ガロア群A_5をもつ５次方程式

稲垣佑都

津山工業高等専門学校総合理工学科（４年）

１．はじめに

３年生の演習の授業（全系横断演習Ⅰ）において，数学の演習を受講した．内容は「ガロア理論を理解しよう」というもので，群論と体論，そしてnを５以上の整数としたとき一般のn次方程式はべき根で解くことができないという理論を学んだ．それは，一般のn次方程式から得られるn次対称群S_nが，$n \geq 5$のとき可解群でないことに理由があった．

一般のn次方程式の群はS_nである．そして，$n \geq 5$のときS_nは可解群でないため，一般のn次方程式はべき根で解くことができない．一方．S_nの正規部分群で単純群でもあるn次交代群A_nも可解群でない．したがって，A_nをもつn次方程式もまたべき根で解くことができない．A_nをもつn次方程式は，S_nをもつn次方程式に比べ，圧倒的に数は少ないはずだ．それならば，A_nをもつn次方程式は何らかの特徴を持つのではないだろうか．このような興味から本研究をスタートさせ，具体的に，A_5をもつ5次方程式の構造に関する研究を行なった．そして，コンピュータを使った研究から，A_5をもつ5次方程式にはリュカ数に関係するものがあるという結果を得た．ここで，n番目のリュカ数L_nとは，$L_0 = 2, L_1 = 1$で，$n \geq 2$のとき$L_n = L_{n-1} + L_{n-2}$から得られる数のことである．

２．先行研究の要約

これまでの5次方程式の構造に関する研究では,Spearman と Williams[2],[3],あるいは,Kavanach の研究[5]による$x^5 + ax + b$と$x^5 + ax^2 + b$の研究がある．しかし，これらは可解な方程式，すなわち二面体群D_5やフロベニウス群F_{20}などをもつ５次方程式の研究である．

$x^5 + ax + b$の研究[2]，[3]の結果をより具体的に述べると，それは，$\varepsilon = \pm 1, c \geq 0, e \neq 0$で，

$$a = \frac{5e^4(3 - 4\varepsilon c\ )}{c^2 + 1}, b = \frac{-4e^5(11\varepsilon + 2c)}{c^2 + 1}$$

ならば，方程式$x^5 + ax + b = 0$は，べき根で解くことができるというものである．さらに，この応用として，$p = 4n + 3$（nは自然数）を素数としたとき，方程式$x^5 + 2px + 2p^2 = 0$の群は可解群ではないことが示されている．しかし，これがS_5かA_5のどちらかになるかについては述べられていない．

一方，元吉文雄の研究[1]は，５次方程式の群をいかに速く決定するかというテーマを扱ったものであるため，本研究から得られたA_5をもつ5次方程式がリュカ数と関係するという

結果については全く触れられていない.

３．方程式の群

a_j　$(1 \le j \le n-1)$を有理数体$\mathbf{Q}$の元とし，n次方程式

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_1 = 0$$

を考える．そして，この方程式のn個の解が全て含まれる$\mathbf{Q}$上の最小の体（最小分解体）をFとする．このとき，　n個の解を互いに置換しあって入れ換えたとき，Fが変化しないような置換だけを集めた集合をn次方程式の群という．

一般のn次方程式の場合の方程式の群はS_nであり，その位数は$n!$である．そしてS_nの偶置換がなす群がn次交代群A_nであり，その位数は$n!/2$である．

４．フリーソフト SageMath を用いたA_5をもつ5次方程式の判定

本研究のテーマであるA_5をもつ5次方程式の因数分解を簡単に説明する．

まず，A_5の位数は$5!/2 = 60$である．ガロア理論によれば，この60という数は，有理数体$\mathbf{Q}$から最小分解体Fまでの拡大次数になる（[6]参照）．具体的には，$\mathbf{Q}$とFの間の部分体が，$\mathbf{Q} \subset \mathrm{K} \subset \mathrm{M} \subset \mathrm{F}$であって，$\mathbf{Q} \subset \mathrm{K}$の拡大次数が 5 であり，　$\mathrm{K} \subset \mathrm{M}$の拡大次数が 4 であり，　$\mathrm{M} \subset \mathrm{F}$の拡大次数が 3 となるような部分体K, Mが存在するのである．このとき，これらの拡大次数の積が$5 \times 4 \times 3 = 60$となる．

したがって，5次方程式

$$x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$$

の左辺を因数分解していく過程で，体Kの中で，左辺は

$$(x - \lambda_1)(x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0) = 0\ , \qquad \lambda_1, b_j \in \mathrm{K}, \quad \lambda_1, b_j \notin \mathbf{Q}$$

と因数分解され，体Mの中では，左辺は

$$(x - \lambda_1)(x - \lambda_2)(x^3 + c_2 x^2 + c_1 x + c_0) = 0, \qquad \lambda_2, c_j \in \mathrm{M}, \quad \lambda_2, c_j \notin \mathrm{K}$$

と因数分解される．そして，体Kの中では，左辺は

$$(x - \lambda_1)(x - \lambda_2)(x - \lambda_3)(x - \lambda_4)(x - \lambda_5) = 0, \qquad \lambda_3, \lambda_4, \lambda_5 \in F, \quad \lambda_3, \lambda_4, \lambda_5 \notin \mathrm{M}$$

と因数分解される．以上のような因数分解の構造をもつ５次方程式の群がA_5である．

今回の研究は，フリーソフト SageMath version 8.6 を使って行なった． SageMath は，そのパッケージに PARI/GP を搭載しおり，方程式の群の計算が可能となっている．SageMath は，2005 年にアメリカワシントン大学の William Stein が主導して開発した．

SageMath を用いた最初の試みは，５次方程式を決め，その因数分解を試みて，その群を決定することであった. すなわち，５次方程式を定め, その５次方程式の一つの解をaとし，aを含む$\mathbf{Q}$上の最小な拡大体を$\mathrm{K} = \mathbf{Q}(a)$とし，５次式をKの中で SageMath に因数分解させる．もし，5次式が１次式と４次式に分解されたなら，定めた５次方程式はA_5の可能性がある．そこで，次に得られた４次式から４次方程式を作り，その解をbとし，bを含むK上の最小な拡大体を$\mathrm{M} = \mathrm{K}(b)$とし，４次式をMの中で SageMath に因数分解させる．もし，４次

式が１次式と３次式に分解されたなら，定めた５次方程式はA_5の可能性がある．そして，得られた３次式から３次方程式を作り，その解をcとし，cを含むM上の最小な拡大体をF＝M(c)とし，３次式をFの中でSageMathに因数分解させる．もし，３次式が１次式に分解されたなら,定めた5次方程式はA_5となる.しかし,この方法は,体を拡大するたびにSageMathの因数分解にかかる計算量が増え，一つの５次方程式がA_5であることを判定するのに，１０分以上の時間を要した.

詳細は理解していないが，論文[4]などを見ると，SageMath が計算で呼び出す Magma と Gap には Transitive permutation group で，その位数が 32 以下のリストが組み込まれており，それを使って方程式の群の位数が計算できるアルゴリズムが開発されている．このことから，SageMath には方程式の群を高速に決定するコマンドがあるのではないかと思い，調査した結果

```
G=f.galois_group(pari_group=True)
```

というコマンドにたどりついた．このコマンドを用いると，一つの５次方程式がA_5であることを判定することは一瞬であった．その後，SageMath 上で動く Python2 を使ったプログラムを書き，この結果，短時間で多くの５次方程式が扱えるようになり，それらの群のデータを得ることができるようになった.

５．研究計画

A_5をもつ５次方程式を決定するための SageMath 上で動く Python2 を使ったプログラムを作り，A_5をもつ５次方程式

$$a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0=0$$

のデータを分析することにした．ここで，a_iは整数とした．確かに大量のA_5をもつ５次方程式のデータを得ることはできるようになったが，得られたデータの多さから，何らかの法則を発見することは難しかった．そこで，係数のパラメータをsとtなどの２個に限定し研究すれば，もう少し有用なデータが得られ，深い考察ができるのではないかと考えた．そして，今回の研究では，

$$x^5+sx+t=0,\quad x^5+sx^2+t=0,\quad x^5+sx^3+t=0,\quad x^5+sx^4+t=0$$

というタイプの方程式を扱うことにした.

６．方程式 $x^5+sx^4+t=0$ の研究結果

方程式 $x^5+sx^4+t=0$の群がA_5であるsとtを調査したところ，特に，$s=5$のときtについて以下のデータが得られた.

$$t=64,320,7744,20480,53824,141120,369664$$

$$t=-320,-1280,-3136,-8000,-54080,-141376,-369920$$

これらは全て64の倍数であり$t=64u$とすると，

$$u = 1,5,45,121,320,841,2205,5776$$
$$u = -5,-9,-49,-125,-845,-2209,-5780$$

である．

ここで，注目した数列はL_0 =2 のリュカ数L_nであり，$n \geq 1$のL_nは，

$$1,3,4,7,11,18,29,47,76,\cdots$$

であり，L_n^2は，

$$1,9,16,49,121,324,841,2209,5776,\cdots$$

である．そこで，数列$u_n \quad (n \geq 1)$を，

$u_1 = {L_1}^2 = 1,\quad u_2 = {L_2}^2 - 4 = 9 - 4 = 5\ ,\quad u_3 = {L_3}^2 = 16,$

$u_4 = {L_4}^2 - 4 = 49 - 4 = 45,\quad u_5 = {L_5}^2 = 121,\quad u_6 = {L_6}^2 - 4 = 324 - 4 = 320,$

$u_7 = {L_7}^2 = 841,\quad u_8 = {L_8}^2 - 4 = 2209 - 4 = 2205,\quad u_9 = {L_9}^2 = 5776,\cdots$

すなわち，

$$u_{2n-1} = L_{2n-1}^2,\qquad u_{2n} = {L_{2n}}^2 - 4$$

と置くと，$1 \leq n \leq 9$である整数nについて，方程式 $x^5 + 5x^4 + 64u_n = 0$ $(u_3$は除く$)$ の群はA_5であるといえる．実は，方程式 $x^5 - 5x^4 - 64u_n = 0$ $(u_3$は除く$)$の群もA_5である．

同様に，数列$v_n \quad (n \geq 1)$を，

$v_1 = {L_1}^2 + 4 = 5,\quad v_2 = {L_2}^2 = 9\ ,\quad v_3 = {L_3}^2 + 4 = 16 + 4 = 20,$

$v_4 = {L_4}^2 = 49,\quad v_5 = {L_5}^2 + 4 = 121 + 4 = 125,\quad v_6 = {L_6}^2 = 324,$

$v_7 = {L_7}^2 + 4 = 841 + 4 = 845,\ v_8 = {L_8}^2 = 2209,\ v_9 = {L_9}^2 + 4 = 5776 + 4 = 5780,\cdots$

すなわち，

$$v_{2n-1} = L_{2n-1}^2 + 4,\qquad v_{2n} = {L_{2n}}^2$$

と置くと，$1 \leq n \leq 9$, である整数nについて，方程式 $x^5 + 5x^4 - 64v_n = 0$ $(v_3$は除く$)$と $x^5 - 5x^4 + 64v_n = 0$ $(v_3$は除く$)$の群はA_5である．

次の予想を得ることができた．

予想１． L_n（$n \geq 1$）をリュカ数とする．このとき，

(1) $u_{2n-1} = L_{2n-1}^2$ ，$u_{2n} = L_{2n}^2 - 4$と置いたとき，u_3を除く方程式$x^5 + 5x^4 + 64u_n = 0$ と$x^5 - 5x^4 - 64u_n = 0$ の群はいずれもA_5である．

(2) $v_{2n-1} = L_{2n-1}^2 + 4,\ v_{2n} = {L_{2n}}^2$ と置いたとき，v_3を除く方程式$x^5 + 5x^4 - 64v_n = 0$ と $x^5 - 5x^4 + 64v_n = 0$ の群はいずれもA_5である．

予想１は，SageMath によれば$n = 10000$までは正しい．

７．方程式 $x^5 + sx^3 + t = 0$ の研究結果

前節で，A_5をもつ方程式$x^5 + sx^4 + t = 0$がリュカ数から得られることが予想された．方程式 $x^5 + sx^3 + t = 0$についてもこの観点から研究した．その結果，A_5をもつ方程式につい

て以下のデータが得られ，これはとても簡単に扱えるものだった．

$x^5+15x^3\pm 81u_n=0$が群A_5をもつリスト

$$u_n=4,11,29,76,199,521$$

$x^5-15x^3\pm 81v_n=0$が群A_5をもつリスト

$$v_n=3,7,18,47,123,322,843$$

以下の予想が得られた．

予想２． L_n（$n\geq 1$）をリュカ数とする．このとき，

$$u_n=L_{2n+1},\qquad v_n=L_{2n}$$

と置くと，方程式 $x^5+15x^3\pm 81u_n=0$ と $x^5-15x^3\pm 81v_n=0$ の群はいずれもA_5である．

予想２は，SageMath によれば$n=10000$までは正しい．

８．方程式 $x^5+sx^2+t=0$ の研究結果

方程式$x^5+s_nx^2+t_n=0$については，$s_n=\pm 10L_n$ ，　$t_n=\pm 24L_n$（複号同順）を考える必要があった．以下の表１がそのデータである．

表１

n	1	2	3	4	5	6	7	8
L_n	1	3	4	7	11	18	29	47
s_n	10	30	40	70	110	180	290	470
t_n	24	72	96	168	264	432	696	1128
群	A_5	S_5	D_5	S_5	A_5	S_5	A_5	S_5

n	9	10	11	12	13	14	15	16
L_n	76	123	199	322	521	843	1364	2207
s_n	760	1230	1990	3220	5210	8430	13640	22070
t_n	1824	2952	4776	7728	12504	20232	32736	52968
群	A_5	S_5	A_5	S_5	A_5	S_5	A_5	S_5

n	17	18	19	20	21	22	23	24
L_n	3571	5778	9349	15127	24476	39603	64079	103682
s_n	35710	57780	93490	151270	244760	396030	640790	103682
t_n	85704	138672	224376	363048	587424	950472	1537896	2488368
群	A_5	S_5	A_5	S_5	A_5	S_5	A_5	S_5

表１より以下の予想が得られた.

予想３. $L_n\,(n \geq 1)$をリュカ数とする. このとき, 方程式$x^5 \pm 10x^2 \pm 24 = 0$ （復号同順）の群はA_5であり，さらに，$n \geq 3$で

$$s_n = \pm 10L_{2n-1}, \qquad t_n = \pm 24L_{2n-1} \quad \text{（複号同順）}$$

と置くと，方程式 $x^5 + s_n x^2 + t_n = 0$ の群はいずれもA_5である.

予想３は，SageMath によれば$n = 10000$までは正しい.

９．方程式 $x^5 + sx + t = 0$ の研究結果

方程式 $x^5 + sx^3 + t = 0$に関するA_5の群をもつ方程式として,

$$x^5 + 20x \pm 16 = 0, \qquad x^5 + 95x \pm 76 = 0, \qquad x^5 + 145x \pm 232 = 0$$

などが見つかった．そして，これらを

$$x^5 + 5nx \pm 4m = 0$$

と置くと，(n, m)のリストとして,

$$(n, m) = (4,4), (19,19), (19,133), (29,58), (44,44), (44,132), (64,128), (79,79), (124,124), \cdots$$

などが挙がった．リュカ数に的を絞りこれらのデータを考察した．その結果,

$$n = m = 4, 4 \times 11, 11 \times 29, 29 \times 76, \cdots$$

であるものを発見した．すなわち,

$$x^5 + (5 \times 4)x + (4 \times 4) = 0, \qquad x^5 + (5 \times 4 \times 11)x + (4 \times 4 \times 11) = 0$$

$$x^5 + (5 \times 11 \times 29)x + (4 \times 11 \times 29) = 0, \qquad x^5 + (5 \times 29 \times 76)x + (4 \times 29 \times 76) = 0$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

は，A_5の群をもつ方程式であった．これより以下の予想が得られた.

予想４．L_n（$n \geq 1$）をリュカ数とする．このとき，$n \geq 0$に対して

$$u_n = L_{2n+1}L_{2n+3}$$

と置くと，方程式 $x^5 + 5u_n x \pm 4u_n = 0$ の群はいずれもA_5である.

予想４は，SageMath によれば$n = 10000$までは正しい.

１０．本研究で得られた成果

本研究では，A_5の群をもつ５次方程式 $x^5 + sx^4 + t = 0$，$x^5 + sx^3 + t = 0$，$x^5 + sx^2 + t = 0$，$x^5 + sx + t = 0$に関する研究を行なった．その結果，リュカ数に関係する予想１から予想４を立てることができた. いくつかの論文を検索したが，これまでA_5の群をもつ５次方

程式とリュカ数との関係を扱ったものは見つからなかった．したがって，今回の研究結果は予想とはいえ，新しい発見であることが期待される．

１１．今後の発展と展開の可能性，今後の研究の予定

今後の研究の発展と展開について，次の二つを挙げることができる．一つ目は，A_5の群をもつ方程式 $x^5+sx^4+tx^3+u=0, x^5+sx^4+tx^2+u=0, x^5+sx^4+tx+u=0$に関する研究である．これらについては，リュカ数だけでなくフィボナッチ数列との関係性が見えてきている．二つ目は，今回挙げた４つの予想の証明についてである．論文[5]や指導教員のアドバイスなどからその方向性が徐々に見えてきている．次の機会にこのことが報告できればと考えている．

謝辞

本論文に対して，日本高専学会高専・大学部会の先生方から貴重な多くのアドバイスをいただき，とても参考になりました．ここに感謝申し上げます．

参考文献

[1] 元吉文雄，５次方程式の可解性の高速判定法，数理解析研究所講究録第 848 巻 1993 年 1-5

[2] Blair K. Spearman and Kenneth S. Williams, Characterization of solvable quintics x^5+ax+b, The American Mathematical Monthly Vol. 101, No. 10 (Dec., 1994), pp. 986-992

[3] Blair K. Spearman and Kenneth S. Williams, ON SOLVABLE QUINTICS x^5+ax+b AND x^5+ax^2+b, ROCKY MOUNTAIN JOURNAL OF MATHEMATICS Volume 28, Number 2, Spring 1998

[4] Claus Fieker and Jürgen Klüners, Computation of Galois groups of rational polynomials, LMS J. Comput. Math. 17 (1) (2014) 141-158

[5] Ryan Kavanach, ON IRREDUCIBLE RATIONAL QUINTICS, https://rak.ac/files/papers/galois.pdf

[6] 彌永昌吉，有馬哲，浅枝陽，代数入門，東京図書，1990