都民カレッジ '99-II 「群とガロア理論」資料 (担当：中村博昭)

2 次方程式の解の公式は、中学・高校でお馴染みであるが、3 次、4 次となると、あまり紹介されていないようなので、まとめておく。一般には n 次方程式 $x^n + a_1x^{n-1} + \cdots + a_n = 0$ を扱いたいが、$X = x - \frac{a_1}{n}$ という置換えで $n-1$ 乗の係数が 0 の形、つまり $X^n + b_2X^{n-2} + \cdots + b_n = 0$ の形を考えれば十分ということになる。(この置換えは後に述べるチルンハウス変換の特別な場合に相当する)。

3 次方程式の解の公式
デルフェルロ・タルタリア・カルダノによる

3 次方程式 $X^3 + pX + q = 0$ の解 (の一つ) は、

$$\sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2}} + \sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2}}$$

で表される。ここで 2 つの 3 乗根は、積が $-\frac{p}{3}$ となるようにとる。

因数分解の公式として知られている恒等式

$$X^3 + Y^3 + Z^3 - 3XYZ = (X + Y + Z)(X^2 + Y^2 + Z^2 - XY - YZ - ZX)$$

を利用する。X を未知数、Y, Z を定数と見なすと左辺は

$$X^3 - (3YZ)X + (Y^3 + Z^3)$$

と見なせるから、連立方程式

$$\begin{cases} p &= 3YZ, \\ q &= Y^3 + Z^3 \end{cases}$$

が満たされるような Y, Z が見つかれば、上の恒等式の右辺を見て $X = -Y - Z$ が解の一つになることがわかる。ところが、Y^3, Z^3 を 2 解とする 2 次方程式

$$T^2 - qT + (\frac{p}{3})^3 = 0$$

の 3 乗根が Y, Z を与える。(マイナス符号は 3 乗根記号の内部に入れられることに注意) 条件を満たすように 3 乗根の組を与える仕方は、一組を与えた後は、それぞれ (ω, ω^2), (ω^2, ω) を乗じた組も同じ条件を満たす。そこで元の方程式に対して、都合 3 つの解が与えられたことになる。

4 次方程式の解の公式
フェラーリの解法のオイラーによる改良

4 次方程式 $X^4 + pX^2 + qX + r = 0$ の解 (の一つ) は、まず、3 次方程式

$$T^3 + \frac{p}{2}T^2 + (\frac{p^2}{16} - \frac{r}{4})T - (\frac{q}{8})^2 = 0$$

の解 T_1, T_2, T_3 を求め、それらの平方根の符号を

$$\sqrt{T_1}\sqrt{T_2}\sqrt{T_3} = -\frac{q}{8}$$

となるように定めるとき、

$$X = \sqrt{T_1} + \sqrt{T_2} + \sqrt{T_3}$$

で与えられる。

4 次の因数分解の公式として次のようなものがある:

$$X^4 + Y^4 + Z^4 + W^4 - 2(X^2Y^2 + X^2Z^2 + X^2W^2 + Y^2Z^2 + Y^2W^2 + Z^2W^2) + 8XYZW$$
$$= (X + Y + Z + W)(X + Y - Z - W)(X - Y + Z + W)(X - Y - Z + W).$$

ここで X を未知数、Y, Z, W を定数と見なすと左辺は

$$X^4 - 2(Y^2 + Z^2 + W^2)X^2 + (8YZW)X + \{Y^4 + Z^4 + W^4 - 2(Y^2Z^2 + Y^2W^2 + Z^2W^2)\}$$

と見なせるから、連立方程式

$$\begin{cases} p &= -2(Y^2 + Z^2 + W^2), \\ q &= 8YZW, \\ r &= Y^4 + Z^4 + W^4 - 2(Y^2Z^2 + Y^2W^2 + Z^2W^2) \\ &= (Y^2 + Z^2 + W^2)^2 - 4(Y^2Z^2 + Y^2W^2 + Z^2W^2) \end{cases}$$

が満たされるような Y, Z, W が見つかれば、上の恒等式の右辺を見て $X = -Y - Z - W$ が解の一つになることがわかる。ところが、Y^2, Z^2, W^2 を 3 解とする 3 次方程式を $T^3 - \alpha T^2 + \beta T - \gamma = 0$ とすると、計算により

$$\alpha = Y^2 + Z^2 + W^2 = -\frac{p}{2},$$
$$\beta = Y^2Z^2 + Z^2W^2 + Y^2W^2 = \frac{p^2}{16} - \frac{r}{4},$$
$$\gamma = Y^2Z^2W^2 = (\frac{q}{8})^2.$$

この方程式 (分解方程式という) の 3 解ををカルダノの公式を用いて求め、それぞれの平方根として Y, Z, W を定めればよいが、条件式 $YZW = \frac{q}{8}$ を満たすように平方根のトリオをとる必要がある。そのようにして取ったときの $X = -Y - Z - W$ が元の 4 次方程式の一根を与える。符号の取り方を注意してマイナス符号を平方根の枝の取り方にいいくるめたのが上の公式。条件を満たすように 3 つ組の平方根の符号をとる仕方は、一組正しいのが見つかれば、他はそれを $+--, -+-, --+$ とチェンジしたのが 3 通りあり、都合 4 つの解が得られる。この導き方は、飯高茂先生が高校時代に思いついた由 ([1][2])。

チルンハウス変換

与えられた n 次方程式 $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n = 0$ を別の n 次方程式に変数変換する。アイデアは、ある多項式 $\phi(X)$ を与えて、$f(X) = 0$ の解を $x_1, \ldots, x_n$ とするときに、$y_1 = \phi(x_1), \ldots, y_n = \phi(x_n)$ を解とする n 次方程式 $g(Y) = Y^n + b_1Y^{n-1} + \cdots + b_{n-1}Y + b_n = 0$ をつくりましょう、ということである。

対称式の理論をうまく使う。$p_1, p_2, \ldots, p_n$ をオリジナルな解たち $x_1, \ldots, x_n$ の巾和対称式、$P_1, P_2, \ldots, P_n$ を変換後の解たち $y_1 = \phi(x_1), \ldots, y_n = \phi(x_n)$ の巾和対称式とする。(例えば、$p_2 = x_1^2 + \cdots + x_n^2$, $P_3 = y_1^3 + \cdots + y_n^3$ etc.)

いま、$c_1, \ldots, c_n$ を文字として、$Y = \phi(X) = c_{n-1}X^{n-1} + \cdots + c_0$ で変換するとしよう。$\phi(X), \phi(X)^2, \phi(X)^3, \ldots$ を $f(X)$ で割った余りに置き換えてから $X = x_i$ $(i = 1, \ldots, n)$ を代入し i について和を取れば、

$$\begin{cases} P_1 &= c_{n-1}p_{n-1} + \cdots + c_1p_1 + c_0, \\ P_2 &= c_{n-1}^{(2)}p_{n-1} + \cdots + c_1^{(2)}p_1 + c_0^{(2)}, \\ &\cdots \\ P_n &= c_{n-1}^{(n)}p_{n-1} + \cdots + c_1^{(n)}p_1 + c_0^{(n)} \end{cases}$$

の形の式が得られる。ここで各 $c_i^{(k)}$ は文字 $c_0, \ldots, c_{n-1}$ たちの適当な斉 k 次式の形をしている。よく知られているように、巾和対称式と基本対称式は互いに線形結

合で表し合う (ニュートンの公式; [6],[5]5.3 参照) から、この式で、$y_1, \ldots, y_n$ たちの基本対称式を、$x_1, \ldots, x_n$ たちの基本対称式、つまり最初に与えられた $f(X)$ の係数 $a_1, \ldots, a_n$ たちで表せることになる。こうして、変換後の方程式 $g(Y)$ が計算できる。ニュートンの公式は、次数について斉次の形をしているから、こうして計算された $g(Y) = Y^n + b_1 Y^{n-1} + \cdots + b_{n-1} Y + b_n$ の係数たちは、b_1 は $c_0, \ldots, c_{n-1}$ たちの斉 1 次式、b_2 は $c_0, \ldots, c_{n-1}$ たちの斉 2 次式,... という格好をしている。(以上のプロセスを、$f(X)$ と $\phi(X) - Y$ の終結式として説明する流儀もある。[1])

さて、$n \geq 5$ として、上の $\phi(X)$ を 4 次までの範囲におさめて (つまり、$c_5 = \cdots = c_{n-1} = 0$ として) 考えよう。すると上で注意したように、斉次な線形形式 ℓ, 2 次形式 q, 3 次形式 t を用いて、

$$\begin{cases} b_1 &= \ell(c_0, c_1, c_2, c_3, c_4), \\ b_2 &= q(c_0, c_1, c_2, c_3, c_4), \\ b_3 &= t(c_0, c_1, c_2, c_3, c_4), \end{cases}$$

とあらわすことができる。これらが全部 0 になるように、c_0, c_1, c_2, c_3, c_4 を与えることができる。実際、最初の $b_1 = 0$ から c_i のうちのどれかの文字を他であらわしておいて、それを $b_2 = 0, b_3 = 0$ から消去することができる。すると $b_2 = 0$ は c_i 達のうち 4 文字に関する 2 次形式だが、Sylvester の定理 (またはラグランジュの方法) より、これを平方完成して、$b_2 = \lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2$ の形にできる ($\lambda_1, \lambda_2, \lambda_3, \lambda_4$ は線形形式)。そこで $\lambda_1 = \sqrt{-1}\lambda_2$, $\lambda_3 = \sqrt{-1}\lambda_4$ を連立させて、4 文字のうち 2 文字を残りの 2 文字の線形結合で書いて、$b_2 = 0$ が満たされるようにしておくことが出来る。最後に、それらを $b_3 = 0$ に代入してさらに 2 文字を消去すれば、残った 2 文字の c_i に関する 3 次斉次式となり、カルダノの公式により、その 2 文字の比をひとつ決めてやることができる。

このようにして決めた c_0, c_1, c_2, c_3, c_4 でチルンハウス変換をすれば、n 次方程式の係数のうち、2 番目、3 番目、4 番目の係数を 0 にすることができる。(但し、上で平方完成を解いたり、3 次方程式を解いたりしているので、変換後の係数は一般にはその分だけ膨らんでくることに注意。) 特に、5 次方程式は、$Y^5 + b_4 Y + b_5 = 0$ の形に変換できる。ここでさらに $Y = \sqrt[4]{-b_4} Z$ とおけば、方程式は $Z^5 - Z - c = 0$ にまで簡単化される。この形を 5 次方程式のブリング・ジェラードの標準形という。

5 次 (以上の) 方程式を一般的に根号で解く公式は存在しない (アーベル・ルフィニ)。ガロアは、n 次方程式が根号で解けるときと解けないときの違いを構造的に明らかにした。ガロア理論を用いると、例えば $Z^5 - Z - c = 0$ が根号で解けるための必要十分条件が、「分解方程式」$T^6 - 8T^5 + 40T^4 - 160T^3 + 400T^2 - (512 + 3125c^4)T + (256 + 9375c^4) = 0$ が有理解を少なくとも一つ持つことであることが示される ([7])。

付録１：ギリシャの３大作図問題

定規とコンパスのみを用いて...

円積問題

円が与えられたとして、それと同じ面積を有する正方形を作図せよ。

抹香鯨が、人相学的に一つのスフィンクスであるとすれば、骨相学者にとって、その脳体は、かの同面積の正方形を作りえない幾何学的円のごときものだ。(メルヴィル『白鯨』第８０章「胡桃」より)

立方体倍積問題

与えられた立方体の２倍の体積を持つ立方体 (の一辺) の長さを作図せよ。

伝説によれば、紀元前５世紀に、アテネの人口のおよそ４分の１もの人々の命を奪う程の疫病がはやりました。疫病の猛威を多いに恐れた人々は、守護神アポロンを祭ったデロス島の神殿に代表団を送り、御託宣所でお伺いをたてたところ、『立方体をしたアポロンの祭壇を２倍にせよ』との御神託が下りました。そこで、早速、一辺の長さを２倍にした祭壇をつくり奉ったのですが、一向に疫病が止みませんでした。そこで再度お伺いをたてたところ、『辺の長さではなく、体積を丁度２倍にせよ』というお告げがくだったのでした...

角の３等分問題

任意に角度 (たとえば６０度) が与えられたとき、その角度の３等分を作図せよ。

注：２等分なら簡単。

付録２：太古の方程式の問題

メソポタミアの粘土板の問題

直方体の長さと幅と深さがある。長さを分母とする単位分数が幅である。長さと幅との和の１２倍は深さで、体積は ３０ である。長さと幅と深さをもとめよ。

答：$2, \frac{1}{2}; 30$

リンドパピルスの問題

例題２９：ある数にその $\frac{2}{3}$ を加え、またその和の $\frac{1}{3}$ を加える。次に全部の和の $\frac{1}{3}$ を求めると１０であるという。ある数を求めよ。

答：$13\frac{1}{2}$

おまけ：(ディオファントスの生涯『古代ギリシャ詞華集』より)

神はディオファントスに一生の６分の１を少年として過ごす事を認め、そのあと一生の１２分の１たってから鬚をのばさせた。さらに一生の７分の１たったあと結婚生活に入らせ、５年後に子どもをお与えになった。ああ晩年に生まれたあわれな子よ。息子は父の一生の半分を生きたのち、冷酷な死によって連れて行かれてしまった。父は深い悲しみを、この数の科学で４年間癒した後、一生を閉じた。

答：８４才

参考文献

[1] 山下純一「ガロアへのレクイエム」現代数学社, １９８６

[2] 和田秀男「代数方程式論」数理科学, １９７９年１１月号, 17–22

[3] ボイヤー「数学の歴史１ ~ ５」朝倉書店

[4] 上垣渉「ギリシア数学のあけぼの」日本評論社 １９９５

[5] 西山享「多項式のラプソディー」日本評論社 １９９９

[6] 高木貞治「代数学講義」共立出版 (改訂新版 １９６５)

[7] D.S.Dummit “Solving solvable quintics” Math.Comp. 57 (1991), 387–401.

[8] 矢野健太郎 (一松信 解説)「角の三等分」日本評論社

[9] 高崎昇「方程式の歴史」総合科学出版