と定義する。特別な場合として、m=n ならば行列式であり、またm=1 ならば普通の多項式そのものである。

さて２つの多項式(n>m)

$$f(x)=a_nx^n+\ldots+a_1x+a_0,\quad g(x)=b_mx^m+\ldots+b_1x+b_0$$

があるとき、f(x)にb_mの累乗を掛けて g(x) で割った剰余は、次のような行列に附随した多項式として表される。

[第１行に $a_n,\ldots,a_1,a_0$ を並べる。第２行には $b_m,\ldots,b_1,b_0$(残りには0 を補充) を並べ、以下第n-m+2 行までは、順次それを1 つずつ右へずらせて左からは０を補ったものを並べた行列。]

一般に $j=0,1,...,m-1$ について、$a_n,...,a_1,a_0$の列（残りには0を補う）を1つずつ右へずらせながら $m-j$行並べ、その下に $b_m,...,b_1,b_0$ の列を$n-j$ 行、同様に順次1つずつ右へずらせながら並べて作った行列に附随する多項式を、第j次の部分終結式(subresultant)という。

特に $j=m-1$のときは上に述べた剰余であり、$j=0$ のときは終結式 Res(f,g) として昔から知られている量である。

では中間の部分終結式が何を表すのか？　それが本質的に、f,g に互除法を施して両者の最大公約式を求める途中に現れる剰余を表すことは、以前からうすうす知られていたらしい。　しかしそれに部分終結式という名をつけ、その事実をはっきりと示したのは、コリンズ(1966)らの業績であって、意外に新しい。

コリンズは詳しい定理を与えているが、一般的に述べるとかえってわかりにくいので、わざとぼかして述べておく。

理論的に最も簡単（その代り計算は最も手間がかかる）場合は、毎回剰余の次数が1ずつ下り、最後に定数が残る場合である。　このときには第$j-k$ 次の部分終結式が、第k 回目の剰余と、定数倍の違いを無視して一致する。

もしも途中で剰余の次数が大幅に下ったり、途中で割り切れたりした場合には、対応する次数の剰余がない部分終結式は、0になるかまたは高次の項が消えて低次の式に退化する。　場合によっては、定数倍の違いを除いて同じ剰余が別のj に対して現れる。

一般に $j=0,1,...$次の部分終結式のうち、初めて0でない多項式が、最初のf, g の最大公約式を与える。　この事実から、昔から知られた定理「f,g が共通零点をもつための必要十分条件は、両者の終結式が0であること」が、容易に導かれる。

初めて0でない部分終結式によって最大公約式を求めようという算法は、普通の数を係数とする多項式に対しては、推奨できない。　行列式の計算に誤差が入って、答が0か0でないかの判定が微妙になるからである。　しかし有限体の上の多項式の場合のように、四則計算がすべて誤差なしに可能な場合には、ときとして互除法よりも早いことがある。　現れる行列に0が多く、次数が低い方の係

数列を上に並べ変えるといった工夫をすると、消去法によって簡単に行列式が計算できるからである。

IV　代数方程式の数値解法

4．1　展望

(i) 梗概　今日単に Algebra (代数学) といえば「抽象代数学」を意味する。しかしこの語は永らく「代数方程式論」を意味した。　その影響は意外と近年まで及んでいる。　今世紀の初頭に発行されたドイツの「数学百科全書」の"Algebra"の部分では、今日では信じられない程多くのページを、代数方程式の数値解法にさいている。

昔の方法の中には、例えばグレーフェの方法のように、今日の計算機の設計不備(?) のために、うまく利用できないものも多い。　全体として近年では、予備情報なしにデータを入れれば答がえられるという「ものぐさ」方式指向と、必要な予備情報をできるだけ与えて能率よく解く方法とに分かれてきたようである。

後者は予備情報なしに粗い近似値を求める方法と、粗い近似値から精度を効率よく上げる方法とに分かれる。　いずれにせよすべての代数方程式を、ただ一つの方法だけでうまく解こうという純血主義(?) は無理であり、「目的のためには手段を選ばず」をいとわずに実行する必要がある。

これからの解法としては、数式処理との併用が不可欠であろう。　解の重複度を数値的に求める算法は多数研究されており、それらは貴重だが、導関数との最大公約式を計算して利用するのを拒否すべき理由はない。

(ii) 粗い近似値を求める方法　実解に対して、これからマイコンを利用するのに最も適した方法は、関数のグラフを書いて、それがx軸と交わる点を求める手法であろう。　この目的には、グラフ全体を奇麗に書くことよりも、x軸の近くを精密に書くのを主としたプログラムが望まれる。

複素解については、等高線を書く方法もあるが、3．1で述べたガウスの証明算法を、マイコンに乗せるのがよいらしい。

ごく粗い近似から、いくらか精度を上げる目的には、二分法とはさみうち法とが推奨できる。 はさみうち法(regula falsi;直訳すれば、偽の位置)とは、関数値の符号が異る2点 a,bではさみ、a,b での値を線分で補間して、x軸との交点を次の近似とする方法である。

(iii) よい近似値から精度を高める方法　昔からニュートン法が愛用されている。 近年停止則の理論的な研究も進み、有用な方法だが大域的な収束性を持たないので、いい加減な初期値から始めるのは危険である。

実係数の代数方程式の複素解を求めるためには、以前は（今でも?)2次因数を求める2変数のニュートン法に当る、ベアストウ法（ヒッチコック法などの名もある）がよく使われた。 うまく使えば便利な方法であることは正しいが、特に大部分が実解で一対の複素解のみをもつ方程式では、よほどよい初期値から始めないと、たいてい2実解をもつ2次因子に収束してしまう。

すべての解を求めたい場合には、デュラン・ケルナー(Durand-Kerner) 法が標準になりつつある。 その由来は色々あるが、公式は次の通りである。

$p(x)=a_n x^n+a_{n-1}x^{n-1}+...+a_1 x+a_0=0$ の近似解 $x_1^{(\nu)},...,x_n^{(\nu)}$ が既知のとき

$$x_k^{(\nu+1)}=x_k^{(\nu)}-p(x_k^{(\nu)})\Big/ a_n\prod_j (x_k^{(\nu)}-x_j^{(\nu)}),$$ 積は $j\neq k$ について.

この方法は、ある意味で大域的な収束性を持つこと、重心不変性のあること(近似解の和が真の解の和 $-a_{n-1}/a_n$ に等しい）、誤差が自分自身の誤差と他の誤差の和との積という形で評価され、2乗収束である上に比較的一様であること, などの長所が多い。

3乗収束するように変形した公式も数多く知られていて、それぞれ特徴がある。ただ私のささやかな経験では、それらは数十桁以上という高精度用であって、十桁前後の普通の計算用には、まず本来のデュラン・ケルナー法を推奨する。「いくらか遅いが確実」な点を強調したい。

複素解には、よい複素数計算プログラムを用意して、複素数のニュートン法などを適用するのが最良と思う。

(iv) 次数低下について　一つの解αをえたとき、$p(x)$を$x-\alpha$で割って次数を下げる操作である。　ウィルキンソンは繰返し、そのためには絶対値の小さい解から実行せよと力説して、例をも多数あげているが、それは「多項式の割算を高次の項から行う」ことを絶対条件とした場合の話である。　平野菅保氏（当時東芝、現在日大）が指摘したように、多項式を$x-\alpha$で割るときには、手間はかかるが上と下とから割って、剰余を最大影響項（αを代入したときに絶対値が最大になる項）にしわよせするように工夫すれば、どのような大きさの解から始めても、次数低下で精度を失う心配はない。　ーこの例は、簡単な基本計算でも、伝統的な計算法にこだわらずに考えれば、工夫すべき余地が少なくないことを示している！

４．２　無平方分解と疑似無平方分解

多項式$p(x)$を既約因子の積に分解したとき、同じ項の２乗以上が現れないとき、無平方(square-free) という。　それは$p(x)=0$の解がすべて単純解であることと同じである。

$p(x)=0$　の解αが単純解であるための必要十分条件は

$$p(\alpha)=0,\ p'(\alpha)\neq 0\ ,\ p' は導関数\ dp/dx$$

である。　なおここでの導関数には、極限の概念は不要であって、形式的に x^n の導関数を nx^{n-1} と定義してよい。

これを使うと、次の定理が容易に証明できる。

定理　多項式$p(x)$が無平方であるための必要十分条件は、$p(x)$とその導関数$p'(x)$とが互いに素なことである。

多項式$p(x)$を次のように因数分解したものを、その無平方分解という。

$$p(x)=p_1(x)[p_2(x)]^2\ldots[p_\ell(x)]^\ell;$$

ここに$p_1,p_2,\ldots,p_\ell$は互いに素な無平方多項式

理論的には、$p(x)$を既約因子の積に分解して、それぞれの累乗の項をまとめれば、無平方分解になる。　しかし重要なのは、

「多項式の完全な因数分解は困難だが、その無平方分解は以下に述べるように、まったく機械的な計算でできる」ことである。

なお有理関数の不定積分の有理関数部分は、分母の無平方分解だけで機械的に計算できる（エルミートの算法）。

無平方分解の算法　1°. $p(x)$と $p'(x)$との最大公約式$d(x)$を互除法で求める。

2°. $e(x)=p(x)/d(x)$と置く。　$e(x)$と$d(x)$との最大公約式を求める。

3°. $e(x)$を$d(x)$との最大公約式で割った商が、最初の因子$p_1(x)$ である。

4°. $d(x)$を最初の$p(x)$と思って、1.～3.の操作を、無平方になる（すなわち最初の最大公約式が定数になる）まで反復すると、順次第2 以下の因子をうる。

ところで、普通の数値計算では誤差が伴うために、剰余が0になったか否かの判定が微妙である。一 A=B ?という判定はたいてい不成立であり、差の絶対値がある限界以下? という判定にしなければならない。

しかしこれを逆手にとって、適当な（かなり大きい）限界ϵをとり、剰余の係数の絶対値がすべてϵ以下になったら、割り切れたものとみなす、という近似が考えられる。　このような判定によって、「ϵに対する疑似無平方分解」ともいうべき操作が可能である。

これは代数方程式 $p(x)=0$ が近接解を持つ場合に有効である。　ϵが大きい（粗い分解能の）ときには、近接解は重複解とみなされて、疑似的な累乗の項が現れるだろう。　ϵを小さくして試みれば、近接解が分離されて無平方と判定されるかもしれない。　色々なϵについて計算して比較すれば、近接解に対する有用な情報をうることができる。

同様のことは、$p(x)=0$が虚部の絶対値の小さい一対の複素解（近接解）をもつときにも成立つ。　打切り判定用のϵをかなり大きくとって、形式的に実数のニュートン法を適用すると、大体近接解の付近で止る。　ϵを小さくすると、初めのうちは収束するように見えるが、そのうちに突然遠くに飛ぶ現象が起こる。このような場合には、そこに近接複素解があるものと判断してよい。

いずれにせよ真の解をうるには、改めてその付近を精密に計算する。

4．3　代数方程式の条件指数

条件指数という語は、もともと行列（一次変換）の誤差解析に対して使われた言葉だが、近年は次のように拡張されている。

ノルム空間Xから他のノルム空間Yへの写像fの、点xにおける条件指数とは

$$\lim_{\varepsilon\to 0}\sup_{\|h\|=\varepsilon} \|f(x+h)-f(x)\|\cdot\|x\| / \|f(x)\|\|h\|$$

で定義される量である。 いわば xに対して hだけの変移が入ったときに、像の変化の相対的な誤差を表す量である。 fが普通のn次元線型空間から同じ次元の線型空間に移す線型写像であり、それを行列Aで表現すれば、これは古典的な定義 $\|A\|\|A^{-1}\|$ と一致する。

条件指数が大きければ、fが連続であるにも拘らず、僅かの誤差が入っても像が大きく変化するという、極めて敏感な問題になる。

ウィルキンソンは、僅かの誤差でも答が大きく変る多数の実例を示したが、近年ガウチ(Gautschi)が、代数方程式の解に対する条件指数という概念を導入して、それらを理論的に説明するとともに、思いかけないような例を多数あげている。

直交多項式などをも考えるために、基底として k(=0,1,...,n)次の多項式 $p_k(x)$ をとり、代数方程式を

$$f(x)=\sum_{k=0}^{n} a_k p_k(x) = 0 \quad ; \quad a_n = 1$$

の形に置く。 このとき一つの解 $\xi^{(0)}$ に対する係数 a_ℓ の条件指数は、

$$c_\ell = \lim_{a_\ell\to a_\ell^{(0)}} \left| \frac{\xi(a)-\xi^{(0)}}{\xi^{(0)}} \Big/ \frac{a_\ell - a_\ell^0}{a_\ell^0} \right| \qquad \left[\text{他の } a_k \text{ は固定；} \xi(a) \text{ は } a \text{ に対する解}\right]$$

であり、$c_\ell (0\leq \ell < n)$の絶対値の和を解 $\xi^{(0)}$ の条件指数とよぶ。$=\sum_{k=0}^{n-1} |a_k^0 p_k(\xi^{(0)})| / |\xi^{(0)} f'(\xi^{(0)})|$

もちろん条件指数はただ一つの数にすぎないから、誤差の影響を本質的に表す量であるとしても、それを絶対視して振回すのは、「偏差値信仰」と同じような偏見である。 またガウチも多くの興味深い実例を示しているものの、理論的な裏付けが不十分な印象を受ける。 しかしそのいくつかの例は、極めて教訓的なので紹介する。

例1　$x_\nu=\nu$, $\nu=1,...,n$; n=20のときをウィルキンソンが例示し、係数に10^{-7}の誤差が入ったたけで、5 対の複素解が現れることを注意している。 nが大きいとき、最も条件指数の大きい解は、ほぼ$n/\sqrt{2}$ に当るものであって、その大きさは n=10 のとき 2.3×10^6, n=20のとき 5.4×10^{13} などである。

これらをn で割り、区間[0,1] に直して、直交多項式（第２種チェビシェフ多項式）で表現すると、条件指数は n=20 でも 1.4×10^4 程度にすぎない。 しかし区間がこれと合わない他の直交多項式で無理に表すと、ものによっては普通のx^kを使った場合よりも悪くなる。

例2　$\pm1,\pm2,...,\pm n/2$ を解とする普通の多項式では、対称性があるせいか、条件指数ははるかに小さい。 n=20 で 6.3×10^3, n=40でも 5.8×10^8 程度にすぎない。 これをn で割り、区間[-1,1]の直交多項式で表すと、さらに小さくなる：n=20 で 325程度。

例3　$2^{-\nu}$, $\nu=1,...,n$ は良性であることをウィルキンソンが示している。実際その条件指数は、上に有界(137以下) である。 もちろん計算に当っては、それらの積のような意味のある極めて小さい数が、下へのあふれとして0にされてしまわないように、注意する必要がある。

これを直交多項式で表現すると、かえって悪くなり、条件指数はn とともに増える。 他方 $2,2^2,...,2^n$ を解とする方程式を [0,∞[での直交多項式であるラゲールの多項式で表現したときは、条件指数はゆっくり増えるが、n=20で数百の程度である。

例4　1 のn 乗根を解とする二項方程式は最も条件がよくて、各解の条件指数はすべて同じ 1/nである。 他の直交多項式で表すと、極めて悪い。

他にも多くの例がある。 あるものは常識的だが、ある結果はむしろ意外である。 一ついえるのは、うまくいった例を形式的に真似しても、失敗するということである。

4．4　ホモトピー法について

ホモトピーとは（島田教授の講義にもあった通り）連続変形を意味する。 与えられた方程式を簡単に答がわかる方程式から連続変形して、解の変化を追い掛

けようという発想である。

この考えは、1970年代の初め頃に、シカゴ大学経営学部のORの専門家が、苦しまぎれ(?)に発案したものとされる。 数学的な裏付けが十分でないまま、実用算法として現場で使われた。 日本にも1970年代後半に経済学関係の本に翻訳紹介されていたが、数学者（計算機科学者・数値計算の専門家を含む）の関心をひかず、注目され始めたのはつい最近である。 予備的な知識が不要という「ものぐさ」向きであることと、並列計算が可能であることが特徴で注目をひき始め、数学的な基礎付もほぼ出来上がっている。

もっとも実例ではやはり手抜きをせずに、例えば実解の個数などを調べて、個数が合うような初期方程式をとったほうが効率的である。

元来の方法は、次の通りであった。

n次の $f(x)=0$ に対して、$d(x)=x^n-1$ （解は$\exp(2i\pi k/n);k=1,...,n$）をとり、$f(x;t)=tf(x)+(1-t)d(x)$, $0\leqq t\leqq 1$ と置いて、既知の$t=0$ のときの解から tの変化に伴って動く解を、$t=1$ まで追跡する。 ある tのときの解がわかれば、t が少し増えたときの変化は、ニュートン法などで計算できる。

問題が起るのは、途中で$f(x;t)=0$に重複解が生じて、軌跡が交差した場合である。 初期方程式$d(x)=0$をうまくとれば避けられるが、そのあたりの解析が最初は不完全だった。

1980年代になって、ホモトピー法は一般の代数方程式に対してよりも、むしろ行列の固有値問題において固有ベクトルをも計算したい場合に有用なことがはっきりした。 特に行列が対称な場合には、ホモトピー法は結果的には、19世紀から知られていた、レーリー商と逆反復法との組合せと一致することが確かめられた。

対称行列**A**に対して、ベクトル**v**のレーリー商とは

$$\mu = \mathbf{v}^T\cdot \mathbf{A}\cdot\mathbf{v} / \mathbf{v}^T\cdot\mathbf{v},\qquad \mathbf{v}^T \text{ は転置横ベクトル}$$

である。 **v**が**A**の固有ベクトルに近ければ、μは対応する固有値の極めてよい近似値になる。

逆反復法とは、Aの近似固有値λと近似固有ベクトルvとが既知のとき、

$$(A - \lambda I) \cdot x = v$$

を解くと、xはvの定数 c倍に近くて、いっそうよい近似固有ベクトルであり、$\lambda + 1/c$ がいっそうよい近似固有値になる、という事実を活用し、必要ならばこれを反復する方法である。

したがって対称行列Aに対する具体的算法は次のようになる。

1°.なるべくならば、ハウスホルダー変換により、Aを予め三重対角行列に変換しておく。

2°.固有値と固有ベクトルが直にわかる初期行列Dを選ぶ。 例えばAの対角線成分からなる対角行列をとる。 ―実際にはこの選択は必ずしも最良ではなく、むしろ乱数で成分を決めたランダムな対角行列から始めるほうがよいことが多い。

3°.$A(t) = tA + (1-t)D$ と置く。 あるt(最初は0)に対する固有値λと固有ベクトルvとがわかったとする。 tを少し増やしてt′とし、A(t′)に対するvのレーリー商をその近似固有値とし、vに対する逆反復法によって、よい近似固有ベクトルを求める。 必要ならばこの操作を繰り返す。

4°.Aが三重対角行列のときには、スツルム列により定数α以下の固有値の個数が計算できるので、必要ならば(特に全部の固有値を求めるときには)それを検算に利用する。

この操作をt=1 まで繰り返す。 途中で発散したり、重複解が現れたりしないことは、理論的に保証できる。

一見手間が掛るように見えるが、数十元以上の行列で特に全部の固有値・固有ベクトルを求める場合には、これまで標準算法とされていたQR法よりもかえって早いようである。 但し初期行列のとりかたや、t を進める刻みの大きさなど、色々と技法の工夫を要する。

ホモトピー法の歴史は、一面では分野間の交流の重要性を示すとともに、他方では昔の人々が考えた技法の再点検が必要なことを暗示しているように思う。