研究紹介 (星 明考)

研究テーマ: 数論とその周辺

1　5 次方程式の解の公式 (?)

みなさんは，2 次方程式 $ax^2+bx+c=0$ の解を求めることができると思います．解の公式は $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ ですので，$x^2+x+1=0$ の解なら，$x=\frac{-1\pm\sqrt{-3}}{2}$ の 2 つです．では，次に 3 次方程式 $ax^3+bx^2+cx+d=0$ の解を求めることはできるでしょうか？例えば，$x^3+2x^2+2x+1=0$ の解は求められるでしょうか？3 次方程式の解の公式を習っていないから出来ないというのも一つの答えでしょう．しかし，そんなに簡単にあきらめていいのでしょうか？答えは，$x=-1,\ \frac{-1\pm\sqrt{-3}}{2}$ の 3 つです．そうです，$x^3+2x^2+2x+1=(x+1)(x^2+x+1)$ と因数分解すれば，3 つの解が求まります．しかし，$x^3+2x+1=0$ の解と言われると困ってしまうと思います．なぜなら，どうやっても (整数の範囲では) 因数分解できないからです．

3 次方程式にはカルダーノの公式があったはず，と思った人もいるかもしれません．カルダーノの著書『Ars Magna (偉大なる技法)』(1545 年) には 3 次方程式及び 4 次方程式の解法が述べられています．具体的な公式は，例えば [足立, 第 6 章], [三宅, 第 1 章], [雪江, 代数学 1, 第 3 章] などを見て下さい．カルダーノの公式という名前は付いていますが，3 次方程式の解の公式はタルターリアによって発見され，カルダーノに伝えられたと言われています．しかし，ここでは歴史的なことには立ち入りません．興味のある方は，例えば [ヘルマン, 第 1 章, タルターリア VS カルダーノ 三次方程式を解く] を見て下さい．

ここでは話を，一気に大学レベルに上げて，5 次方程式について考えたいと思います．3 次方程式，4 次方程式も解の公式があるのだから，5 次, 6 次, 7 次, ... と次から次へと作って行けばいいのでは？そうすれば世の中にも役に立つ，と思われる方もいらっしゃるでしょう．ここで，解の公式とは，2 次方程式の解の公式と同様に，m 乗根 $\sqrt[m]{\cdot}$ と四則演算 $(+,-,\times,\div)$ を組み合わせて，一般の方程式の解をその係数 $(a, b, c, \ldots)$ を用いて表示するものを指すことにします．しかし，現在でも 5 次方程式の解の公式は知られていません．それどころか，ニールス・ヘンリック・アーベル[1](1802–1829) は次のことを示しました．

[1] ノーベル数学賞はありませんが，アーベルの生誕 200 年を記念して創設され，ノルウェー科学文学アカデミーから授与されるアーベル賞というものがあります (賞金約 1 億円)．さらに，40 才以下に受賞が限定されているフィールズ賞があり，日本は 3 名ものフィールズ賞受賞者，小平邦彦 (1954)，広中平祐 (1970)，森重文 (1990) を輩出しています．

定理 (アーベル, 1824)
n を 5 以上の整数とする．このとき，n 次方程式には解の公式は存在しない．

そうです．5 次以上の場合には解の公式自体が存在しないのです．解の公式がない？それじゃあ解を求めるのはあきらめよう，というのも一つの考え方です．しかし，カール・フリードリヒ・ガウス (1777–1855) によって証明された代数学の基本定理は，n 次方程式の解が複素数の中に確かに n 個あることを指し示しています．

代数学の基本定理 (ガウス, 1799)
n 次方程式は，複素数の中に重複度を込めて n 個の解を持つ．

なぜ 5 次になると解の公式が存在しなくなるのか？4 次と 5 次の違いは何なのか？色々と気になることがあると思います．それを教えてくれるのがエヴァリスト・ガロア (1811–1832) による**ガロア理論**です．だったらそれを早く教えてくれと思った方は，大学 3 年生の代数系 II の授業まで待ってください．そんなに待てないという場合には，[足立] や [彌永] などのガロア理論に関連する本を手に取ってみるのもいいでしょう．ガロア理論によれば，n 次代数方程式 $f(x) = a_n x^n + \cdots + a_1 x + a_0 = 0$ に対して，ガロア群 $\mathrm{Gal}(f/\mathbb{Q})$ という群 (ぐん) を計算すれば，その解がルートと四則演算を組み合わせて書けるかどうかが次のようにして分かります:

定理 (ガロア, 1830)
n 次方程式 $f(x) = 0$ の解が m 乗根 $\sqrt[m]{\cdot}$ と四則演算を繰り返し使って書ける
$\iff$ 多項式 $f(x)$ のガロア群 $\mathrm{Gal}(f/\mathbb{Q})$ は可解群．

そうすると今度は可解群とは何なんだ？ということになりますが，それは大学の代数の本 (特に，群論の本) に譲ります．大抵のガロア理論の本にも出ていると思います．例えば，[雪江, 代数学 1] などを手に取ってみて下さい．ここでは，ガロア理論の詳細は説明せず，代わりに具体例を説明します．

まず，$f(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ を 5 次方程式とします．5 次式が因数分解できる場合には，低次の場合に帰着できるので，$f(x)$ は既約 (因数分解できない) を仮定します．このとき，$f(x)$ のガロア群 $\mathrm{Gal}(f/\mathbb{Q})$ と呼ばれるものは，5 つのタイプ S_5, A_5, F_{20}, D_5, C_5 のうちいずれかになることが知られています[2]．すなわち，実は，5 次方程式と一言で言っても 5 つのタイプが存在するということです．そのうち，最初の 2 つのタイプである S_5 と A_5 は可解群ではなく，残りの 3 つ F_{20}, D_5, C_5 は可解群です．先ほどのガロアの定理を用いれば，S_5 と A_5 タイプの 5 次方程式は，そもそも解が m 乗根 $\sqrt[m]{\cdot}$ と四則演算の繰り返し使っては書けません．しがたがって，一般の 5 次方程式に通用するような解の公式は存在

[2]それぞれ，5 次対称群, 5 次交代群, 位数 20 のフロベニウス群, 位数 10 の二面体群, 5 次巡回群, と呼ばれるものですが，ここでは解説はしません．

し得ないわけです．ちなみに，(既約な) 2 次方程式は C_2 の 1 タイプしかなく，3 次方程式は S_3, C_3 の 2 タイプ，4 次方程式は S_4, A_4, D_4, V_4, C_4 の 5 タイプあり，それらの全てが可解群です．

勝手な 5 次方程式 $f(x) = 0$ が与えられたとき，そのガロア群 $\mathrm{Gal}(f/\mathbb{Q})$ がどのタイプになるのかを求めるアルゴリズムはよく知られており，代数計算ソフト (例えば [Sage]) を使ってコンピュータを使って計算することができます．具体例を挙げてみると，以下の表 1 のようになります．

5 次方程式	ガロア群 $\mathrm{Gal}(f_i/\mathbb{Q})$
$f_1(x) = x^5 - x^3 - x^2 + x + 1 = 0$	$\longrightarrow S_5$
$f_2(x) = x^5 + x^4 - 2x^2 - 2x - 2 = 0$	$\longrightarrow A_5$
$f_3(x) = x^5 + x^4 + 2x^3 + 4x^2 + x + 1 = 0$	$\longrightarrow F_{20}$
$f_4(x) = x^5 - x^3 - 2x^2 - 2x - 1 = 0$	$\longrightarrow D_5$
$f_5(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0$	$\longrightarrow C_5$

表 1

ガロアの定理から，$f_1(x) = 0$ と $f_2(x) = 0$ の解は，もはや m 乗根 $\sqrt[m]{\cdot}$ と四則演算を繰り返し組み合わせても，解を表示することができないことが分かるわけです．

この節の最後に，私の研究の紹介ですが，**ガロア逆問題**に関連する数論を研究しています．ガロア逆問題とは，簡単に言うと，(表 1 のように) n 次方程式 $f(x) = 0$ を与えるごとにガロア群 $\mathrm{Gal}(f/\mathbb{Q})$ が定まる通常のガロア理論とは逆に，先にガロア群側を指定した時に，そのガロア群が出てくるような $f(x) = 0$ は存在するか？(見つけることができるか？) という問題です．$n = 5$ の (既約な) 場合は，5 タイプあり表 1 のように，5 タイプともある方程式 $f_i(x) = 0$ のガロア群として実際に出現したので OK です．また各 n に対してガロア群になり得るタイプは有限種類であることも分かります．しかし，n を大きくして，一般の整数 n に対して，全てのタイプが実際に出現するか，すなわちガロア逆問題[3]は現在でも未解決問題です．

さらに研究に興味がある場合は，例えば [三宅, 第 VII 章] を見て下さい．

2　ディオファンタス方程式

前節では，代数方程式の解の公式の有無について述べました．その解は当然ながら複素数 (もしくは，実数) の世界の中で考えられていました．しかし，数論では，特に整数解 (整数の解) や有理数解 (有理数の解) のみに興味が注がれることがあります．例えば，ピエール・ド・フェルマー (1607–1665) が「真に驚嘆すべき証明を発見したが，この余白はそれを書くには狭すぎる」と書き残したという有名

[3]数論の言葉でいえば，絶対ガロア群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の商群として全ての有限群が現れるか？

なフェルマーの最終定理 (フェルマーの大定理やフェルマー予想とも呼ばれます) は，以下のように述べられます: 3 以上の自然数 n に対して，

$$x^n + y^n = z^n$$

を満たす整数解 (x, y, z) は，自明な $xyz = 0$ を除いて存在しない．フェルマーの最終定理は，1994 年にアンドリュー・ワイルズによって，現代の数論である岩澤理論，ガロア表現，楕円曲線，保型形式の理論などを用いて，(一部，リチャード・テイラーの協力もあり) 谷山-志村予想 (半安定な場合) を解決することによって証明されました．興味のある方は，例えば [加藤] などを見て下さい．

このように，整数解を求めるという文脈において，整数係数の多変数 $(x, y, z, \ldots)$ の不定方程式はディオファンタス方程式と呼ばれています．以下では，私のこれまでの研究の中から，**トゥエ方程式**というある特別な形をしているディオファンタス方程式の整数解を求める研究を紹介したいと思います．

$F(x, y)$ を既約な 3 次以上の整数係数の斉次多項式とします．このとき，整数 $k \neq 0$ に対して，ディオファンタス方程式 $F(x, y) = k$ はトゥエ方程式と呼ばれています．例えば，方程式 $x^3 - 3xy^2 - y^3 = 1$ はトゥエ方程式です．

定理 (トゥエ, 1909)
トゥエ方程式 $F(x, y) = k$ の整数解 (x, y) は有限個しかない．

その証明法は，全く想像できないかもしれませんが，代数方程式の解となる複素数 (代数的数という) が有理数ではあまり良く近似できないことに基づいています．しかし，有限個であることが分かっても，全ての整数解 (x, y) を具体的に計算することは一般には難しい問題です．例えば，上述したトゥエ方程式 $x^3 - 3xy^2 - y^3 = 1$ の解を全て求めよ，と言われると $(x, y) = (2, 1), (1, -3), (-3, 2)$ が解であることはすぐに確認できても，これで全てであることはどうやって示せばよいのか，すぐには分かりません．

アラン・ベイカー[4]は，1968 年に整数解 (x, y) の最大値，最小値が具体的に計算可能であることを示しました．しかしながら，その最大値，最小値は，一般にはとてつもなく大きいもので，コンピュータで計算しても，とても生きている間には到達できそうにはないほど大きい，という類のものです．

1990 年，E. Thomas は整数 $m \geq -1$ を動かす[5]ことによって，無限個のトゥエ方程式 $F_m(x, y) = x^3 - mx^2y - (m + 3)xy^2 - y^3 = k$ を考察し，$k = 1$ の場合に，$m + 1 \leq 10^3$ と $1.365 \times 10^7 \leq m + 1$ なる範囲の整数解 (x, y) を全て求めました．さらに M. Mignotte は 1993 年に残りの場合も全ての整数解を決定しました．こうして，初めて**無限個の**トゥエ方程式の整数解 (x, y) が全て決定されました．その $k = 1$ に対する整数解の全ては，整数 $m \geq -1$ に対して，$(x, y) = (0, -1), (-1, 1), (1, 0)$

[4]ディオファンタス方程式に関する功績により，1970 年にフィールズ賞を受賞．
[5]本来は全ての整数 m を動かすことができるのですが，ここでは簡単のため $m \geq -1$ とします．

及び

$$(x,y)=(-1,-1),(-1,2),(2,-1) \qquad (m=-1),$$
$$(x,y)=(5,4),(4,-9),(-9,5) \qquad (m=-1),$$
$$(x,y)=(2,1),(1,-3),(-3,2) \qquad (m=0),$$
$$(x,y)=(-7,-2),(-2,9),(9,-7) \qquad (m=2)$$

で与えられます．さらに，1996 年，M. Mignotte, A. Pethö, F. Lemmermeyer の 3 人は $1<k\leq 2m+3$ なる整数 k に対して，$F_m(x,y)=k$ の全ての整数解 (x,y) を決定しました．その整数解は，全ての整数 $m\geq -1$ に対して，$k=a^3$ のとき，$(x,y)=(0,-a),(-a,a),(a,0)$ 及び $k=2m+3$ のとき，

$$(x,y)=(-1,2),(2,-1),(-1,-1),(-1,m+2),(m+2,-m-1),(-m-1,-1)$$

と $(m,k)=(1,5)$ に対する 6 組の例外

$$(x,y)=(1,-4),(-4,3),(3,1),(3,-11),(-11,8),(8,3)$$

からなります．1999 年，G. Lettl, A. Pethö, P. Voutier の 3 人は，超幾何関数による近似を用いて，より広い整数 k を動かせるように改善しました．私はこれを k が m^2+3m+9 の (正の) 約数を動けるようにし，$F_m(x,y)=k$ の全ての整数解 (x,y) を決定しました．それらは $k=a^3$ のとき，$(x,y)=(0,-a),(-a,a),(a,0)$ と次の表 2 における 66 組の整数解 (x,y) で与えられます．そして最小分解体の一致という現象との対応を見つけて，なぜ 66 組存在するのかを明らかにしました (2011 年).

m	k	m^2+3m+9	(x,y)
-1	1	7	$(-1,-1)$, $(-1,2)$, $(2,-1)$
-1	1	7	$(5,4)$, $(4,-9)$, $(-9,5)$
-1	7	7	$(2,1)$, $(1,-3)$, $(-3,2)$
0	1	9	$(2,1)$, $(1,-3)$, $(-3,2)$
0	3	9	$(-1,-1)$, $(-1,2)$, $(2,-1)$
1	13	13	$(-5,-2)$, $(-2,7)$, $(7,-5)$
2	1	19	$(-7,-2)$, $(-2,9)$, $(9,-7)$
3	9	3^3	$(-1,-1)$, $(-1,2)$, $(2,-1)$
3	9	3^3	$(-4,-1)$, $(-1,5)$, $(5,-4)$
5	7^2	7^2	$(-1,-2)$, $(-2,3)$, $(3,-1)$
5	7^2	7^2	$(-4,-1)$, $(-1,5)$, $(5,-4)$
5	7^2	7^2	$(19,3)$, $(3,-22)$, $(-22,19)$
12	3^3	$3^3\cdot 7$	$(-1,-1)$, $(-1,2)$, $(2,-1)$
12	3^3	$3^3\cdot 7$	$(-13,-1)$, $(-1,14)$, $(14,-13)$
12	$189=3^3\cdot 7$	$3^3\cdot 7$	$(-4,-1)$, $(-1,5)$, $(5,-4)$
54	$343=7^3$	$3^2\cdot 7^3$	$(-1,-2)$, $(-2,3)$, $(3,-1)$
54	$1029=3\cdot 7^3$	$3^2\cdot 7^3$	$(-4,-1)$,$(-1,5)$, $(5,-4)$
66	$4563=3^3\cdot 13^2$	$3^3\cdot 13^2$	$(-5,-2)$, $(-2,7)$, $(7,-5)$
1259	$226981=61^3$	$7\cdot 61^3$	$(-4,-5)$, $(-5,9)$, $(9,-4)$
1259	$226981=61^3$	$7\cdot 61^3$	$(-13,-1)$, $(-1,14)$, $(14,-13)$
1259	$1588867=7\cdot 61^3$	$7\cdot 61^3$	$(-3,-19)$, $(-19,22)$, $(22,-3)$
2389	$300763=67^3$	$19\cdot 67^3$	$(-7,-2)$, $(-2,9)$, $(9,-7)$

表 2

参考文献

[足立] 足立恒雄 (著), ガロア理論講義 [増補版], 日本評論社, 2003.

[彌永] 彌永昌吉 (著), ガロアの時代 ガロアの数学，第一部 時代篇, 第二部 数学篇, シュプリンガー・フェアラーク東京, 1999, 2002.

[加藤] 加藤和也 (著), 解決!フェルマーの最終定理, 日本評論社, 1995.

[ヘルマン] ハル・ヘルマン (著), 三宅克哉 (訳), 数学 10 大論争, 紀伊國屋書店, 2009.

[三宅] 三宅克哉 (著), 方程式が織りなす代数学, 共立出版, 2011.

[雪江] 雪江明彦 (著), 代数学 1 群論入門, 代数学 2 環と体とガロア理論, 代数学 3 代数学のひろがり, 日本評論社, 2010, 2010, 2011.

[Sage] W. A. Stein et al., Sage Mathematics Software (Version 5.8), The Sage Development Team, 2013, `http://www.sagemath.org`.