

群論演習 と J (その 2)

Yahoo 知恵袋の問答から

中野 嘉弘 (札幌市、86歳)

FAX 011-588-3354, E-mail yoshihiro@river.ocn.ne.jp

1. は し が き

JAPLA 4月の研究会の後、Yahoo 知恵袋に、次のような質問が出された。
「位数 48 の群が可解であることを証明せよ」の解答を求む！
order 48 の group が solvable (soluble, lösbar) である事の
証明である。

既に知られている事に、対称群 S_n は、 $n \leq 4$ ならば「可解」であり、
 $n \geq 5$ ならば、「可解でない」がある。代数方程式の解(根の公式)が、
4次までで、5次以上は「加減乗除と根号計算では解けない」事が、天才児、
ガロア Galoi の名と共に、周知である。
その類の話であるから、ひょっとすると、次数 48 の代数方程式は、所謂、
「解ける」と云う事かも知れぬと、興味がそそられた。

ガロアと並ぶ天才にアーベルが居る。その名を冠するアーベル群は、
「可換群」つまり、群操作(演算)の順序を交換しても同じであるもので、
可換群の時は、問題は素直(判り易い、解答し易い)になる。
今の「可解群」は、それに次ぐ程度に、取扱い易い群なのだそうだ。
(詳しくは、その中間に、「ベキ零群 nilpotent group」なる概念が
挿入されるのだそうだ。ベキ零群は可解群であるが、逆は成立せず。
たとえば、3次対称群は可解であるが、ベキ零群では無い。)
その可解群を定義するには、「交換子群」の定義を先にする必要が
ある。前稿は、それに言及しかけたところまでであった。

(前稿再録 7. 正規部分群(不変部分群))

岩波講座 応用数学 11 [基礎8] 群と表現: 江沢 洋・島 和久 p.14 (文献 7) に
面白い記述がある。

● Normal Sub-Group, 正規部分群、不変部分群、Invariant Sub-Group

$$N = \{i, a_9, a_{10}, a_{11}\}$$

$$= \{1|2|3|4|, |2\ 1|4\ 3|, |3\ 1|4\ 2|, |3\ 2|4\ 1|\}$$

4次の場合に限り、交代群(対称群)は正規部分群を持つと云われているが、その例で
ある。

本によっては、一般的に次のようにも書く。

$$N = I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

キ 正規部分群を持たない群を単純(Simple)と云う。 5次交代群は単純群であり、従って可解群では無い。

●与群Gから正規部分群を作る方法に交換子(commutator)法がある。 かくして出来る群を交換子群と云う。

段々、尤もらしくなってきた。 次回にゆっくりやろう。 (前稿再録終わり)

2. 交換子群

「交換子」は commutator である。 その定義は、入門書(文献3)によれば、

定義： 群Gの要素 x, y から、その逆元 $x(-1), y(-1)$ について、
 $xyx(-1)y(-1)$ の形の元全体から生成される、Gの部分群をGの交換子群と云い、記号、 $[G, G]$ で表す。

注意： $xyx(-1)y(-1)$ の形の元を、有限個、掛け合わせた集合から成る群である。

性質： 1) 可換(アーベル)群の交換子群は要素1のみからなる。

(証明1) 全要素について $xy = yx$ から、 $xyx(-1)y(-1) = 1$ が成立。

2) $[G, G]$ は G の正規部分群である。

(証明2) $x \in G, aba(-1)b(-1) \in [G, G]$ について

$$\begin{aligned} x(aba(-1)b(-1))x(-1) &= \\ (xax(-1))(xbx(-1))((xax(-1))(-1))((xbx(-1))(-1)) &\in [G, G] \end{aligned}$$

3) 剰余群 $G/[G, G]$ は可換(アーベル)群である。

(証明3) $[x], [y] \in G/[G, G]$ に対して、

$$[x][y][x](-1)[y](-1) = [xyx(-1)y(-1)] \in [[G, G]] = 1$$

より、 $[x][y] = [y][x]$ なので可換。

5) NがGの正規部分群で、NによるGの剰余群 G/N が可換群ならば、

Nは $[G, G]$ を含む。 即ち $[G, G] \subset N$ である。

(証明4) G/N が可換群ならば、 $[x], [y] \in G/N$ に対して

$$\begin{aligned} [xyx(-1)y(-1)] &= [x][y][x](-1)[y](-1) = 1 \text{ より} \\ xyx(-1)y(-1) &\in N \text{ と成る。 それ故、} [G, G] \subset N \text{。} \end{aligned}$$

しかし、ゴタゴタして判り難い。

3. 交換子 と J

6) 交代群 A_n の 交換子群の例：

$$[A_2, A_2] = 1$$

$$[A_3, A_3] = 1$$

7) $[A_4, A_4] =$ Klein の 四元群 V_4

1に収束する部分群列を持つので可解群である。

- 3) $n \geq 5$ に対して $[A_n, A_n] = A_n$
 A_n ($n \geq 5$) が単純 (1 に収束する部分群列を持たぬ) なので、
 可解では無い。
- 4) 4元数群 Quaternion group $Q = \{1, -1, i, -i, j, -j, k, -k\}$
 ただし、 $ij=-k, ji=k, ii=-1, i(-i)=1$ etc について、
 交換子群 $[Q, Q] = \{1, -1\} = Z_2$ である。
- 5) 対称群 S_n の交換子群は 交代群 A_n である。
 $[S_n, S_n] = A_n$
 A_n ($n \leq 4$) は可解であるから、そこまでは S_n も可解である。
 $n \geq 5$ に対しては、共に、非可解。

理解にはやって見るのが最善だ。それには、群の乗積表を作るのが
 良い。

- 1) 2次対称群 $S_2 = \{\text{単元 } e, (1\ 2)\}$ 故、交代群 $A_2 = \{e\}$ 。
 故に、交換子群 $[A_2, A_2] = \{e\} = 1$ 。

3 次交代群 $A_3 = \{E, S, T\}$ 、 $E = (1\ 2\ 3)$ 、 $S = (2\ 3\ 1)$ 、
 $T = (3\ 1\ 2)$ 。 J 言語 で乗積表を作ろう。
 ベクトル $V = .\ 1\ 2\ 3$ とする。 J 言語の原点 0 を考慮して、
 $e = .((1\ 2\ 3) - 1) \rightarrow 0\ 1\ 2$ として、 $e \{v \rightarrow 1\ 2\ 3$ 単元。
 $s = .((2\ 3\ 1) - 1) \rightarrow 1\ 2\ 0$ として、 $s \{v \rightarrow 2\ 3\ 1$ 、
 $t = .((3\ 1\ 2) - 1) \rightarrow 2\ 0\ 1$ として、 $t \{v \rightarrow 3\ 1\ 2$ 。

$s \{(s \{v\}) \rightarrow s \{2\ 3\ 1 \rightarrow 3\ 1\ 2 = t$ と同じ効果。
 $t \{(t \{v\}) \rightarrow t \{3\ 1\ 2 \rightarrow 2\ 3\ 1 = s$ と同じ効果。
 $t \{(s \{v\}) \rightarrow t \{2\ 3\ 1 \rightarrow 1\ 2\ 3 = e$ と同じ効果。
 $s \{(t \{v\}) \rightarrow s \{3\ 1\ 2 \rightarrow 1\ 2\ 3 = e$ と同じ効果。
 $t \{(s \{v\}) \rightarrow t \{2\ 3\ 1 \rightarrow 1\ 2\ 3 = e$ と同じ効果。

これから、群の乗積表を作れば、

| | | | |
|---|---|---|---|
| | e | s | t |
| e | e | s | t |
| s | s | t | e |
| t | t | e | s |

さらに、 s と t は互いに逆元である事も判る。
 検討しよう。 逆元 t_i は $(1\ 2\ 3 \rightarrow 3\ 1\ 2)$ の逆元故、
 $(3\ 1\ 2 \rightarrow 1\ 2\ 3)$ で、これを (J 言語で) ソートし直せば、
 $(1\ 2\ 3 \rightarrow 2\ 3\ 1)$ となり、これは 元 s である。

- 2) $A_4 = \{1, a, b, r, c, d, e, f, s, g, h, t\}$ 、
 ただし $1 =$ 上 $(1\ 2\ 3\ 4)$
 下 $(1\ 2\ 3\ 4)$ 、

$r = \begin{matrix} \text{上} & (1\ 2\ 3\ 4) \\ \text{下} & (2\ 1\ 4\ 3) \end{matrix}$
 $s = \begin{matrix} \text{上} & (1\ 2\ 3\ 4) \\ \text{下} & (3\ 4\ 1\ 2) \end{matrix}$
 $t = \begin{matrix} \text{上} & (1\ 2\ 3\ 4) \\ \text{下} & (4\ 3\ 2\ 1) \end{matrix}$
 互換で $(1\ 2)(3\ 4)$ 、 $(1\ 3)(2\ 4)$ 、 $(1\ 4)(2\ 3)$ 、

$a = (1)(2\ 3\ 4)$ 、 $b = (1)(2\ 4\ 3)$ 、 $c = (4)(1\ 2\ 3)$ 、 $d = (3)(1\ 2\ 4)$ 、
 $e = (4)(1\ 3\ 2)$ 、 $f = (2)(1\ 3\ 4)$ 、 $g = (3)(1\ 4\ 2)$ 、 $h = (2)(1\ 4\ 3)$ 。

これから群表を作れば、 12×12 の大表になる。 一部のみを示す。
 1 は単元である。 表の対角線に対して、対称である。

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| — | 1 | a | b | r | c | d | e | f | s | g | h | t |
| 1 | 1 | | | | | | | | | | | |
| a | | 1 | | | | | | | | | | |
| b | | 1 | | | | | | | | | | |
| r | | | | 1 | | | | | | | | |
| c | | | | | | | | 1 | | | | |
| d | | | | | | | | | | 1 | | |
| e | | | | | 1 | | | | | | | |
| f | | | | | | | | | | | 1 | |
| s | | | | | | | | | 1 | | | |
| g | | | | | 1 | | | | | | | |
| h | | | | | | | 1 | | | | | |
| t | | | | | | | | | | | | 1 |

この表は、群論の教科書や数学事典類で、見る事が出来る。
 勿論、J 言語で、 A_3 の場合同様に、作成も可能である。

性質：

- 8) A_4 の内、位数 2 の部分群は 3ヶ、
 $\{1, r\}$ 、 $\{1, s\}$ 、 $\{1, t\}$ である。
- 2) A_4 の内、位数 3 の部分群は 4ヶ、
 $\{1, a, b\}$ 、 $\{1, c, e\}$ 、 $\{1, d, g\}$ 、 $\{1, e, f\}$
- 3) A_4 の内、位数 4 の部分群は 1ヶ、
 $\{1, r, s, t\}$ = 実は、前稿 (文献 1) で述べたが
 $Klein$ の4元群と同型である。今は正規部分群である。
 元来、 A_4 も 4 次対称群 S_4 の正規部分群である。
 ある群 G が可換群 (アーベル群) であれば、その部分群は
 正規部分群であるのだ。
- 4) ラグランジュの定理によれば、 A_4 の位数は $4! / 2 = 12$ は、
 その部分群の位数と倍数・約数の関係にある。
 その約数の最高 6 に相当する部分群は、今は無い。
- 9) V_4 の A_4 における 指数 $[A_4 : V_4] = 12 / 4 = 3$ である。
 A_4 / V_4 の位数は 3 で、それは奇数故、巡回群であるので、
 可換群であるので、正規鎖 $A_4 \supset V_4 \supset 1$ を持つ。
 それ故、 A_4 は可解群である。 (対称群 S_4 も可解群である。)

○ 4) 4元数群

実際に演算をトライすれば、 $ij(-i)(-j)=ij(ij)=(-k)(-k)=kk = -1$
等々から、最終的に残る元は、1 と -1 の 2種類のみとなる事が
判る。即ち、群 Z_2 である。

(注意) この群は、 $ij \neq ji$ であるから、可換群では無いが、可解群では
ある。

4. 可解群 に関する 諸定理

10) Burnside の定理： 位数が $p^a \cdot q^b$ (p, q は素数) の群は可解群である。

11) Feit-Thomson の定理： 位数が奇数である群は可解群である。

この証明は有限群論についての最近 (1963) の大成果であって、300ページ
にもなる程だと云う (文献3)。

12) 位数 1 ~ 59 までの群は、全て可解群である。 位数 60 の群に、5次交代群
があるが、可解群では無い。 上記 2 定理以外の理由で、可解群になるものの
位数を (因数分解して) 示せば、次の通り。

2, 2^2 , $2 \cdot 3$, 2^3 , $2 \cdot 5$, $2^2 \cdot 3$, $2 \cdot 7$, 2^4 , $2 \cdot 3^2$, $2^2 \cdot 5$,
 $2 \cdot 11$, $2^3 \cdot 3$, $2 \cdot 13$, $2^7 \cdot 7$, $2 \cdot 3 \cdot 5$, 2^5 , $2 \cdot 17$, $2^2 \cdot 3^2$,
 $2 \cdot 19$, $2^3 \cdot 5$, $2 \cdot 3 \cdot 7$, $2^2 \cdot 11$, $2 \cdot 23$, $2^4 \cdot 3$, $2 \cdot 5^2$,
 $2^2 \cdot 13$, $2 \cdot 3^3$, $2^3 \cdot 7$, $2 \cdot 29$

この内、上記の 3 行目、後ろから 2つ目の $2^4 \cdot 3 = 48$ が問題の
位数である。

(数学的には、答が出て居るのだが、計算的には、解を示すべきなのだろう。

5. む す び

この辺の問題は、18世紀以来、そうそうたる大学者によって研究されて来た
分野である。 ラグランジュ、アーベル、ガロア、ジョルダン、ケーリー、
クロネッカー、フロベニウス 等々。 高級な概念の山あり谷あり、流石の
我等の J 言語といえども、何時でも、快刀乱麻の威力を発揮出来るとは限らぬ。
昨年1月の例会報告、JAPLA 2008/Jan/26 で、私は「5次方程式 Quintic
Equation の 話題 (その1)】 (文献 4) を述べたが、あの時はJ言語の
威力を十分に体感した。 なにしろ、5次方程式の「判別式」まで付録に出来
たのだから！ しかし、「何時もそうだと限らぬ」が、今回の感想である。
今後さらに、JAPLA 会友諸賢の応援をお願いしたい！

文 献

- 0) 中野・西川・山下「群論演習 と J (その 0)、志村論文を応援して」
Proceedings JAPLA 2005

- 1) 中野嘉弘 「群論演習 と J (その1)」
JAPLA 2009/4/25 群表1.txt pp. 8
- 2) http://detail.chiebukuro.yahoo.co.jp/qa/question_detail/q1326192808
- 3) 横田一郎著「群論入門」 p.155、現代数学社、1997.6.20、pp.212、¥2,600
- 4) 中野嘉弘 「5次方程式 Quintic Equation の話題 (その1)」
JAPLA 2008/1/26 Quint.doc pp.11