指数3の無限群が無限可換部分群をもつことの初等的証明

指数3の無限群が無限可換部分群をもつことの初等的証明

新井　広 *

(受領日：2019 年 5 月 7 日)

高知工科大学共通教育教室
〒782–8502 高知県香美市土佐山田町宮ノ口 185

* E-mail: arai.hiroshi@kochi-tech.ac.jp

要約：数学において、群とは、二項演算を備えた集合で、群の公理と呼ばれる条件を満たすものである。群 G の指数とは G の任意の元 g に対して $g^n = e$（単位元）となるような最小の数 n のことである。群 G の部分集合 H が G の演算と同じ演算で群になるとき、H は G の部分群であるという。群 G が可換群であるとは G の任意の 2 元 a、b に対して $ab = ba$ が成り立つことである。本論文の主定理は「指数 3 の無限群は無限可換部分群を持つ」ということである。この定理はバーンサイドの定理とシローの定理を用いて証明することもできるが、ここでは、群論の初学者でも簡単に理解できるように、深遠な定理を用いない証明を与える。

1. 群の定義

1.1 定義の前に

大学初年級で初めて群を学ぶ学生たちでも意識していないだけで群の実例は知っている。整数、有理数、実数、複素数、そのいずれかを和という演算の入った集合ととらえればそれは群になっている。有理数、実数、複素数、そのいずれかから 0 を除いた集合を積という演算の入った集合ととらえればそれは群になっている。

1.2 二項演算

既に「演算」や「和」や「積」という言葉を断りなく用いた。ここで「二項演算」を定義しておこう。

定義 1. 集合 A の 2 つの元の組に集合 A の 1 つの元を対応させる写像を A 上の二項演算という。

実数の演算として通常用いられている和･差･積･商を考えるとき、和は自然数上の二項演算であり、差は整数上の二項演算であるが、差は自然数上の二項演算ではない。$3 - 5 = -2$ は自然数ではないからである。同様に、積は実数上の二項演算であるが、商は実数上の二項演算ではない。しかし商は 0 を除いた実数の二項演算にはなっている。

同様に n を 3 以上の自然数として n 項演算も定義されるが、ここでは二項演算しか用いない。二項演算を単に演算ということもある。

二項演算は写像による (a, b) の像（演算結果）をあらわす記法があると便利である。実数の通常の積などを考える場合にならって、一般の二項演算による (a, b) の像を ab と書き、a と b の積と呼ぶことが多い。その場合写像の対応は $(a, b) \mapsto ab$ とあらわす。二項演算として実数の通常の和を考える場合などはその限りではなく (a, b) の像は $a + b$ とあらわす。その場合写像の対応は $(a, b) \mapsto a + b$ とあらわし、a と b の和と呼ぶ。

1.3 群

定義 2. 単位元と呼ばれる特別な元をもつ集合 G 上に二項演算 $(a, b) \mapsto ab$ が定義され、その演算が次の性質をみたすとき、集合 G はその二項演算に関して群をなすという。 考えている演算が明らかである場合は単に G は群であるともいう。

（結合法則）G の任意の元 a、b、c に対して

$$(ab)c = a(bc)$$

（単位元の性質）単位元を e とするとき、G の任意の元 a に対して

$$ae = ea = a$$

（逆元の存在）G の任意の元 a に対して

$$ab = ba = e$$

となるような G の元 b が存在する。（このような b は 1 つに定まり a の逆元といい、a^{-1} とあらわす。）

注意 3. 以降、e は単位元をあらわすものとする。

例 4. 整数 $\mathbb{Z}$、有理数 $\mathbb{Q}$、実数 $\mathbb{R}$、複素数 $\mathbb{C}$ のそれぞれは、通常用いられている和 $(a,b) \mapsto a+b$ に関して群をなす。単位元は 0 である。次が成り立つことは容易に確かめられる。$\mathbb{Z}$ の任意の元 a、b、c に対して

$$(a+b)+c = a+(b+c)$$
$$a+0 = 0+a = a$$
$$a+(-a) = (-a)+a = 0$$

例 5. 有理数 $\mathbb{Q}$、実数 $\mathbb{R}$、複素数 $\mathbb{C}$ のそれぞれは、通常用いられている積に関して群をなすことはない。結合法則はみたすが、単位元の性質をみたす特定の元が存在しない。0 以外の a に対して $a\times x = x\times a = a$ をみたすものは 1 のみで 1 が単位元の最終候補であるが $1\times 0 = 0\times 1 = 0$ なので 1 も単位元にはなりえない。

例 6. 有理数 $\mathbb{Q}$、実数 $\mathbb{R}$、複素数 $\mathbb{C}$ のそれぞれから 0 を除いたものは、通常の積に関して群をなす。単位元は 1 である。

例 7. 実数を成分とする n 次正方行列のうち行列式が 0 でないものからなる集合を G とおく。G の演算として通常用いられている積を用いれば G はその積に関して群をなす。単位元は単位行列である。a の逆元は a の逆行列である。この群を $\mathrm{GL}(n,\mathbb{R})$ であらわす。

1.4 部分群

定義 8. 群 G の部分集合 H が群 G と同じ演算に関して群となるとき、H は G の部分群であるという。

例 9. 実数 $\mathbb{R}$ を通常の和に関して群とみるとき、整数 $\mathbb{Z}$ は $\mathbb{R}$ の部分群である。

1.5 可換群

定義 10. 群 G の 2 つの元 a、b に対して

$$ab = ba$$

が成立するとき、a と b は可換であるという。

定義 11. 群 G の任意の元 a、b に対して

$$ab = ba$$

が成り立つとき、群 G は可換であるという。

例 12. 整数が通常の和に関してなす群は可換群である。

例 13. $n \geqq 2$ のとき、$\mathrm{GL}(n,\mathbb{R})$ は可換群ではない。

1.6 指数 n の群

まず実数の累乗にならって群の元の累乗を定義しよう。

定義 14. a を群 G の元とし、n を 2 以上の自然数とするとき、n 個の a の積 $\underbrace{a\cdots a}_{n\text{ 個}}$ を a^n とあらわす。$n = 0, 1$ の場合は別に次のように定める。$a^1 = a$、$a^0 = e$。

定義 15. 群 G の任意の元 a に対して $a^n = e$ となるような n のうち最小のものが 3 であるとき、G は指数 3 の群であるという。

例 16. a を単位元 e と異なるものとし、$a^2 \neq a$、$a^3 = e$ と定めると $G = \{e, a, a^2\}$ は指数 3 の群である。

2. 主定理

2.1 主定理の主張

以上の準備で、主定理の主張を理解することができる。

定理 17. 指数 3 の無限群が無限可換部分群をもつ

指数 3 の群の例として先ほど示したものは有限群であった。いくつかの準備をしてから指数 3 の無限群の例を示そう。

定義 18. n を 0 以上の整数とするとき、n を 3 で割ったあまりを $[n]_3$ であらわし、

$$\mathbb{F}_3 = \{[0]_3, [1]_3, [2]_3\}$$

とおく。

注意 19. $\mathbb{F}_3$ には自然に和と積

$$[m]_3 + [n]_3 = [m+n]_3$$
$$[m]_3 \times [n]_3 = [m\times n]_3$$

が定義される。

定義 20.

$$\mathbb{F}_3[X] = \left\{ \sum_{n=0}^{\infty} a_n X^n \;\middle|\; a_n \in \mathbb{F}_3 \quad (n = 0, 1, 2, \ldots) \right\}$$

例 21.

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b, c \in \mathbb{F}_3[X] \right\}$$

とおくと G は指数 3 の無限非可換群である。

$$A = \left\{ \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| \, b \in \mathbb{F}_3[X] \right\}$$

は G の無限可換部分群である。

3. 主定理の証明とその準備

3.1 指数 3 の群の共役類は可換

定理の証明に重要な役割を果たす補題を述べるために準備をする。

定義 22. 群 G の元 a、b に対して $b = g^{-1}ag$ となるような G の元 g が存在するとき、$g^{-1}ag$ を a^g であらわす。a と b は共役であるという。

また、a と共役な元全体を a の共役類といい、a^G であらわす。すなわち

$$a^G = \{a^g \mid g \in G\}$$

補題 23. G を指数 3 の群、a を G の元とするとき、a^G の任意の 2 元は可換である。

この補題を示す前にいくつかの性質を述べておく。

命題 24. G を指数 3 の群、a、g を G の元とするとき、次が成り立つ。

$$\begin{aligned} g^{-1} &= g^2 \\ (ag)^{-1} &= (ag)^2 \\ (ag)^{-1} &= g^2a^2 \end{aligned}$$

補題 23 を示す前に、補題の特殊な場合の命題を述べ、証明しておく。

命題 25. G を指数 3 の群、a を G の元とするとき、共役類 a^G の元と a は可換である。

証明 26. g を G の元とするとき、

$$\begin{aligned} & aa^g \\ &= ag^2ag \\ &= ag^2ag^2g^2 \\ &= (ag^2)^{-1}g^2 \\ &= ga^2g^2 \end{aligned}$$

また

$$\begin{aligned} & a^ga \\ &= (g^2ag)a \\ &= g(ga)(ga) \\ &= g(ga)^{-1} \\ &= ga^2g^2 \end{aligned}$$

よって

$$aa^g = a^ga$$

ここで、もし群の同型や同型写像についての知識があれば命題 25 から補題 23 は直ちに導かれるのだが、ここではきちんと示しておく。

証明 27. 補題 23 を証明する。h, g を G の元とする。

$$\begin{aligned} & a^ha^g \\ &= (h^{-1}ah)(g^{-1}ag) \\ &= h^{-1}ahg^{-1}ag(h^{-1}h) \\ &= h^{-1}a(hg^{-1})a(gh^{-1})h \end{aligned}$$

ここで $\hat{g} = gh^{-1}$ とおけば $\hat{g}^{-1} = hg^{-1}$ となるので

$$\begin{aligned} & h^{-1}a(hg^{-1})a(gh^{-1})h \\ &= h^{-1}(aa^{\hat{g}})h \end{aligned}$$

ここで命題 25 をもちいれば

$$\begin{aligned} & h^{-1}(aa^{\hat{g}})h \\ &= h^{-1}(a^{\hat{g}}a)h \\ &= h^{-1}\hat{g}^{-1}a\hat{g}ah \\ &= h^{-1}\hat{g}^{-1}a\hat{g}ah \\ &= h^{-1}hg^{-1}agh^{-1}ah \\ &= a^ga^h \end{aligned}$$

3.2 指数 3 の群の共役類が生成する群は可換

指数 3 の群の共役類は可換となった。しかしこれは群ではない。これを拡大して群にしたものが重要な役割を果たす。そこで一般の群で部分集合を拡大して群にすることを定義する。

定義 28. 群 G の部分集合 S に対し、S の元あるいは S の元の逆元を有限個とり、それらの積をとったものの集合を S で生成される部分群といい $\langle S \rangle$ であらわす。すなわち

$$\langle S \rangle = \left\{ s_1^{\sigma_1}s_2^{\sigma_2}\cdots s_n^{\sigma_n} \mid n \text{ は自然数}, s_n \in S, \sigma_n = \pm 1 \right\}$$

注意 29. $\langle S \rangle$ は群になる。

命題 30. S の任意の 2 元が可換なら $\langle S\rangle$ は可換群となる。

証明 31. 命題 30 を証明する。S の任意の 2 元 a,b が可換なとき a と b^{-1} が可換なことがいえればよい。

$$\begin{aligned} ab^{-1} &= (b^{-1}b)ab^{-1} \\ &= b^{-1}(ba)b^{-1} \\ &= b^{-1}(ab)b^{-1} \\ &= b^{-1}a \end{aligned}$$

以上のことから次のことが分かる。

命題 32. 群 G を指数 3 の群とし、a を G の元とするとき、$\langle a^G\rangle$ は G の可換部分群である。

以上のことから指数 3 の群の元 a^G が無限の場合については定理が成立することがわかる。残る問題は a^G が有限の場合である。

3.3 中心化群、剰余類

一般に共役類 a^G が大きいとき、a と可換な元の集合（a の中心化群という）はある意味で逆に小さくなる。そのことを正確に述べるための準備をする。

定義 33. 群 G の元 a と可換であるような G の元の集合を a の中心化群といい、$C_G(a)$ あるいは単に $C(a)$ であらわす。すなわち

$$C_G(a) = C(a) = \{g \in G \mid ag = ga\}$$

定義 34. g を群 G の元とし、H を群 G の部分群とするとき、$Hg = \{hg \mid h \in H\}$ の形の集合を G における H による右側剰余類あるいは右剰余類という。

注意 35. 文献によっては Hg を左側剰余類あるいは左剰余類というので注意が必要である。両側剰余類という概念もあり、その言葉と整合をとるなら左（側）剰余類というのがよさそうだが、右（側）剰余類という本が多いようなのでそれに従った。

２つの剰余類は共通部分を持てば一致する性質がある。

命題 36. g_1, g_2 を群 G の元とし、H を群 G の部分群とするとき、$Hg_1 \cap Hg_2 \neq \emptyset$ ならば $Hg_1 = Hg_2$

証明 37. 命題を証明する。$Hg_1 \cap Hg_2$ の元は H のある元 h_1, h_2 を用いて $h_1g_1 = h_2g_2$ とあらわすことができる。すると $g_2 = (h_2)^{-1}h_1g_1$ となり、

$$Hg_2 = H((h_2)^{-1}h_1g_1) = H(h_1g) = Hg_1$$

となることがわかる。

以上のことから次のことがわかる。

注意 38. 群 G は共通部分を持たない右側剰余類の和集合であらわすことができる。

定義 39. H を群 G の部分群とするとき、G における H による右側剰余類全体の集合を G/H であらわす。すなわち

$$G/H = \{Hg \mid g \in G\}$$

また G/H の濃度（元の個数）を 部分群 H の G での指数 といい、$(G : H)$ であらわす。すなわち

$$(G : H) = |G/H|$$

これで共役類の大きさと中心化群の大きさが相反する傾向にあることを正確に記述する準備が整った。

命題 40. 群 G の元 a に対して

$$|a^G| = (G : C(a))$$

証明 41. 命題を証明する。a^G の元と G/H の元に 1 対 1 の対応をつければよい。自然な対応 $g^{-1}ag \mapsto C(a)g$ が 1 対 1 の対応になることを示せばよい。全射は明らかなので単射であること、すなわち異なる元がこの対応で異なる元に移ることを示せばよい。g、h を G の元とするとき、

$$\begin{aligned} g^{-1}ag &\neq h^{-1}ah \\ agh^{-1} &\neq gh^{-1}a \\ gh^{-1} &\notin C(a) \\ C(a)gh^{-1} &\neq C(a) \\ C(a)g &\neq C(a)h \end{aligned}$$

これで a^G が小さいとき、$G/C(a)$ も小さく、それには $C(a)$ が大きくなければならないことがわかる。

命題 42. a を 無限群 G の元とするとき、a^G が有限集合であるならば、a の中心化群 $C(a)$ は無限群である。

証明 43. $|a^G| = |G/C(a)|$ より $|G/C(a)|$ は有限である。G は共通部分を持たないような有限個の $C(a)$ による剰余類の和集合としてあらわされる。$C(a)$ による剰余類は全て濃度が等しいので、$C(a)$ が有限集合だと G も有限集合となるので矛盾。よって $C(a)$ は無限集合である。

共役類が全て有限なら、全ての元の中心化群は無限であり、可換であるような元の列 $\{a_i\}$ をとっていけそうであるが、この列が有限でとまらないためには、$C(a_1) \cap \cdots \cap C(a_n)$ が十分大きくなければならない。このことを正確に述べるための準備をする。

命題 44. H、K が群 G の指数有限の部分群のとき、$H \cap K$ も G の指数有限の部分群である。

証明 45. $(G : H)$ が有限で $H \subset \langle H \cup K \rangle \subset G$ であるから、$(\langle H \cup K \rangle : H)$ は有限である。a、b を $\langle H \cup K \rangle$ の元とするとき、$Ha \cap Kb$ は $c \in Ha \cap Kb$ なる c を用いて $(H \cap K)c$ とあらわせることに注意すると、

$$(\langle H \cup K \rangle : H) = (K : H \cap K)$$

であることがわかり、$(K : H \cap K)$ が有限となることがわかる。このことと $(G : K)$ が有限であることより $(G : H \cap K)$ は有限であることがわかる。

補題 46. 群 G の任意の共役類が有限のとき、群 G の可換な元の無限列 $\{a_i\}$ をとることができる。

証明 47. G から任意に元を選び a_1 とおく。$C(a_1)$ は無限集合なので a_1 と異なる元 a_2 を $C(a)$ から選ぶことができる。$C(a_1) \cap C(a_2)$ は G の部分群となり、$(G : C(a_1) \cap C(a_2))$ は有限なので、$C(a_1) \cap C(a_2)$ は無限集合であり、そこから a_1, a_2 と異なる元 a_3 を選ぶことができる。以下同様にすれば、可換な元の無限列 $\{a_i\}$ をとれることがわかる。

3.4 主定理の証明

証明 48. 主定理を証明する。群 G の指数は 3 なので、補題 23 より全ての共役類は可換である。共役類に無限であるようなもの a^G があれば、命題 30 より $\langle a^G \rangle$ が無限可換部分群となる。共役類が全て有限の場合、補題 46 より可換な無限列 $\{a_i\}$ がとれるので、やはり命題 30 より $\langle \{a_i\} \rangle$ が無限可換部分群となる。いずれの場合でも無限可換部分群の存在がいえる。

4. 終わりに

「指数 3 の無限群は無限可換部分群をもつか」。この問題に接したのは 20 年以上昔のことである。初等的な証明ができると予想し、すぐに証明することができた。出題された方は数学基礎論の研究者で、有限群の知識を使えば証明できると踏んでおられ、後に実際にその方針で証明された。元々は別の問題から派生して考えられた問題であったが、大元の問題が何だったか思い出せず、継続した考察をせずに時が経過してしまった。ある時ネット上で数学基礎論を群論に応用している話題の解説を見た。その中の証明のついていない命題の証明を考えていたら、「指数 3 の無限群は無限可換部分群をもつ」ことを利用すればその命題が証明できることに気づき久しぶりにこの話題を思い出した。折角なので折に触れて何人かの方に話題にしてみた。数学基礎論の研究者に話題提供した際に、初等的な証明でなく、前述の有限群の知識を用いる手法で証明を付けた方もおられた。初等的な証明をする方がなかなか見つからなかったが、本学の関口晃司先生に話題提供したところ、興味を持たれ、いくつかの質問をされ、他に関連する話がないか考えて下さり、何か見つかったら共著で論文を書こうと約束をかわしたが、誠に残念なことに関口先生は亡くなられた。関口先生が初等的な方法で証明をつけて下さっていたことを知ったのは亡くなられた後のことである。改めて関口先生のご冥福をお祈りする。もう関口先生との約束は果たせないので、関連する話題の有る無しにこだわらず 現状までのところをまとめることにした。有限群の研究者にも話題提供してみたが、このようなことはあまり考えられていないのではないかというコメントを頂いた。初等的な証明は広く知られているわけではないようなので、それを知らせるだけでも少しは意味があると考えた。少しでも書く意義を大きくするために、仮想読者を群論初学者として、その勉強道具の一つの材料となりうることを心掛けた。定義はこの話題に沿うような形に変えたものがある。正規部分群や同型定理など初学者に紹介するのに適当な話題を絡めて書くことも出来たが、紙数の関係でそれは控えることにした。それらが良かったどうかは、現時点ではわからない。

文献

1) 浅野 啓三, 永尾 汎, “群論”, 岩波書店, 1965.
2) 斎藤正彦, “はじめての群論”, 日本評論社, 2005.
3) W. Burnside, ”On an unsettled question in the theory of discontinuous groups” Quart. J. Pure Appl. Math., 33 (1902) pp. 230238
4) W. Burnside, ”Theory of Groups of Finite Order” Cambridge University Press, 2nd ed., 1911

An Elementary Proof of the Existence of an Infinite Abelian Subgroup of an Infinite Group of Exponent 3

Hiroshi Arai*

(Received: May 7th, 2019)

Core Studies, Kochi University of Technology
185 Miyanokuchi, Tosayamada, Kami City, Kochi 782–8502, JAPAN

* E-mail: arai.hiroshi@kochi-tech.ac.jp

Abstract: In mathematics, a group is a set equipped with a binary operation which combines any two elements to form a third element under some conditions called the group axioms. The exponent of a group G is the least natural number n such that $g^n = e$ (the identity element) for all $g \in G$. A subset H of a group G is called a subgroup of G if H also forms a group under the same operation of G. A group G is a commutative group, if $ab = ba$ for all $a, b \in G$. The main theorem of this paper is as follows: A group of exponent 3 has a infinite commutative subgroup. We can prove this theorem by using the Burnside Theorem and Sylow Theorem, but we will show a proof without profound theorems, so that even beginners of group theory should be able to easily understand it.