

有限群の p 部分群と斜準同型写像について
On p -subgroups and crossed homomorphisms of finite groups

浅井 恒信 (近畿大学) 庭崎 隆 (愛媛大学)
Tsunenobu Asai (Kinki University) Takashi Niwasaki (Ehime University)

本講演の内容は、竹ヶ原裕元氏 (室蘭工業大学)、千吉良直紀氏 (熊本大学) との共同研究に基づくものである。

1 予想, 及び関連する命題

有限群 A は有限群 G に群の自己同型として作用しているとする。写像 $\lambda: A \rightarrow G$ が斜準同型写像であるとは

$$\lambda(ab) = \lambda(a) \cdot {}^a(\lambda(b)), \quad a, b \in A$$

を満たすときにいう。これは

$$\tilde{\lambda}: A \rightarrow G \rtimes A, \quad a \mapsto \lambda(a)a$$

が群の準同型写像となることと同値である。ここで、 $G \rtimes A$ は G と A の半直積群を表す。 A から G への斜準同型写像全体のなす集合を $Z^1(A, G)$ で表す。また、 A の交換子群を A' と書く。斜準同型写像の個数 $|Z^1(A, G)|$ に関して、次の合同式が成り立つことが予想されている。

予想 1 ([5]). $|Z^1(A, G)| \equiv 0 \pmod{\gcd(|A/A'|, |G|)}$

この予想は、幾つかの特別な場合に成り立つことが確かめられている ([2], [3], [4], [5], [6], [8] 等)。本稿の内容に特に関わるのは、次の場合である。これらにおいて、有限群 G 及びその上の作用は任意でよい。

- A が巡回群の場合 (Frobenius の定理, Hall の定理)。
- $A = C \times E$ で、 C は巡回 p 群, E は初等可換 p 群の場合。ここで p は素数。

さて、予想 1 における交換子群を、 A の一般の正規部分群 A_1 に置き換えて、合同式

$$|Z^1(A, G)| \equiv 0 \pmod{\gcd(|A/A_1|, |G|)}$$

が成り立つ条件を考察し、次の結果を得たことを第 28 回代数的組合せ論シンポジウムで報告した ([1])。ここで、自然数 n に対し、 n_p は n を割る最大の p 巾 (即ち p -part) を表す。

定理 2. A_1 を A の正規部分群とする。 $|A/A_1|$ を割る任意の素数 p に対して、 $A_1 \leq B \trianglelefteq A$ で $|A/B| = |A/A_1|_p$ となる B が存在して、任意の $\lambda \in Z^1(A, G)$, 及び $C_G(\tilde{\lambda}(B))$ の $\tilde{\lambda}(A/B)$ 不変な任意の p 部分群 K に対して、

$$|Z^1_\lambda(A/B, K)| \equiv 0 \pmod{\gcd(|A/B|, |K|)}$$

が成り立つとする。このとき

$$|Z^1(A, G)| \equiv 0 \pmod{\gcd(|A/A_1|, |G|)}$$

が成り立つ。

なお、全ての素数 p について上記の部分群 B が存在することは、 A/A_1 が巾零群であることと同値であることに注意する。

定理 2 を用いることにより、以下のことが証明できる (または同様の議論が証明に使われた)。

定理 3. 全ての素数 p と、アーベル p 群 A , 及び一般の有限群 G に対し、

$$|Z^1(A, G)| \equiv 0 \pmod{\gcd(|A|, |G|_p)}$$

が成り立つならば、予想 1 は正しい。

定理 4 ([5]). 一般の有限群 A, G に対して、

$$|Z^1(A, G)| \equiv 0 \pmod{\gcd(|A/A' : \Phi(A/A')|, |G|)}$$

が成り立つ。ここで、 $\Phi(A/A')$ は A/A' のフラッチニ部分群である。

命題 5. A の正規部分群 B と、 A/B が作用する G の任意の部分群 H に対し、

$$|Z^1(A/B, H)| \equiv 0 \pmod{\gcd(|A/B|, |H|)}$$

が成り立つならば、

$$|Z^1(A, G)| \equiv 0 \pmod{\gcd(|A/B|, |G|)}$$

が成り立つ。

命題 6. K を G の部分群とし、 K_A を K の A 不変な最大の部分群とする。このとき、もし

$$|Z^1(A, K_A)| \equiv 0 \pmod{\gcd(|A|, |K_A|)}$$

が成り立つならば、

$$|Z^1(A, G)| \equiv 0 \pmod{\gcd(|A|, |K|)}$$

が成り立つ。

2 例外 p 群の自己準同型写像の個数

定理 2 における仮定部の合同式は、一般には成り立たない。本節では、例外 p 群 P に対して、 $|\text{Hom}(P, P)|_p = |P/P'|$ であることを計算により確かめる。ここで、例外 p 群とは、 $p = 2$ のときは巡回群、二面体群、一般四元数群、準二面体群のいずれか、 p が奇素数のときは巡回群となる p 群を指す。

まず一般に、有限群 P の、 P 自身への自明な作用を考える。このとき、 $Z^1(P, P) = \text{Hom}(P, P) = \text{End}(P)$ は、 P の自己準同型写像全体のなす集合 (モノイド) である。その位数 $|\text{End}(P)|$ は、もし P の部分群 H 達を分類でき、その自己同型群の位数 $|\text{Aut}(H)|$ がすべて分かるならば、次の等式により計算することができる。

$$|\text{End}(P)| = \sum_{N \trianglelefteq P} \sum_{\substack{H \leq P \\ H \simeq P/N}} |\text{Aut}(H)| \quad (1)$$

例 7 (巡回群と初等可換 p 群). p を素数とし、 C_n で位数 n の巡回群を表す。以下のアーベル群の例では、(1) 式を用いずとも $|\text{End}(P)|$ が求まり、それが $|P| = |P/P'|$ で割り切れることが容易に確かめられるが、(1) 式が実際にどのような値を与えているかを示す。

1. $P = C_p$ のとき。

$$|\text{End}(C_p)| = |\text{Aut}(C_p)| + |\text{Aut}(1)| = (p-1) + 1 = p.$$

$|\text{Aut}(C_p)|$ と $|\text{Aut}(1)|$ はいずれも p と互いに素で、足し算を行って初めて p で割り切れること、しかし p で 1 度しか割り切れないことを注意しておく。

2. $P = C_{p^2}$ のとき。

$$|\text{End}(C_{p^2})| = |\text{Aut}(C_{p^2})| + |\text{Aut}(C_p)| + |\text{Aut}(1)| = (p^2 - p) + (p-1) + 1 = p^2.$$

3. $P = C_p \times C_p$ のとき。

P は \mathbb{Z}_p 上の 2 次元ベクトル空間であり、1 次元部分空間 (つまり位数 p の部分群) は $\frac{p^2-1}{p-1} = p+1$ 個ある。 $|\text{Aut}(C_p \times C_p)| = |\text{GL}_2(p)| = (p^2-1)(p^2-p)$ であるから

$$\begin{aligned} |\text{End}(C_p \times C_p)| &= |\text{Aut}(C_p \times C_p)| + (p+1) \cdot (p+1) |\text{Aut}(C_p)| + |\text{Aut}(1)| \\ &= (p^2-1)(p^2-p) + (p+1)^2(p-1) + 1 = p^4. \end{aligned}$$

位数が同じ p^2 であっても、 $P = C_{p^2}$ と $P = C_p \times C_p$ の $|\text{End}(P)|$ は大きく異なっている。一般に、 $|\text{End}(C_{p^n})| = |C_{p^n}| = p^n$ であり、これは p^{n+1} では割り切れない。他方、 $P = C_p \times \cdots \times C_p$ (n 個の直積) のとき、 $|\text{End}(P)| = |M_n(p)| = p^{n^2}$ である。

例 8 (二面体群). $n = 2^m$, $m \geq 0$ として, 位数 $2n$ の二面体群

$$D_{2n} = \langle x, y \mid x^n = y^2 = 1, yxy = x^{-1} \rangle = \langle x \rangle \rtimes \langle y \rangle$$

を考える。 $D_4 = C_2 \times C_2$ であり, $D_2 = C_2$ である。また, $\text{Aut}(D_{2n})$ は次の通りである。

$$\text{Aut}(D_{2n}) \simeq \begin{cases} 1 & (n=1) \\ S_3 & (n=2) \\ \mathbb{Z}_n \rtimes U(\mathbb{Z}_n) & (n \geq 4) \end{cases}$$

ここで, S_3 は 3 次対称群で位数 6, また $U(\mathbb{Z}_n)$ は $\mathbb{Z}_n = \mathbb{Z}/(n)$ の単数群で, $|\mathbb{Z}_n \rtimes U(\mathbb{Z}_n)| = \frac{n^2}{2} = 2^{2m-1}$ である ([2])。

$n=4$ のとき, $|\text{End}(D_8)|$ は次のように計算できる。 D_8 の位数 2 の部分群は 5 個あり, 中心 $Z(D_8) = \langle x^2 \rangle$ だけが正規である。位数 4 (つまり指数 2) の 3 個の部分群はすべて正規で, $\langle x \rangle$ だけが巡回群である。従って

$$\begin{aligned} |\text{End}(D_8)| &= |\text{Aut}(D_8)| + 1 \cdot 2 |\text{Aut}(D_4)| + 3(4+1) |\text{Aut}(D_2)| + |\text{Aut}(1)| \\ &= 8 + 1 \cdot 2 \cdot 6 + 3 \cdot 5 \cdot 1 + 1 = 36. \end{aligned}$$

$n \geq 8$ のときも同様に, 次のように計算できる。

$$\begin{aligned} |\text{End}(D_{2n})| &= |\text{Aut}(D_{2n})| + 1 \cdot 2 |\text{Aut}(D_n)| + 1 \cdot 4 |\text{Aut}(D_{n/2})| + \dots \\ &\quad + 1 \cdot \frac{n}{4} |\text{Aut}(D_8)| + 1 \cdot \frac{n}{2} |\text{Aut}(D_4)| + 3(n+1) |\text{Aut}(D_2)| + |\text{Aut}(1)| \\ &= 2^{2m-1} + 1 \cdot 2 \cdot 2^{2m-3} + 1 \cdot 2^2 \cdot 2^{2m-5} + \dots \\ &\quad + 1 \cdot 2^{m-2} \cdot 2^3 + 1 \cdot 2^{m-1} \cdot 6 + 3(2^m + 1) \cdot 1 + 1 \\ &= (n+2)^2. \end{aligned}$$

なお, $n \geq 2$ のとき, D_{2n} の交換子群は $\langle x^2 \rangle$ であり, $|D_{2n} : \langle x^2 \rangle| = 4$ である。一方, 上の計算結果より

$$|\text{End}(D_{2n})| = n^2 + 4n + 4 \equiv 4 \pmod{2n}$$

であるから, この場合に予想 1 の合同式 (つまり, $|\text{End}(D_{2n})|$ は 4 で割り切れる) は確かに成り立っているが, 8 では割り切れない。

例 9 (一般四元数群). $n = 2^m$, $m \geq 2$ として, 位数 $2n$ の一般四元数群

$$Q_{2n} = \langle x, y \mid x^{n/2} = y^2, yxy = x^{-1} \rangle$$

を考える。 $\text{Aut}(Q_{2n})$ は次の通りである。

$$\text{Aut}(Q_{2n}) \simeq \begin{cases} S_4 & (n=4) \\ \mathbb{Z}_n \rtimes U(\mathbb{Z}_n) & (n \geq 8) \end{cases}$$

ここで, S_4 は 4 次対称群で位数 24 である。

$n = 4$ のとき, $|\text{End}(Q_8)|$ は次のように計算できる。 Q_8 の位数 2 の部分群は中心 $Z(Q_8) = \langle x^2 \rangle$ だけである。位数 4 の 3 個の部分群はすべて正規で, 巡回群である。従って

$$\begin{aligned} |\text{End}(Q_8)| &= |\text{Aut}(Q_8)| + 3 \cdot 1 |\text{Aut}(D_2)| + |\text{Aut}(1)| \\ &= 24 + 3 \cdot 1 \cdot 1 + 1 = 28. \end{aligned}$$

$n \geq 8$ のときも同様に, 次のように計算できる (これは $n = 4$ の場合を含まない)。

$$\begin{aligned} |\text{End}(Q_{2n})| &= |\text{Aut}(Q_{2n})| + 3 \cdot 1 |\text{Aut}(D_2)| + |\text{Aut}(1)| \\ &= \frac{n^2}{2} + 4. \end{aligned}$$

なお, Q_{2n} の交換子群は $\langle x^2 \rangle$ であり, $|Q_{2n} : \langle x^2 \rangle| = 4$ である。一方, 上の計算結果より $|\text{End}(Q_{2n})| \equiv 4 \pmod{2n}$ であるから, この場合にも予想 1 の合同式は成り立っているが, やはり 8 では割り切れない。

例 10 (準二面体群). $n = 2^m$, $m \geq 3$ として, 位数 $2n$ の準二面体群

$$SD_{2n} = \langle x, y \mid x^n = y^2 = 1, yxy = x^{-1+n/2} \rangle = \langle x \rangle \rtimes \langle y \rangle$$

を考える。 $\text{Aut}(SD_{2n}) \simeq 2\mathbb{Z}_n \rtimes U(\mathbb{Z}_n)$ である。一方, SD_{2n} の正規部分群は次のいずれかである。

$$\langle x^j \rangle \simeq C_{n/j} \quad (\text{ただし } j|n), \quad \langle x^2, y \rangle \simeq D_n, \quad \langle x^2, xy \rangle \simeq Q_n, \quad SD_{2n}$$

単位群を除いて, これらはすべて $\langle x^{n/2} \rangle$ を含み, また $SD_{2n}/\langle x^{n/2} \rangle \simeq D_n$ であるので, SD_{2n} の自明でない剰余群は D_n の剰余群, つまり二面体群である。従って, $|\text{End}(SD_{2n})|$ は次のように計算できる。

$$\begin{aligned} |\text{End}(SD_{2n})| &= |\text{Aut}(SD_{2n})| + 1 \cdot 1 |\text{Aut}(D_n)| + 1 \cdot 2 |\text{Aut}(D_{n/2})| + \cdots \\ &\quad + 1 \cdot \frac{n}{8} |\text{Aut}(D_8)| + 1 \cdot \frac{n}{4} |\text{Aut}(D_4)| + 3 \left(\frac{n}{2} + 1 \right) |\text{Aut}(D_2)| + |\text{Aut}(1)| \\ &= 2^{2m-2} + 1 \cdot 1 \cdot 2^{2m-3} + 1 \cdot 2 \cdot 2^{2m-5} + \cdots \\ &\quad + 1 \cdot 2^{m-3} \cdot 2^3 + 1 \cdot 2^{m-2} \cdot 6 + 3(2^{m-1} + 1) \cdot 1 + 1 \\ &= \frac{n^2}{2} + 2n + 4. \end{aligned}$$

なお, SD_{2n} の交換子群も $\langle x^2 \rangle$ であり, $|SD_{2n} : \langle x^2 \rangle| = 4$ である。一方, 上の計算結果より $|\text{End}(SD_{2n})| \equiv 4 \pmod{2n}$ であるから, この場合にも予想 1 の合同式は成り立っているが, やはり 8 では割り切れない。

3 例外 p 群の特徴づけ

本節では、 P を非可換 2 群とする。次は Alperin-Feit-Thompson の定理である。

定理 11 ([9, (4.9)]). P の位数 2 の元の個数を t とおく。もし $t \equiv 1 \pmod{4}$ ならば、 $|P/P'| = 4$ である。

この定理の仮定は、 $|\text{Hom}(C_2, P)| \equiv 2 \pmod{4}$ と同じである。予想 1 は、 A が巡回群の場合には証明されているので、 $|\text{Hom}(C_2, P)|$ は必ず偶数である。従って、この定理の仮定は、 $|\text{Hom}(C_2, P)| \not\equiv 0 \pmod{4}$ と同じである。

次は Taussky の定理と呼ばれている。

定理 12 ([7, Theorem 5.4.5]). もし $|P/P'| = 4$ ならば、 P は例外 2 群である。

これらから、 $|\text{Hom}(C_2, P)| \not\equiv 0 \pmod{4}$ ならば、 P は例外 2 群であることが分かる。また、この逆が成り立つことも容易に確かめることができる。

この命題は Murai-Takegahara により、更に次のように拡張されている。

定理 13 ([10], [11]). ある自然数 r に対して、 $|Z^1(C_{p^r}, P)| \not\equiv 0 \pmod{\gcd(p^{r+1}, |P|)}$ となるならば、 P は例外 2 群である。

このような観点に立つと、前節までの結果から、次のバリエーションに辿り着く。

定理 14. 非可換 2 群 P に対し、 P が例外 2 群であることと、 $|\text{End}(P)| \not\equiv 0 \pmod{8}$ であることは同値である。

証明. P が例外 2 群のとき、主張が正しいことは前節で確かめた。逆に、 P は例外 2 群でないと仮定する。Taussky の定理 (定理 12) より、 $|P/P'| \geq 8$ である。 P の正規部分群 B で、 P/B が位数 8 の可換群となるものが存在する。このとき、 P/B は C_8 , $C_4 \times C_2$, $C_2 \times C_2 \times C_2$ のいずれかに同型であるが、これらの群については予想 1 が解決されており、 $|Z^1(P/B, H)| \equiv 0 \pmod{\gcd(|P/B|, |H|)}$ が任意の有限群 H とその上への作用に対して成り立っている。よって、命題 5 より

$$|\text{End}(P)| = |\text{Hom}(P, P)| \equiv 0 \pmod{\gcd(|P/B|, |P|)} = 8$$

を得る。 □

なお、講演時には「予想 1 が正しければ、定理 14 が成り立つ」と紹介したが、後日竹ヶ原氏から、命題 5 を用いた上記の証明が指摘されたので、ここではそれを掲載させていただいた。

参考文献

- [1] T. Asai and T. Niwasaki, 有限群の斜準同型に関する予想の拡張について, 第 28 回代数的組合せ論シンポジウム報告集 (2011).
- [2] T. Asai, T. Niwasaki and Y. Takegahara, Crossed homomorphisms from rank 2 abelian to exceptional p -groups, *J. Algebra* **270** (2003) 212–237.
- [3] T. Asai and Y. Takegahara, On the number of crossed homomorphisms, *Hokkaido Math. J.* **28** (1999), 535–543.
- [4] T. Asai and Y. Takegahara, $|\text{Hom}(A, G)|$, IV, *J. Algebra* **246** (2001), 543–563.
- [5] T. Asai and T. Yoshida, $|\text{Hom}(A, G)|$, II, *J. Algebra* **160** (1993), 273–285.
- [6] R. Brauer, On a theorem of Frobenius, *American Math. Monthly* **76** (1969), 12–15.
- [7] D. Gorenstein, *Finite Groups*, Chelsea Publishing Company, New York (1980).
- [8] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* (2) **40** (1935), 468–501.
- [9] I. M. Isaacs, *Character theory of finite groups*, Academic Press (1976).
- [10] M. Murai, On the number of p -subgroups of a finite group, *J. Math. Kyoto Univ.* **42** (2002) 161–174.
- [11] M. Murai and Y. Takegahara, Hall's relations in finite groups, *J. Algebra* **271** (2004) 312–326.