乗法群が対称群と同型な skew brace の同型類の数について

お茶の水女子大学　理学部　数学科
新井利沙 (Risa ARAI)

概要

Skew brace とは, 集合 B に $(B, \cdot), (B, \circ)$ が群となる 2 つの二項演算 $\cdot, \circ$ が定義され, brace relation を満たす $(B, \cdot, \circ)$ のことをいう．同じ位数を持つ有限群 G, N に対して $(B, \circ) \cong G, (B, \cdot) \cong N$ となる skew brace $(B, \cdot, \circ)$ の同型類の数 $b(G, N)$ を考察する．本稿では, $G = S_n$ として, $b(G, N)$ の計算結果を紹介する.

1　背景

理論物理学に現れた Yang Baxter 方程式の研究において集合論的解がある ([9]). Yang Baxter 方程式の**集合論的解**とは, X が集合で, 写像

$$r : X \times X \longrightarrow X \times X; (x, y) \mapsto (\sigma_x(y), \tau_y(x))$$

が全単射で,

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r)$$

を満たす組 (X, r) のことである. 各 $x \in X$ に対して, σ_x, τ_x が全単射のとき, 解 (X, r) は**非退化**であるといい, $r^2 = \mathrm{id}_{X \times X}$ となるとき解 (X, r) は **involutive** であるという. Involutive な非退化集合論的解を研究するため, Rump [13] は brace という代数的構造を定義した. ここで, Cedó, Jespers, Okniński [8] により定義された left brace の定義を確認する.

定義 1.1. 次のすべてを満たす 2 つの二項演算 $\cdot, \circ$ が定義された集合 $B = (B, \cdot, \circ)$ を **left brace** という.

(a) $(B, \cdot)$ はアーベル群である.
(b) $(B, \circ)$ は群である.
(c) (brace relation) 任意の $a, b, c \in B$ に対して,

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c)$$

が成り立つ. ここで, a^{-1} はアーベル群 $(B, \cdot)$ における a の逆元である.

この left brace と Rump の brace は同値であることが知られている. 一方, involutive でない非退

化集合論的解も網羅するために Guarnieri, Vendramin [10] が left brace を skew left brace に一般化した.

Skew left brace とは, 定義 1.1(a) がアーベル群に限らず群となり, また (b), (c) も満たす, $(B, \cdot, \circ)$ のことである. 以下, 簡単のため left を省略して, skew brace と呼ぶことにする. Skew brace の分類は, Yang Baxter 方程式の解を構築するために必要な手順の一つであることが知られている.

本稿を通じて, G, N を同じ位数を持つ群とする. $(B, \circ) \cong G, (B, \cdot) \cong N$ となる skew brace の同型類の数を $b(G, N)$ と書くことにする. 様々な G, N について, $b(G, N)$ を計算した先行研究があるので, 紹介する. G, N の位数が squarefree のとき, $b(G, N)$ は [2] により, 計算されている. また, $N = C_2 \times C_2 \times C_4 \times C_4$ のとき $b(G, N)$ の値は [3] によって, そして, $N = C_4 \times C_4 \times C_4$ のとき $b(G, N)$ の値は [4] により計算されている. ただし, C_i は位数 i の巡回群を表す. このように 2 つの群 G, N に対して, $b(G, N)$ の研究が行われている. 本稿では, $b(S_n, N)$ を考える.

2 Skew brace の基本事項

Skew brace は [10] により定義された. 再び skew brace の定義を確認し, 基本事項を紹介する.

定義 2.1. 次のすべてを満たす 2 つの二項演算 $\cdot, \circ$ が定義された集合 $B = (B, \cdot, \circ)$ を **skew brace** という.

(a) $(B, \cdot)$ は群である.
(b) $(B, \circ)$ は群である.
(c) (brace relation) 任意の $a, b, c \in B$ に対して,

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c)$$

が成り立つ. ここで, a^{-1} は群 $(B, \cdot)$ における a の逆元である.

また, 群 $(B, \cdot)$ を skew brace B の**加法群**, 群 $(B, \circ)$ を skew brace B の**乗法群**という.

例 2.2. $N = (N, \cdot)$ を群とする. このとき, 二項演算 $\circ$ を, 任意の $g, h \in N$ に対して,

$$g \circ h = g \cdot h$$

と定義すると, $(N, \cdot, \circ)$ は skew brace となる. 実際, $(N, \cdot)$ は群であるから, $(N, \circ)$ も群となる. また任意の $g, h, k \in N$ に対して,

$$g \circ (h \cdot k) = g \cdot (h \cdot k) = g \cdot h \cdot k$$
$$(g \circ h) \cdot g^{-1} \cdot (g \circ k) = (g \cdot h) \cdot g^{-1} \cdot (g \cdot k) = g \cdot h \cdot k$$

より, brace relation が成り立つ.

例 2.3. $N = (N, \cdot)$ を群とする. このとき, 二項演算 $\circ$ を, 任意の $g, h \in N$ に対して,

$$g \circ h = h \cdot g$$

と定義すると, $(N, \cdot, \circ)$ は skew brace となる．実際, $(N, \cdot)$, $(N, \circ)$ が群になることは明らかであるから, brace relation が成り立つことを確認する．任意の $g, h, k \in N$ に対して,

$$\begin{aligned} g \circ (h \cdot k) = (h \cdot k) \cdot g = h \cdot k \cdot g \\ (g \circ h) \cdot g^{-1} \cdot (g \circ k) = (h \cdot g) \cdot g^{-1} \cdot (k \cdot g) = h \cdot k \cdot g \end{aligned}$$

より, brace relation が成り立つ.

Skew brace に関する基本事項をいくつか確認する.

補題 2.4. $B = (B, \cdot, \circ)$ を skew brace とする．任意の $a, b \in B$ に対して,

$$(a \circ b)^{-1} = a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1}$$

が成り立つ.

Proof. $(B, \cdot, \circ)$ は brace relation を満たすから, 任意の $a, b, c \in B$ に対して,

$$a \circ (c \cdot b) = (a \circ c) \cdot a^{-1} \cdot (a \circ b)$$

が成り立つ．$d = c \cdot b$ とおくと,

$$\begin{aligned} a \circ d &= (a \circ (d \cdot b^{-1})) \cdot a^{-1} \cdot (a \circ b) \\ &= (a \circ d) \cdot a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1} \cdot (a \circ b). \end{aligned}$$

左から, $a \circ d$ の加法逆元, 右から $a \circ b$ の加法逆元をかけると,

$$(a \circ b)^{-1} = a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1}$$

となり示された. □

命題 2.5. $B = (B, \cdot, \circ)$ を skew brace とする．このとき, 次が成り立つ.

(a) 加法群の単位元と乗法群の単位元は一致する.

(b) 任意の $a \in B$ に対して, 写像

$$\gamma_a : B \longrightarrow B; b \mapsto a^{-1} \cdot (a \circ b)$$

は群 $(B, \cdot)$ の自己同型である.

(c) 写像

$$\gamma : (B, \circ) \longrightarrow \mathrm{Aut}(B); a \mapsto \gamma_a$$

は群準同型である．ただし, γ_a は (b) の写像とする.

Proof. (a) 乗法群の単位元を $\tilde{1}$, 加法群の単位元を 1 と書くことにする．$(B, \cdot, \circ)$ は skew brace なので, brace relation が成り立って

$$\begin{aligned} 1 \circ \tilde{1} &= 1 \circ (\tilde{1} \cdot 1) \\ &= (1 \circ \tilde{1}) \cdot 1^{-1} \cdot (1 \circ 1) \\ &= (1 \circ \tilde{1})(1 \circ 1) \\ &= 1 \circ 1 \end{aligned}$$

両辺左から, 1 の乗法逆元をかけると, $1 = \tilde{1}$ となり, 乗法群と加法群の単位元は一致する.
(b) 任意の $a, b, c \in B$ に対して,

$$\begin{aligned}\gamma_a(b \cdot c) &= a^{-1} \cdot (a \circ (b \cdot c)) \\ &= a^{-1} \cdot (a \circ b) \cdot a^{-1} \cdot (a \circ c) \\ &= \gamma_a(b) \cdot \gamma_a(c)\end{aligned}$$

より, γ_a は準同型である. また, $\gamma_a(b) = \gamma_a(c)$ ならば, $a^{-1} \cdot (a \circ b) = a^{-1} \cdot (a \circ c)$ であるから, $b = c$ となり γ_a は単射である. 任意の $c \in B$ に対して, $b = (\bar{a})^{-1} \cdot (\bar{a} \circ c)$ とおけば,

$$\begin{aligned}\gamma_a(b) &= a^{-1} \cdot (a \circ ((\bar{a})^{-1} \cdot (\bar{a} \circ c))) \\ &= a^{-1} \cdot ((a \circ (\bar{a})^{-1}) \cdot a^{-1} \cdot (a \circ \bar{a} \circ c)) \\ &= a^{-1} \cdot (a \circ (\bar{a})^{-1}) \cdot a^{-1} \cdot c \\ &= (a \circ \bar{a})^{-1} \cdot c & &\text{(補題 2.4 より)} \\ &= c\end{aligned}$$

となり, γ_a は全射である. ただし, $\bar{a}$ は a の乗法逆元を表すものとする. よって, 示された.
(c) 任意の $a, b, c \in B$ に対して,

$$\gamma(a \circ b)(c) = \gamma_{a \circ b}(c) = (a \circ b)^{-1} \cdot ((a \circ b) \circ c) = (a \circ b)^{-1} \cdot (a \circ b \circ c)$$

であり,

$$\begin{aligned}(\gamma(a)\gamma(b))(c) &= \gamma_a(b^{-1} \cdot (b \circ c)) \\ &= a^{-1} \cdot (a \circ (b^{-1} \cdot (b \circ c))) \\ &= a^{-1} \cdot ((a \circ b^{-1}) \cdot a^{-1} \cdot (a \circ b \circ c)) \\ &= a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1} \cdot (a \circ b \circ c) \\ &= (a \circ b)^{-1} \cdot (a \circ b \circ c) & &\text{(補題 2.4 より)}\end{aligned}$$

となり, $\gamma(a \circ b) = \gamma(a)\gamma(b)$ が示せた. □

次に, skew brace の同型を定義する.

定義 2.6. $B_1 = (B_1, \cdot_1, \circ_1)$, $B_2 = (B_2, \cdot_2, \circ_2)$ を skew brace とする. このとき, 写像 $\psi : B_1 \longrightarrow B_2$ が, 任意の $a, b \in B_1$ に対して,

$$\begin{aligned}\psi(a \cdot_1 b) &= \psi(a) \cdot_2 \psi(b) \\ \psi(a \circ_1 b) &= \psi(a) \circ_2 \psi(b)\end{aligned}$$

を満たすとき, 写像 ψ を**準同型**, この写像が全単射でもあるとき, 写像 ψ は**同型**という. B_1 から B_2 への同型写像が存在するとき, B_1, B_2 は**同型である**といい, $B_1 \cong B_2$ とかく.

3 Holomorph の正則部分群

以下, $\mathrm{Perm}(N)$ を N の対称群, $\mathrm{Inn}(N)$ を N の内部自己同型群, $Z(N)$ を N の中心とする．また, 任意の $g \in N$ に対して, $C(g)$ は, $C(g) : N \longrightarrow N; n \mapsto gng^{-1}$ を表すとする．

$$\rho : N \longrightarrow \mathrm{Perm}(N); g \mapsto (x \mapsto xg^{-1}),$$
$$\lambda : N \longrightarrow \mathrm{Perm}(N); g \mapsto (x \mapsto gx)$$

とする．また, N の **holomorph** を,

$$\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$$

と定義する．本節では, holomorph の正則部分群と skew brace の関係および holomorph の正則部分群の作り方について考える．定理 3.5, 命題 3.7 で述べるが, 群 N の holomorph $\mathrm{Hol}(N)$ の G と同型な正則部分群を計算し, $\mathrm{Aut}(N)$ によるそれらの共役類を調べることにより, $b(G, N)$ が求められる．

3.1 Holomorph の正則部分群と skew brace の関係

まず, 群作用が正則であることの定義を確認する．

定義 3.1. H を群, $X \neq \emptyset$ を集合とする．$H \times X \longrightarrow X; (\sigma, x) \mapsto \sigma \cdot x$ を左群作用とする．この作用が,

- (推移的) 任意の $x, y \in X$ に対して $\sigma \in H$ が存在して $y = \sigma \cdot x$
- (自由) 任意の $x \in X, \sigma_1, \sigma_2 \in H$ に対して $\sigma_1 \cdot x = \sigma_2 \cdot x$ ならば $\sigma_1 = \sigma_2$

をともに満たすとき, この作用は**正則**であるという．

注意 3.2. H の集合 X への左群作用が推移的であることと, $x_0 \in X$ を固定し, 任意の $y \in X$ に対して, $\sigma \in H$ が存在して $\sigma \cdot x_0 = y$ が成り立つことは同値である．また H の集合 X への左群作用が自由であることと, 任意の $x \in X, \sigma \in H$ に対して, $\sigma \cdot x = x$ ならば $\sigma = 1$ であることは同値である．

命題 3.3. H を $\mathrm{Perm}(N)$ の部分群とすると, $H \times N \longrightarrow N; (\sigma, g) \mapsto \sigma(g)$ は左群作用である．このとき, 次の (a), (b) は同値である．

(a) この作用が正則である．
(b) 写像 $\xi_H : H \longrightarrow N; \sigma \mapsto \sigma(1)$ が全単射である．

これらが成り立つとき, H を**正則部分群**という．

Proof (a)$\Longrightarrow$(b). $\xi_H(\sigma) = \xi_H(\sigma')$ ならば $\sigma(1) = \sigma'(1)$ である．作用は自由であるから, $\sigma = \sigma'$ となる．よって, 写像 ξ_H は単射である．考えている作用は推移的なので, 任意の $g \in N$ に対して, $(\sigma, 1) \mapsto \sigma(1) = g$ となる $\sigma \in H$ が存在する．よって, 写像 ξ_H は全射である． □

Proof (b)$\Longrightarrow$(a). ξ_H は全射であるから, 任意の $g \in N$ に対して, $\sigma(1) = \xi_H(\sigma) = g$ となる $\sigma \in H$ が存在する．よって作用が推移的であることが示せた．また, 任意の $g \in N, \sigma \in H$ に対して,

$\sigma(g) = g$ と仮定する．ξ_H は全単射だから, $\sigma' \in H$ が存在して, $g = \xi_H(\sigma') = \sigma'(1)$ である．よって, 仮定から, $\sigma(\sigma'(1)) = \sigma'(1)$ が成り立つ．$\sigma(\sigma'(1)) = (\sigma\sigma')(1)$ であるから, $\sigma(g) = g$ ならば, $\xi_H(\sigma\sigma') = \xi_H(\sigma')$ であることがわかる．写像 ξ_H は単射であるから, $\sigma\sigma' = \sigma'$ となり, $\sigma = 1$ とわかる．よってこの群作用は自由である． □

例 3.4. $\rho(N)$, $\lambda(N)$ は $\mathrm{Perm}(N)$ の正則部分群である．これは, 写像

$$\begin{aligned} \xi_{\rho(N)} &: \rho(N) \longrightarrow N; \rho(g) \mapsto \rho(g)(1) = g^{-1}, \\ \xi_{\lambda(N)} &: \lambda(N) \longrightarrow N; \lambda(g) \mapsto \lambda(g)(1) = g \end{aligned}$$

は全単射であることからしたがう．

$\mathrm{Hol}(N)$ の正則部分群と, skew brace は密接に関わっている．[10, Theorem 4.2] より次のことがわかる．

定理 3.5. 群 $N = (N, \cdot)$ の holomorph $\mathrm{Hol}(N)$ の正則部分群と, $(N, \cdot, \circ)$ が skew brace となる二項演算 $\circ$ は一対一対応する．$\mathrm{Hol}(N)$ の正則部分群 R を, $\{\gamma_g\}_{g\in N} \subseteq \mathrm{Aut}(N)$ を用いて $R = \{\rho(g)\gamma_g \mid g \in N\}$ と表したとき, R は N 上の二項演算

$$g \circ h = g \cdot \gamma_g(h)$$

と対応し, R は, 対応する二項演算 $\circ$ のなす群 $(N, \circ)$ と同型である．

例 3.6. 正則部分群 $\rho(N)$ に対応する二項演算は例 2.2 の演算である．
実際, $\rho(N) = \{\rho(g)\mathrm{id} \mid g \in N\}$ であるから, 任意の $g, h \in N$ に対して,

$$g \circ h = g \cdot \mathrm{id}(h) = g \cdot h$$

である．
正則部分群 $\lambda(N)$ に対応する二項演算は例 2.3 の演算である．
実際, $\lambda(N) = \{\lambda(g)\mathrm{id} \mid g \in N\} = \{\rho(g)C(g^{-1}) \mid g \in N\}$ であるから, 任意の $g, h \in N$ に対して,

$$g \circ h = g \cdot C(g^{-1})(h) = g \cdot g^{-1} \cdot h \cdot g = h \cdot g$$

である．

次に, この $\mathrm{Hol}(N)$ の正則部分群を用いて, skew brace の同型を表す ([10, Proposition 4.3])．

命題 3.7. $\mathrm{Hol}(N)$ の正則部分群 R_1, R_2 に対して, 対応する二項演算を $\circ_1, \circ_2$ とする．このとき,

$$(N, \cdot, \circ_1) \cong (N, \cdot, \circ_2) \Longleftrightarrow \exists \psi \in \mathrm{Aut}(N) \text{ s.t. } \psi R_1 \psi^{-1} = R_2.$$

定理 3.5, 命題 3.7 より, $b(G, N)$ を調べるために, $\mathrm{Hol}(N)$ の G と同型な正則部分群の数を調べ, それらの $\mathrm{Aut}(N)$ による共役類を考えればよい．次の第 3.2 節では $\mathrm{Hol}(N)$ の正則部分群の作り方を紹介する．

3.2 $\mathrm{Hol}(N)$ の正則部分群の作り方

以下, G, N は有限群とする. 本節では, 交差準同型と fixed point free pair により $\mathrm{Hol}(N)$ の正則部分群を作る方法を紹介する. まず, 交差準同型を用いて $\mathrm{Hol}(N)$ の正則部分群を作る. はじめに交差準同型の定義を確認する.

定義 3.8. 準同型 $\mathfrak{f} : G \longrightarrow \mathrm{Aut}(N)$ が与えられたとき, $\mathfrak{g} : G \longrightarrow N$ が任意の $\sigma_1, \sigma_2 \in G$ に対して,

$$\mathfrak{g}(\sigma_1\sigma_2) = \mathfrak{g}(\sigma_1) \cdot \mathfrak{f}(\sigma_1)(\mathfrak{g}(\sigma_2))$$

を満たすとき, 写像 $\mathfrak{g}$ を $\mathfrak{f}$ **に関する交差準同型**という.

準同型 $\mathfrak{f} : G \longrightarrow \mathrm{Aut}(N)$ に関する交差準同型 $\mathfrak{g} : G \longrightarrow N$ について, $\mathfrak{g}(1) = 1$ である. 実際,

$$\begin{aligned}\mathfrak{g}(1) &= \mathfrak{g}(1) \cdot \mathfrak{f}(1)(\mathfrak{g}(1)) \\ &= \mathfrak{g}(1) \cdot \mathrm{id}(\mathfrak{g}(1)) \\ &= \mathfrak{g}(1) \cdot \mathfrak{g}(1)\end{aligned}$$

よって, $\mathfrak{g}(1) = 1$ である. このことから, 交差準同型は準同型であるとは限らないが, 準同型と同じように単位元を保つことがわかる.

準同型 $\mathfrak{f} : G \longrightarrow \mathrm{Aut}(N)$ と, この $\mathfrak{f}$ に関する全単射交差準同型 $\mathfrak{g} : G \longrightarrow N$ が与えられたとき,

$$R_{(\mathfrak{f},\mathfrak{g})}(G) = \{\rho(\mathfrak{g}(\sigma))\mathfrak{f}(\sigma) \mid \sigma \in G\} \tag{1}$$

は $\mathrm{Hol}(N)$ の G と同型な正則部分群である. また, $\mathrm{Hol}(N)$ の G と同型なすべての正則部分群はこのように作ることができる ([12, Proposition 2.1]).

また, fixed point free pair で正則部分群を作ることができる. まずは fixed point free pair の定義を確認する ([6]).

定義 3.9. $f, g : G \longrightarrow N$ を準同型とする. $f(\sigma) = g(\sigma)$ が成り立つならば, $\sigma = 1$ であるとき, (f, g) を **fixed point free pair** という. (以下, fixed point free pair を fpf pair とかくことにする.)

$f, g : G \longrightarrow N$ を準同型とする. (f, g) が fpf pair であるとき,

$$R_{(f,g)}(G) = \{\rho(g(\sigma))\lambda(f(\sigma)) \mid \sigma \in G\} \tag{2}$$

は $\mathrm{Hol}(N)$ の G と同型な正則部分群である ([6]). また,

$$\begin{aligned}R_{(f,g)}(G) &= \{\rho(g(\sigma))\lambda(f(\sigma)) \mid \sigma \in G\} \\ &= \{\rho(g(\sigma)f(\sigma)^{-1})\rho(f(\sigma))\lambda(f(\sigma)) \mid \sigma \in G\} \\ &= \{\rho(g(\sigma)f(\sigma)^{-1})C(f(\sigma)) \mid \sigma \in G\}\end{aligned}$$

とかける. ここで,

$$\begin{aligned}\mathfrak{f} &: G \longrightarrow \mathrm{Aut}(N); \sigma \mapsto C(f(\sigma)) \\ \mathfrak{g} &: G \longrightarrow N; \sigma \mapsto g(\sigma)f(\sigma)^{-1}\end{aligned}$$

とおくと, $\mathfrak{f}$ は明らかに準同型であり, $\mathfrak{g}$ は $\mathfrak{f}$ に関する全単射な交差準同型である ([12]). 実際, $\mathfrak{g}$ が $\mathfrak{f}$ に関する交差準同型であることについて, 任意の $\sigma, \sigma' \in G$ に対して,

$$\begin{aligned}\mathfrak{g}(\sigma\sigma') &= g(\sigma\sigma') \cdot f(\sigma\sigma')^{-1} \\ &= g(\sigma) \cdot g(\sigma') \cdot f(\sigma')^{-1} \cdot f(\sigma)^{-1} \\ &= g(\sigma) \cdot f(\sigma)^{-1} \cdot f(\sigma) \cdot g(\sigma') \cdot f(\sigma')^{-1} \cdot f(\sigma)^{-1} \\ &= \mathfrak{g}(\sigma) \cdot C(f(\sigma))(\mathfrak{g}(\sigma'))\end{aligned}$$

となり, したがう. $\mathfrak{g}$ が全単射であることについて, $\mathfrak{g}(\sigma) = \mathfrak{g}(\sigma')$ であるとすると, $g(\sigma) \cdot f(\sigma)^{-1} = g(\sigma') \cdot f(\sigma')^{-1}$ であり, $g(\sigma'^{-1}\sigma) = f(\sigma'^{-1}\sigma)$ と変形できる. (f, g) は fpf pair であるから, $\sigma'^{-1}\sigma = 1$ となり, $\sigma = \sigma'$ がいえた. よって, $\mathfrak{g}$ は単射である. G, N は有限群で, 同じ位数を持つので, 全射もしたがう. よって, $\mathfrak{g}$ は全単射で $\mathfrak{f}$ に関する交差準同型である. $R_{(f,g)}(G) = R_{(\mathfrak{f},\mathfrak{g})}(G)$ となるから, 式 (2) の作り方が式 (1) の作り方の一例となることがわかる.

さらに, $Z(N) = \{1\}$ のとき, 式 (1) において $\mathfrak{f}$ の像が $\mathrm{Inn}(N)$ に含まれているならば, 対応する正則部分群は式 (2) の作り方でも作ることができる. 実際, $\mathfrak{f}$ は準同型 $f : G \longrightarrow N$ を用いて,

$$\mathfrak{f} : G \longrightarrow \mathrm{Aut}(N); \sigma \mapsto C(f(\sigma))$$

とかけ,

$$\begin{aligned}R_{(\mathfrak{f},\mathfrak{g})}(G) &= \{\rho(\mathfrak{g}(\sigma))\mathfrak{f}(\sigma) \mid \sigma \in G\} \\ &= \{\rho(\mathfrak{g}(\sigma))C(f(\sigma)) \mid \sigma \in G\} \\ &= \{\rho(\mathfrak{g}(\sigma) \cdot f(\sigma))\rho(f(\sigma)^{-1})\rho(f(\sigma))\lambda(f(\sigma)) \mid \sigma \in G\} \\ &= \{\rho(\mathfrak{g}(\sigma) \cdot f(\sigma))\lambda(f(\sigma)) \mid \sigma \in G\}\end{aligned}$$

とかける. ここで,

$$g : G \longrightarrow N; \sigma \mapsto \mathfrak{g}(\sigma) \cdot f(\sigma)$$

とおくと, $g : G \longrightarrow N$ も準同型で, (f, g) は fpf pair である ([12]). 実際,

$$\begin{aligned}g(\sigma\sigma') &= \mathfrak{g}(\sigma\sigma') \cdot f(\sigma\sigma') \\ &= \mathfrak{g}(\sigma) \cdot C(f(\sigma))(\mathfrak{g}(\sigma')) \cdot f(\sigma) \cdot f(\sigma') \\ &= \mathfrak{g}(\sigma) \cdot f(\sigma) \cdot \mathfrak{g}(\sigma') \cdot f(\sigma)^{-1} \cdot f(\sigma) \cdot f(\sigma') \\ &= \mathfrak{g}(\sigma) \cdot f(\sigma) \cdot \mathfrak{g}(\sigma') \cdot f(\sigma') \\ &= g(\sigma) \cdot g(\sigma')\end{aligned}$$

より, g は準同型である. また, $\sigma \in G$ に対して, $g(\sigma) = f(\sigma)$ ならば, $\mathfrak{g}(\sigma) \cdot f(\sigma) = f(\sigma)$ となり, $\mathfrak{g}(\sigma) = 1$ である. ここで, $\mathfrak{g}(1) = 1$ であり, $\mathfrak{g}$ は単射であるから, $\sigma = 1$ である. よって, (f, g) は fpf pair である. したがって, $R_{(\mathfrak{f},\mathfrak{g})}(G) = R_{(f,g)}(G)$ となるから $R_{(\mathfrak{f},\mathfrak{g})}(G)$ は式 (2) の作り方でも作ることができることがわかる. 特に, $Z(N) = \{1\}$ かつ $\mathrm{Aut}(N) = \mathrm{Inn}(N)$ のとき, $\mathrm{Hol}(N)$ の G と同型な正則部分群は式 (2) の作り方でも作ることができることがわかった ([6], [7]). しかし, N の中心が自明でないとき $\mathrm{Hol}(N)$ のすべての G と同型な正則部分群は式 (2) の作り方で作ることができるとは限らない.

また異なる fpf pair から作られる $\mathrm{Hol}(N)$ の正則部分群が一致する可能性がある. 式 (2) の作り方により作られた, 一致する $\mathrm{Hol}(N)$ の正則部分群について, 次が成り立つ.

命題 3.10. $f, f', g, g' : G \longrightarrow N$ は準同型で, $(f,g), (f',g')$ は fpf pair とする. $Z(N) = \{1\}$ のとき, $\mathrm{Hol}(N)$ の正則部分群 $R_{(f,g)}(G), R_{(f',g')}(G)$ に対して,

$$R_{(f,g)}(G) = R_{(f',g')}(G) \Longleftrightarrow \exists \pi \in \mathrm{Aut}(G) \text{ s.t. } (f,g) = (f' \circ \pi, g' \circ \pi).$$

このように対応する正則部分群が一致する fpf pair は同一視することができる.

4 主定理

$G = S_n$, N を G と同じ位数を持つ群とする. このとき,

$$(B, \circ) \cong G, \ \ (B, \cdot) \cong N$$

となる skew brace $(B, \cdot, \circ)$ の同型類の数 $b(G,N)$ について筆者は考察した. 定理 3.5 より, $\mathrm{Hol}(N)$ の G と同型な正則部分群が存在しない N について, $b(G,N)$ は 0 である. [11] より, $\mathrm{Hol}(N)$ の G と同型な正則部分群が存在するような N は,

$$\begin{aligned} n = 1,2 \text{ のとき } & N \cong S_n \\ n = 3 \text{ のとき } & N \cong S_3, \ C_6 \\ n = 4 \text{ のとき } & N \cong S_4, \ A_4 \times C_2, \ S_3 \times C_2 \times C_2, \ C_6 \times C_2 \times C_2 \\ n \geq 5, n \neq 6 \text{ のとき } & N \cong S_n, \ A_n \times C_2 \\ n = 6 \text{ のとき } & N \cong S_6, \ A_6 \times C_2, \ M_{10} \end{aligned}$$

ただし, C_i は位数 i の巡回群, M_{10} は 10 次のマシュー群を表すとする. 次のことを明らかにした.

定理 4.1.

(1) $n = 1, 2$ のとき

$$b(S_n, S_n) = 1.$$

(2) $n = 3$ のとき

$$b(S_3, S_3) = 2, \ \ b(S_3, C_6) = 1.$$

(3) $n = 4$ のとき

$$b(S_4, S_4) = 4, \ \ b(S_4, A_4 \times C_2) = 4, \ \ b(S_4, S_3 \times C_2 \times C_2) = 4, \ \ b(S_4, C_6 \times C_2 \times C_2) = 3.$$

(4) $n \geq 5, n \neq 6$ のとき

$$b(S_n, S_n) = 2\left(1 + \left\lfloor \frac{n}{4} \right\rfloor\right), \quad b(S_n, A_n \times C_2) = 2\left(1 + \left\lfloor \frac{n-2}{4} \right\rfloor\right).$$

(5) $n = 6$ のとき

$$b(S_6, S_6) = 4, \quad b(S_6, A_6 \times C_2) = 2, \quad b(S_6, M_{10}) = 2.$$

注意 4.2. (2) は [1] の結果である. (3) から (5) について, $b(S_n, S_n)$ $(n \geq 4)$, $b(S_n, A_n \times C_2)$ $(n \geq 5)$ の場合を除き, 数式処理システム Magma [5] を用いて計算した. Magma を用いていない場合について, 第 3 節の内容や [7] を元に, $n \geq 3$ のとき, $Z(S_n) = \{1\}$ であること, そして, $n \neq 6$ のとき, $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ であることを用いて考察した.

5　今後について

今後, 数式処理システム Magma を用いて計算した部分について, 新たに $\mathrm{Hol}(N)$ の正則部分群の構成方法を考えることによりすべての場合について $b(S_n, N)$ を理論値として求めたい.

本稿の執筆および研究を進めるにあたり, Cindy Tsang 助教にご指導を賜りました. 感謝申し上げます.

参考文献

[1] Acri, E.; Bonatto, M. Skew braces of size pq. Comm. Algebra 48 (2020), no. 5, 1872–1881. MR4085764

[2] Alabdali, Ali A.; Byott, Nigel P. Skew braces of squarefree order. J. Algebra Appl. 20 (2021), no. 7, Paper No. 2150128, 21 pp. MR4269712

[3] Ballester-Bolinches, A.; Esteban-Romero, R.; Pérez-Calabuig, V. Enumeration of left braces with additive group $C_2 \times C_2 \times C_4 \times C_4$. Ric. Math., in press.

[4] Ballester-Bolinches, A.; Esteban-Romero, R.; Pérez-Calabuig, V. Enumeration of left braces with additive group $C_4 \times C_4 \times C_4$. Math. Comp. 93 (2024), no. 346, 911–919. MR4678589

[5] Bosma, Wieb; Cannon, John; Playoust, Catherine. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). J. Symbolic Comput. 24 (1997), no. 3-4, 235–265. MR1484478

[6] Byott, Nigel P.; Childs, Lindsay N. Fixed-point free pairs of homomorphisms and nonabelian Hopf-Galois structures. New York J. Math. 18 (2012), 707–731. MR2991421

[7] Carnahan, Scott; Childs, Lindsay. Counting Hopf Galois structures on non-abelian Galois field extensions. J. Algebra 218 (1999), no. 1, 81–92. MR1704676

[8] Cedó, Ferran; Jespers, Eric; Okniński, Jan. Braces and the Yang-Baxter equation. Comm. Math. Phys. 327 (2014), no. 1, 101–116. MR3177933

[9] Drinfeld, V. G. On some unsolved problems in quantum group theory. Quantum groups (Leningrad, 1990), 1–8, Lecture Notes in Math., 1510, Springer, Berlin, 1992. MR1183474

[10] Guarnieri, L.; Vendramin, L. Skew braces and the Yang-Baxter equation. Math. Comp. 86 (2017), no. 307, 2519–2534. MR3647970

[11] Tsang, Cindy. Hopf-Galois structures on a Galois S_n-extension. J. Algebra 531 (2019), 349–360. MR3953015

[12] Tsang, Cindy. Non-existence of Hopf-Galois structures and bijective crossed homomorphisms. J. Pure Appl. Algebra 223 (2019), no. 7, 2804–2821. MR3912948

[13] Rump, Wolfgang. Braces, radical rings, and the quantum Yang-Baxter equation. J. Algebra 307 (2007), no. 1, 153–170. MR2278047