

SKEW BRACE の構成方法とその応用について

お茶の水女子大学 ツァン シンディ (シンイー)

Cindy (Sin Yi) Tsang Ochanomizu University

1 はじめに

Skew brace は Yang–Baxter 方程式の集合論的解の研究において Guarnieri–Vendramin [8] によって定義された代数的構造であり, Rump [9] が導入した brace の一般化である.

定義 1.1. Skew brace とは, 二つの群演算 $\cdot$ と $\circ$ が定義された集合 $A = (A, \cdot, \circ)$ であって,

$$(1.1) \quad \forall a_1, a_2, a_3 \in A : a_1 \circ (a_2 \cdot a_3) = (a_1 \circ a_2) \cdot a_1^{-1} \cdot (a_1 \circ a_3)$$

を満たすものである. 本稿では, 任意の $a \in A$ について, a の群 $(A, \cdot)$ における逆元を a^{-1} と表し, 群 $(A, \circ)$ における逆元を $\bar{a}$ と表す. また, 群 $(A, \cdot)$ と $(A, \circ)$ の単位元は, 同一であることが容易に確かめられ 1 と書く. さらに, 群 $(A, \cdot)$ と $(A, \circ)$ をそれぞれ A の加法群と乗法群と呼ぶ. **Brace** とは, 加法群がアーベル群であるような skew brace のことを言う.

例えば, 群 $(A, \cdot)$ が与えられたとする. このとき, 明らかに $(A, \cdot, \cdot)$ が skew brace となる. このような skew brace は本質的に群と変わらないため **trivial** であると言う. 同様に, 任意の $a, a' \in A$ に対して $a \cdot^{\text{op}} a' = a' \cdot a$ とおくと, 簡単な計算により $(A, \cdot, \cdot^{\text{op}})$ が skew brace となることもわかる. このような skew brace は **almost trivial** であると言う.

本稿の目的は, 群の分解 (第 2 節) と群の半直積 (第 4 節) それぞれを用いた, 群から skew brace を構成する方法を紹介することである. 第 3 節では, 群の分解を用いた構成方法の応用として, 筆者が [11] にて得られた skew brace の加法群と乗法群の関係性に関する研究成果を述べる. 第 5 節では, 群の半直積を用いた構成方法の応用として, 筆者が [7] にて得られた skew brace の位数と性質の関連性に関する研究成果 (Ferrara 氏と Trombetti 氏との共同研究) を報告する.

2 群の分解を用いた構成方法

本節では, 群 $A = (A, \cdot)$ を固定し, 群の分解を用いて $(A, \cdot, \circ)$ が skew brace となる演算 $\circ$ の定め方を考える. 以下の命題はよく知られている事実である. ただし, $\text{Map}(A, A)$ は A から A への写像全体の集合を表すとする.

命題 2.1. 写像 $\lambda : A \longrightarrow \text{Map}(A, A); a \mapsto \lambda_a$ が与えられたとし,

$$\circ : A \times A \longrightarrow A; (a, a') \mapsto a \circ a' := a \cdot \lambda_a(a')$$

とおく. このとき, $(A, \cdot, \circ)$ が skew brace となるのは,

$$(2.1) \quad \forall a \in A : \lambda_a \in \text{Aut}(A), \quad \forall a, a' \in A : \lambda_{a \cdot \lambda_a(a')} = \lambda_a \lambda_{a'}$$

が成り立つとき, かつそのときに限る.

証明. まず, 任意の $a \in A$ に対して, 写像 λ_a は演算 $\circ$ を用いて

$$\lambda_a : A \longrightarrow A; \quad \lambda_a(x) = a^{-1} \cdot (a \circ x)$$

と書けることに注意する. また, 任意の $x_1, x_2 \in A$ に対して,

$$\begin{aligned} \lambda_a(x_1 \cdot x_2) = \lambda_a(x_1) \cdot \lambda_a(x_2) &\iff a \cdot \lambda_a(x_1 \cdot x_2) = a \cdot \lambda_a(x_1) \cdot a^{-1} \cdot a \cdot \lambda_a(x_2) \\ &\iff a \circ (x_1 \cdot x_2) = (a \circ x_1) \cdot a^{-1} \cdot (a \circ x_2) \end{aligned}$$

であるため, 写像 λ_a が A の自己準同型であることと, 式 (1.1) が $a_1 = a$ において成立することは同値である. よって, 以下の証明において, すべての $a \in A$ に対して写像 λ_a が A の自己準同型である, つまり式 (1.1) が成立すると仮定してよい.

さて, $(A, \cdot, \circ)$ が skew brace であるとする. 任意の $a \in A$ に対して, 演算 $\cdot$ と $\circ$ のどちらに関しても a の逆元が存在するため, 写像 λ_a は全単射である. λ_a が A の自己準同型であるとしているため, $\lambda_a \in \text{Aut}(A)$ となる. また, 任意の $a, a', x \in A$ に対して,

$$\begin{aligned} \lambda_{a \cdot \lambda_a(a')}(x) &= \lambda_{a \circ a'}(x) \\ &= (a \circ a')^{-1} \cdot a \cdot a^{-1} \cdot (a \circ (a' \circ x)) \\ &= \lambda_a(a')^{-1} \cdot \lambda_a(a' \circ x) \\ &= \lambda_a(a'^{-1} \cdot (a' \circ x)) \\ &= (\lambda_a \lambda_{a'})(x) \end{aligned}$$

と変形できる. ただし, 下から二番目の等式は, 写像 λ_a が演算 $\cdot$ を保つため従う. 元 $x \in A$ が任意であったため, $\lambda_{a \cdot \lambda_a(a')} = \lambda_a \lambda_{a'}$ が言える. 以上より, 条件 (2.1) が成り立つ.

逆に, 条件 (2.1) が成り立つとする. 式 (1.1) が成立するとしているため, $(A, \circ)$ が群であることを示せたらよい. 群の三つの公理を確認する.

- 結合法則 任意の $a, a', a'' \in A$ に対して, 条件 (2.1) を用いると,

$$\begin{aligned} a \circ (a' \circ a'') &= a \cdot \lambda_a(a') \cdot (\lambda_a \lambda_{a'})(a'') \\ &= (a \circ a') \cdot \lambda_{a \circ a'}(a'') \\ &= (a \circ a') \circ a'' \end{aligned}$$

と変形できる. したがって, 結合法則が成り立つ.

- 単位元の存在 条件 (2.1) の二番目の式に $a = a' = 1$ を代入すると,

$$\lambda_1 \lambda_1 = \lambda_{1 \cdot \lambda_1(1)} = \lambda_1$$

となり, $\lambda_1 \in \text{Aut}(A)$ のため $\lambda_1 = \text{id}_A$ が成り立つ. すると, 任意の $a \in A$ に対して,

$$\begin{aligned} a \circ 1 &= a \cdot \lambda_a(1) = a \cdot 1 = a \\ 1 \circ a &= 1 \cdot \lambda_1(a) = 1 \cdot a = a \end{aligned}$$

が成り立つ. したがって, 群 A の単位元 1 が $(A, \circ)$ の単位元をなす.

- 逆元の存在 任意の $a \in A$ に対して, $\lambda_a \in \text{Aut}(A)$ より逆写像が存在して, 条件 (2.1) の二番目の式に $a' = \lambda_a^{-1}(a^{-1})$ を代入すると,

$$\lambda_a \lambda_{\lambda_a^{-1}(a^{-1})} = \lambda_{a \cdot \lambda_a(\lambda_a^{-1}(a^{-1}))} = \lambda_1 = \text{id}_A$$

となり, $\lambda_{\lambda_a^{-1}(a^{-1})} = \lambda_a^{-1}$ が成り立つ. すると,

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

となるため, 元 $\lambda_a^{-1}(a^{-1})$ が a の $(A, \circ)$ における逆元をなす.

以上より, $(A, \circ)$ は群であり, $(A, \cdot, \circ)$ は skew brace である. □

例えば, $(A, \cdot, \cdot)$ が trivial となる演算 $\cdot$ は自明な写像

$$\lambda : A \longrightarrow \text{Aut}(A); \quad a \mapsto \lambda_a := \text{id}_A$$

と対応し, $(A, \cdot, \cdot^{\text{op}})$ が almost trivial となる演算 $\cdot^{\text{op}}$ は内部自己同型が誘導する写像

$$\lambda : A \longrightarrow \text{Aut}(A); \quad a \mapsto \lambda_a := \text{conj}(a^{-1})$$

と対応する。ただし、各 $a \in A$ に対して、

$$\text{conj} : A \longrightarrow \text{Inn}(A); \quad \text{conj}(a) = (x \mapsto a \cdot x \cdot a^{-1})$$

は A から A の内部自己同型群 $\text{Inn}(A)$ への自然な準同型を表す。

以下の命題は [10, Theorem 2.3] にて言及されており、本質的に [4, Lemma 7.1] と全く同じである。また、命題 2.2 において、 A の自明な分解 $A = A\{1\} = \{1\}A$ から構成される skew brace はそれぞれ trivial と almost trivial である。

命題 2.2. A の部分群 B, C が存在して、

$$A = BC, \quad B \cap C = 1$$

が成り立つとき、各 $a \in A$ について、一意に定まる $b_a \in B, c_a \in C$ を用いて $a = b_a c_a$ と表せる。任意の $a, a' \in A$ に対して、このノーテーションを用いて

$$a \circ a' = a \cdot \text{conj}(c_a^{-1})(a')$$

とおくと、 $(A, \cdot, \circ)$ は skew brace となる。また、乗法群 $(A, \circ)$ は $a \mapsto (b_a, c_a^{-1})$ により $B \times C$ と同型である。

証明. 命題 2.1 より、演算 $\circ$ と対応する写像

$$\lambda : A \longrightarrow \text{Aut}(A); \quad a \mapsto \lambda_a := \text{conj}(c_a^{-1})$$

が条件 (2.1) の二番目の式を満たせばよい。実際、任意の $a, a' \in A$ に対して、

$$(2.2) \quad a \cdot \lambda_a(a') = b_a c_a \cdot c_a^{-1} \cdot b_{a'} c_{a'} \cdot c_a = b_a b_{a'} \cdot c_{a'} c_a$$

と表されるため、元 $a \cdot \lambda_a(a')$ を写像 λ で写すと

$$\lambda_{a \cdot \lambda_a(a')} = \text{conj}((c_{a'} c_a)^{-1}) = \text{conj}(c_a^{-1}) \text{conj}(c_{a'}^{-1}) = \lambda_a \lambda_{a'}$$

が得られる。乗法群の同型類の主張に関しても、同様に (2.2) を用いて容易に示せる。 $\square$

次の命題が与える構成方法は筆者が [14] にて、自身の結果 [11, Proposition 2.7] を改良したものである。乗法群の同型類の主張に関しては、本質的に [2, Corollary 4] より従うものである。また、上述の論文 [2, 11, 14] のどれにおいても、群 A の中心 $Z(A)$ が自明である仮定に基づいているが、本稿の執筆にあたり、この仮定は不要であることが判明した。証明自体は [14, Proposition 3.2] とほぼ全く同じである。

命題 2.3. $\text{Aut}(A)$ の部分群 Φ, Ψ が存在して,

$$\Phi\Psi = \Phi\text{Inn}(A) = \Psi\text{Inn}(A), \quad \Phi \cap \Psi = 1$$

が成り立つとき, 各 $a \in A$ について, 一意に定まる $\phi_a \in \Phi, \psi_a \in \Psi$ を用いて $\text{conj}(a) = \phi_a\psi_a$ と表せる. 任意の $a, a' \in A$ に対して, このノーテーションを用いて

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

とおくと, $(A, \cdot, \circ)$ は skew brace となる. また, 乗法群 $(A, \circ)$ は $a \mapsto (\phi_a, \psi_a^{-1})$ により

$$\{(\phi, \psi) \in \Phi \times \Psi \mid \phi\text{Inn}(A) = \psi\text{Inn}(A)\}$$

へ射影し, その核は群 $A = (A, \cdot)$ の中心 $Z(A, \cdot)$ である.

証明. 命題 2.1 より, 演算 $\circ$ と対応する写像

$$\lambda : A \longrightarrow \text{Aut}(A); \quad a \mapsto \lambda_a := \psi_a^{-1}$$

が条件 (2.1) の二番目の式を満たせばよい. 実際, 任意の $a, a' \in A$ に対して,

$$(2.3) \quad \text{conj}(a \cdot \lambda_a(a')) = \phi_a\psi_a \cdot \text{conj}(\psi_a^{-1}(a')) = \phi_a\psi_a \cdot \psi_a^{-1} \cdot \phi_{a'}\psi_{a'} \cdot \psi_a = \phi_a\phi_{a'} \cdot \psi_{a'}\psi_a$$

と表されるため, 元 $a \cdot \lambda_a(a')$ を写像 λ で写すと

$$\lambda_{a \cdot \lambda_a(a')} = (\psi_{a'}\psi_a)^{-1} = \psi_a^{-1}\psi_{a'}^{-1} = \lambda_a\lambda_{a'}$$

が得られる. 乗法群の同型類の主張に関しても, 同様に (2.3) を用いて容易に示せる. □

3 加法群と乗法群の関係性

本節では, 命題 2.2 と命題 2.3 の応用として, skew brace の加法群と乗法群の関係性に関する研究成果を述べる. まず, 以下の定理の (1) と (2) はそれぞれ [4] と [15] から分かる.

定理 3.1. 有限 skew brace において, 以下が成り立つ.

- (1) 加法群が冪零群であれば乗法群は可解群である.
- (2) 乗法群が冪零群であれば加法群は可解群である.

以下の予想は [15] にて Byott's Conjecture として述べられており, いまだに未解決である. 様々な進展はあったが, 現時点では [5] が最良の結果を示していると考えられる.

予想 3.2. 有限 skew brace において、乗法群が非可解群であれば加法群も非可解群である。

一方で、予想 3.2 の逆は成立しない。具体的な反例については、命題 2.2 もしくは命題 2.3 を使えば、以下のように簡単に作れる。

まず、加法群となる非可解群 $A = (A, \cdot)$ を固定する。 A の部分群 B, C が存在して、

$$A = BC, \quad B \cap C = 1, \quad B, C \text{ は可解群}$$

となるとき、命題 2.2 から得られる skew brace の乗法群 $(A, \circ)$ は $B \times C$ と同型であるため可解群である。例えば、5 次対称群 A_5 について、

$$A_5 = A_4 \langle (12345) \rangle, \quad A_4 \cap \langle (12345) \rangle = 1, \quad A_4, \langle (12345) \rangle \text{ は可解群}$$

が成り立つため、加法群は非可解群の A_5 であって、乗法群は可解群の $A_4 \times C_5$ となる skew brace が存在する。同様に、 $\text{Aut}(A)$ の部分群 Φ, Ψ が存在して、

$$(3.1) \quad \Phi\Psi = \Phi\text{Inn}(A) = \Psi\text{Inn}(A), \quad \Phi \cap \Psi = 1, \quad \Phi, \Psi \text{ は可解群}$$

となるとき、命題 2.3 から得られる skew brace の乗法群 $(A, \circ)$ は正規アーベル部分群 $Z(A, \cdot)$ を持ち、その商群は $\Phi \times \Psi$ の部分群と同型であるため $(A, \circ)$ は可解群である。筆者 [11] は以上の考察を用いて、予想 3.2 の逆の反例となる skew brace の加法群になり得る有限非アーベル単純群を、以下のように分類することに成功した。

定理 3.3. 有限非アーベル単純群 $A = (A, \cdot)$ に対して、以下が同値である。

- (a) $(A, \circ)$ が可解群であって $(A, \cdot, \circ)$ が skew brace となるような演算 $\circ$ が存在する。
- (b) $(A, \cdot)$ が以下のいずれかと同型である。

$$\text{PSL}_3(3), \text{PSL}_3(4), \text{PSL}_3(8), \text{PSU}_3(8), \text{PSU}_4(2), \text{M}_{11}, \text{PSL}_2(q)$$

ただし、 $q \neq 2, 3$ は任意の素数冪を表す。

証明 (b) $\Rightarrow$ (a). 命題 2.3 より $\text{Aut}(A)$ の部分群 Φ, Ψ が存在して、かつ (3.1) が成り立てばよい。実際、 $A \not\cong \text{PSL}_2(q)$ のときは MAGMA [3] を用いて確かめることができ、 $A \cong \text{PSL}_2(q)$ のときは $\Phi\Psi = \text{PGL}_2(q)$ として、 Φ, Ψ をそれぞれ適当な Singer cycle の生成する部分群と一次元部分空間の安定化群とすればよい。詳細は [11] を参照のこと。 $\square$

注 3.4. 命題 2.3 に相当する [11, Proposition 2.7] において、 Φ が $\Phi \cap \text{Inn}(A)$ 上で分裂する仮定があった。しかし、 $A \cong \text{PSU}_3(8)$ のとき、この分裂条件かつ (3.1) を満たす $\text{Aut}(A)$ の部分

群 Φ, Ψ が存在しないため [11] では非常に複雑な MAGMA コードを用いて (a) を示している. のちに示された [2, Corollary 4] によりこの分裂条件は不要であることが分かったため, 証明を上述のように簡略できるようになった.

4 群の半直積を用いた構成方法

本節では, 群 $B = (B, \cdot)$ と $C = (C, \cdot)$ を固定し, 群の半直積を用いて $(B \times C, \cdot, \circ)$ が skew brace となる $B \times C$ 上の演算 $\cdot$ と $\circ$ の定め方を考える. ただし, ここで紹介するすべての構成方法において, $B \times 1$ と $1 \times C$ は trivial な部分 skew brace をなし, それぞれ群 B と C と同一視できる. つまり, 任意の $b, b' \in B, c, c' \in C$ に対して

$$(b, 1) \cdot (b', 1) = (b, 1) \circ (b', 1) = (bb', 1)$$

$$(1, c) \cdot (1, c') = (1, c) \circ (1, c') = (1, cc')$$

が成り立ち, それぞれ群 B と C の演算によって与えられる.

以下の命題は [8, Example 1.4 & Example 1.5] にて言及されており, よく知られているものである. その証明は非常に簡単であるため省略する.

命題 4.1. 以下が成り立つ.

(1) 準同型 $\beta : C \longrightarrow \text{Aut}(B)$ について,

$$\forall b, b' \in B, c, c' \in C : (b, c) \cdot (b', c') = (bb', cc'), (b, c) \circ (b', c') = (b\beta_c(b'), cc')$$

とおくと, $(B \times C, \cdot, \circ)$ は skew brace となる.

(2) 準同型 $\alpha : C \longrightarrow \text{Aut}(B)$ について,

$$\forall b, b' \in B, c, c' \in C : (b, c) \cdot (b', c') = (b\alpha_c(b'), cc'), (b, c) \circ (b', c') = (bb', cc')$$

とおくと, $(B \times C, \cdot, \circ)$ が skew brace となるのは,

$$\forall c, c' \in C : c' \equiv cc'c^{-1} \pmod{\ker(\alpha)}$$

が成り立つとき, かつそのときに限る.

まず, 加法群が $B \rtimes C$ であって乗法群が $B \rtimes C$ であるような skew brace の構成方法を紹介する. 以下の命題は [12, Section 8] によるものであり, $\beta : B \longrightarrow \text{Aut}(C)$ を自明な準同型とすれば命題 4.1 (2) に帰着する.

命題 4.2. 準同型 $\alpha : C \longrightarrow \text{Aut}(B)$, $\beta : B \longrightarrow \text{Aut}(C)$ について,

$$\forall b, b' \in B, c, c' \in C : (b, c) \cdot (b', c') = (b\alpha_c(b'), cc'), (b, c) \circ (b', c') = (bb', c\beta_b(c'))$$

とおくと, $(B \times C, \cdot, \circ)$ が skew brace となるのは,

$$(4.1) \quad \forall b \in B, c, c' \in C : c' \equiv c\beta_b(c')c^{-1} \pmod{\ker(\alpha)}$$

が成り立つとき, かつそのときに限る.

証明. $(B \times C, \cdot)$ と $(B \times C, \circ)$ は明らかに群をなす. 任意の $a_i = (b_i, c_i) \in B \times C$ ($i = 1, 2, 3$) に対して, 簡単な計算により,

$$a_1 \circ (a_2 \cdot a_3) = (b_1 b_2 \alpha_{c_2}(b_3), c_1 \beta_{b_1}(c_2 c_3))$$

$$(a_1 \circ a_2) \cdot a_1^{-1} \cdot (a_1 \circ a_3) = (b_1 b_2 \alpha_{c_1 \beta_{b_1}(c_2) c_1^{-1}}(b_3), c_1 \beta_{b_1}(c_2 c_3))$$

と変形できるため, $(B \times C, \cdot, \circ)$ が skew brace となることと (4.1) は同値である. $\square$

次に, 加法群と乗法群のどちらも $B \rtimes C$ であるような skew brace の構成方法を紹介する. ただし, 演算 $\circ$ を定める際にはひねた半直積を用いる. 以下の命題は [7, Section 3] によるものであり, (1) において $\alpha : C \longrightarrow \text{Aut}(B)$ を自明な準同型とすれば命題 4.1 (1) に帰着する. 命題を提示する前に, 演算 $\cdot$ と $\circ$ の定め方のモチベーションについて説明しよう.

$A = (A, \cdot, \circ)$ を skew brace とする. また,

$$B = (B, \cdot) = (B, \circ), \quad C = (C, \cdot) = (C, \circ)$$

を trivial な部分 skew brace とし, 群として見なす. A は加法 $\cdot$ と乗法 $\circ$ のどちらに関しても

$$(A, \cdot) = B \rtimes C, \quad (A, \circ) = B \rtimes C$$

のように B と C の半直積であるとする. このとき, 任意の $b, b' \in B, c, c' \in C$ に対して

$$(b \cdot c) \cdot (b' \cdot c') = (b\alpha_c(b')) \cdot (cc')$$

$$(4.2) \quad (b \circ c) \circ (b' \circ c') = (b\beta_c(b')) \circ (cc')$$

$$(4.3) \quad (c \circ b) \circ (c' \circ b') = (cc') \circ (\beta_{c'}^{-1}(b)b')$$

を満たす準同型 $\alpha, \beta : C \longrightarrow \text{Aut}(B)$ が誘導される. $b \cdot c$ をペア (b, c) と同一視すれば, 命題 4.2 の演算 $\cdot$ が得られる. $\lambda : (A, \circ) \longrightarrow \text{Aut}(A, \cdot)$ を命題 2.1 によって定まる準同型とする.

(1) 任意の $b \in B, c \in C$ に対して $\lambda_b(c) = b^{-1}cb$ が成り立つとすると,

$$b \circ c = b \cdot \lambda_b(c) = cb c^{-1} \cdot c = \alpha_c(b) \cdot c$$

と変形できるため, $b \circ c$ はペア $(\alpha_c(b), c)$ と対応する. この同一視に基づき (4.2) の等式を書き直せば, 命題 4.3 (1) にある演算 $\circ$ の定め方が得られる.

(2) 任意の $b \in B, c \in C$ に対して $\lambda_c(b) \in B$ が成り立つとすると,

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

と変形できるため, $c \circ b$ はペア $((\alpha_c \lambda_c)(b), c)$ と対応する. この同一視に基づき (4.3) の等式を書き直せば, 命題 4.3 (2) にある演算 $\circ$ の定め方が得られる. 命題 4.3 (2) にある λ は上述の準同型から制限により誘導されるものに当たる.

計算が煩雑になるため, $B = (B, +)$ をアーベル群に限定する.

命題 4.3. ここでは $B = (B, +)$ をアーベル群とし, その演算を $+$ と表記することとする. 準同型 $\alpha : C \rightarrow \text{Aut}(B)$ が与えられたとし,

$$\forall b, b' \in B, c, c' \in C : (b, c) \cdot (b', c') = (b + \alpha_c(b'), cc')$$

とおく. このとき, 以下が成り立つ.

(1) 準同型 $\beta : C \rightarrow \text{Aut}(B)$ について,

$$\forall b, b' \in B, c, c' \in C : (\alpha_c(b), c) \circ (\alpha_{c'}(b'), c') = (\alpha_{cc'}(b + \beta_{c'}(b')), cc')$$

とおくと, $(B \times C, \cdot, \circ)$ が skew brace となるのは,

$$(4.4) \quad \forall c, c' \in C : \alpha_c \beta_{c'} = \beta_{c'} \alpha_c$$

が成り立つとき, かつそのときに限る.

(2) 準同型 $\beta, \lambda : C \rightarrow \text{Aut}(B)$ について,

$$\forall b, b' \in B, c, c' \in C : ((\alpha_c \lambda_c)(b), c) \circ ((\alpha_{c'} \lambda_{c'})(b'), c') = ((\alpha_{cc'} \lambda_{cc'})(\beta_{c'}^{-1}(b) + b'), cc')$$

とおくと, $(B \times C, \cdot, \circ)$ が skew brace となるのは,

$$(4.5) \quad \forall c, c' \in C : \alpha_c \lambda_{c'} = \lambda_{c'} \alpha_c, \alpha_{c'}(\lambda_{cc'} \beta_{cc'}^{-1} - \lambda_{c'} \beta_{c'}^{-1}) = \lambda_c \beta_c^{-1} - \text{id}_B$$

が成り立つとき, かつそのときに限る.

証明. $(B \times C, \cdot)$ は明らかに群をなす. また, (1) と (2) の演算 $\circ$ はそれぞれ全単射

$$B \times C \longrightarrow B \rtimes_{\beta} C; \quad (b, c) \mapsto (\alpha_c^{-1}(b), c)$$

$$B \times C \longrightarrow (B \rtimes_{\beta} C)^{\text{op}}; \quad (b, c) \mapsto ((\alpha_c \lambda_c)^{-1}(b), c^{-1})$$

が同型となるように定まっているため, (1) と (2) のどちらにおいても $(B \times C, \circ)$ は明らかに群をなす. ただし, 上付き文字の op は opposite group を意味する.

(1) において, 任意の $a_i = (\alpha_{c_i}(b_i), c_i) \in B \times C$ ($i = 1, 2, 3$) について,

$$\begin{aligned} a_1 \circ (a_2 \cdot a_3) &= (\alpha_{c_1 c_2 c_3}(b_1 + \beta_{c_1}(\alpha_{c_3}^{-1}(b_2) + b_3)), c_1 c_2 c_3) \\ (a_1 \circ a_2) \cdot a_1^{-1} \cdot (a_1 \circ a_3) &= (\alpha_{c_1 c_2}(\beta_{c_1}(b_2)) + \alpha_{c_1 c_2 c_3}(b_1 + \beta_{c_1}(b_3)), c_1 c_2 c_3) \end{aligned}$$

と変形できる. 計算の詳細は [7] を参照のこと. b_1, b_3 の項はつねに一致する. ゆえに, b_2 の項を比較すれば, $(B \times C, \cdot, \circ)$ が skew brace となることと (4.4) は同値であることを導く.

(2) において, 任意の $a_i = ((\alpha_{c_i} \lambda_{c_i})(b_i), c_i) \in B \times C$ ($i = 1, 2, 3$) について,

$$\begin{aligned} a_1 \circ (a_2 \cdot a_3) &= ((\alpha_{c_1 c_2 c_3} \lambda_{c_1 c_2 c_3})(\beta_{c_2 c_3}^{-1}(b_1) + (\lambda_{c_3}^{-1} c_2^{-1} \alpha_{c_3}^{-1} \lambda_{c_2})(b_2) + \lambda_{c_3}^{-1} c_2^{-1} c_3(b_3)), c_1 c_2 c_3) \\ (a_1 \circ a_2) \cdot a_1^{-1} \cdot (a_1 \circ a_3) &= ((\alpha_{c_1 c_2} \lambda_{c_1})(\lambda_{c_2}(\beta_{c_2}^{-1}(b_1) + b_2) - b_1) + (\alpha_{c_1 c_2 c_3} \lambda_{c_1 c_3})(\beta_{c_3}^{-1}(b_1) + b_3), c_1 c_2 c_3) \end{aligned}$$

と変形できる. 計算の詳細は [7] を参照のこと. b_3 の項はつねに一致する. b_2 の項に着目すると, $(B \times C, \cdot, \circ)$ が skew brace となるためには, 任意の $c, c' \in C$ について $\alpha_c \lambda_{c'} = \lambda_{c'} \alpha_c$ が成立する必要があると分かる. この必要条件を仮定した上で整理して, さらに $\alpha_{c_1 c_2}^{-1} \lambda_{c_1}^{-1}$ で写すと, 上二式にある b_1 の項がそれぞれ

$$(\alpha_{c_3} \lambda_{c_2 c_3} \beta_{c_2 c_3}^{-1})(b_1), \quad (\lambda_{c_2} \beta_{c_2}^{-1})(b_1) - b_1 + (\alpha_{c_3} \lambda_{c_3} \beta_{c_3}^{-1})(b_1)$$

となる. 両者を比較してさらに整理すれば, $(B \times C, \cdot, \circ)$ が skew brace となることと (4.5) は同値であることを導く. $\square$

5 位数と性質の関連性

本節では, 命題 4.3 (2) の応用として, skew brace の位数と性質の関連性に関する研究成果を報告する. まず, 群において, 以下の定理は Dickson [6] によって知られている.

定理 5.1. 自然数 n の素因数分解を $n = p_1^{e_1} \cdots p_d^{e_d}$ としたとき, 以下が同値である.

- (a) 位数 n の群はすべてアーベル群である.
- (b) 任意の $1 \leq i \leq d$ に対して $e_i \leq 2$ であって, $i \neq j$ のとき $p_i \nmid p_j^{e_j} - 1$ が成り立つ.

筆者と共同研究者の Ferrara 氏と Trombetti 氏が [7] にて, 様々な性質を検討し skew brace において同様の定理を証明できないか考察した. 本稿では, skew brace の冪零性に関する性質に焦点を当てて議論を行う.

$A = (A, \cdot, \circ)$ を skew brace とする. 群の交換子の類似として,

$$\forall a, b \in A : a * b = a^{-1} \cdot (a \circ b) \cdot b^{-1}$$

とおき, A のスター積と呼ぶ. また, A の部分集合 X, Y に対して, $X * Y$ を加法群 $(A, \cdot)$ における $\{x * y : x \in X, y \in Y\}$ の生成する部分群とおく. さらに, 群の中心の類似として,

$$\text{Soc}(A) = \{a \in A \mid \forall x \in A : a \cdot x = x \cdot a \text{ \& } a * x = 1\}$$

$$\text{Ann}(A) = \{a \in A \mid \forall x \in A : a \cdot x = x \cdot a \text{ \& } a * x = 1 \text{ \& } x * a = 1\}$$

とおき, それぞれ A の **socle** と A の **annihilator** と呼ぶ. どちらも A のイデアルとなることが知られている. つまり, どちらも $(A, \cdot)$ かつ $(A, \circ)$ の正規部分群であって,

$$\forall a \in A : a \cdot \text{Soc}(A) = a \circ \text{Soc}(A), a \cdot \text{Ann}(A) = a \circ \text{Ann}(A)$$

が成り立つ. ゆえに, skew brace の商 $A/\text{Soc}(A)$ および $A/\text{Ann}(A)$ が自然と定まる.

以下の定義において, (1),(2) は群の降中心列の類似であって, (3),(4) は群の昇中心列の類似である. それぞれの列を用いて, skew brace における冪零性が定義される.

定義 5.2. $A = (A, \cdot, \circ)$ を skew brace とする.

- (1) A の **left series** とは, 帰納的に定義される列

$$A^1 = A, \quad A^{m+1} = A * A^m \quad (m \geq 1)$$

である. $A^m = 1$ となる m が存在するとき, A は **left nilpotent** であると言う.

- (2) A の **right series** とは, 帰納的に定義される列

$$A^{(1)} = A, \quad A^{(m+1)} = A^{(m)} * A \quad (m \geq 1)$$

である. $A^{(m)} = 1$ となる m が存在するとき, A は **right nilpotent** であると言う.

(3) A の **socle series** とは, 帰納的に定義される列

$$\text{Soc}_0(A) = 1, \quad \text{Soc}_m(A)/\text{Soc}_{m-1}(A) = \text{Soc}(A/\text{Soc}_{m-1}(A)) \quad (m \geq 1)$$

である. $\text{Soc}_m(A) = A$ となる m が存在するとき, A は **socle nilpotent** である, または **finite multipermutation level** を持つと言う.

(4) A の **annihilator series** とは, 帰納的に定義される列

$$\text{Ann}_0(A) = 1, \quad \text{Ann}_m(A)/\text{Ann}_{m-1}(A) = \text{Ann}(A/\text{Ann}_{m-1}(A)) \quad (m \geq 1)$$

である. $\text{Ann}_m(A) = A$ となる m が存在するとき, A は **annihilator nilpotent** である, または **centrally nilpotent** であると言う.

注 5.3. $A = (A, \cdot, \cdot^{\text{op}})$ が almost trivial な skew brace であるとき, スター積 $*$ が群 $(A, \cdot)$ の交換子に帰着するため, 定義 5.2 にある A の冪零性はすべて $(A, \cdot)$ の冪零性と同等である. 一方で, $A = (A, \cdot, \cdot)$ が trivial な skew brace であるとき, スター積 $*$ が単位元のみ出力するため, A はつねに left nilpotent と right nilpotent であり, A の socle nilpotency と annihilator nilpotency は $(A, \cdot)$ の冪零性と同等である.

興味深いことに, 定義 5.2 にある冪零性について, left nilpotency を除いて対応する位数がすべて定理 5.1 (b) を満たす自然数となる. この現象の原因は, 以下の定理にある.

定理 5.4. $A = (A, \cdot, \circ)$ を skew brace とする. 加法群 $(A, \cdot)$ と乗法群 $(A, \circ)$ がともに冪零群であるとき, 以下が同値である.

- (1) A は right nilpotent である.
- (2) A は socle nilpotent である.
- (3) A は annihilator nilpotent である.

定理 5.4 はよく知られている事実であり, 証明については総説 [13, Section 5] を参照のこと. 以下の定理は, 筆者と Ferrara 氏と Trombetti 氏が [7] にて得られた結果の一つである. 詳細は省略するが, left nilpotency に対応する位数も [7] にて特定されている.

定理 5.5. 自然数 n の素因数分解を $n = p_1^{e_1} \cdots p_d^{e_d}$ としたとき, 以下が同値である.

- (a) 位数 n の skew brace はすべて right nilpotent である.
- (b) 位数 n の skew brace はすべて socle nilpotent である.
- (c) 位数 n の skew brace はすべて annihilator nilpotent である.
- (d) 任意の $1 \leq i \leq d$ に対して $e_i \leq 2$ であって, $i \neq j$ のとき $p_i \nmid p_j^{e_j} - 1$ が成り立つ.

証明. 位数 n の非冪零群が存在するとき, 注 5.3 より, 位数 n の right nilpotent でない skew brace も存在する. 同様に, 位数 n の socle nilpotent でも annihilator nilpotent でもない skew brace も存在する. よって, 位数 n の群がすべて冪零群であるような自然数 n に限定して考えてよい. すると, 定理 5.4 より (a) $\Leftrightarrow$ (d), (b) $\Leftrightarrow$ (d), (c) $\Leftrightarrow$ (d) は互いに同値となる. 証明は全く同じであるが, ここでは socle nilpotent に注目し (b) $\Leftrightarrow$ (d) の証明を解説する.

まず, (d) $\Rightarrow$ (b) について, $A = (A, \cdot, \circ)$ を位数 n の skew brace とする. このとき, 定理 5.1 より, $(A, \cdot)$ も $(A, \circ)$ もアーベル群である. $P_1, \dots, P_d$ を $(A, \cdot)$ の Sylow 部分群とすると, これらは $(A, \cdot)$ の特性部分群であるため $(A, \circ)$ の部分群ともなる. 実際,

$$\forall 1 \leq i \leq d, \forall a, a' \in P_i : a \circ a' = a \cdot \lambda_a(a') \in P_i \text{ \& } \bar{a} = \lambda_{\bar{a}}(a^{-1}) \in P_i$$

が成り立つ. $(A, \circ)$ もアーベル群であるため, A は素数冪位数の skew brace の直積

$$(A, \cdot, \circ) = (P_1, \cdot, \circ) \times \cdots \times (P_d, \cdot, \circ)$$

として表せる. 各 $1 \leq i \leq d$ について, 仮定 (d) より $|P_i|$ は素数もしくは素数の二乗である. しかし, 任意の素数 p に対して [1] より, 同型を除いて位数 p, p^2 の skew brace は,

$$(\mathbb{Z}/p\mathbb{Z}, +, +), \quad (\mathbb{Z}/p^2\mathbb{Z}, +, +), \quad (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, +, +)$$

の三つの trivial な skew brace と,

$$(\mathbb{Z}/p^2\mathbb{Z}, +, \circ), \quad a \circ a' = a + a' + paa'$$

$$(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, +, \circ), \quad \begin{bmatrix} a \\ b \end{bmatrix} \circ \begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} a+a'+bb' \\ b+b' \end{bmatrix}$$

の二つの trivial でない skew brace のみである. どれも socle nilpotent であるのは容易に確認できる. ゆえに, $P_1, \dots, P_d$ はすべて socle nilpotent であり, A も socle nilpotent である.

次に, (b) $\Rightarrow$ (d) について, (d) が成り立たないとき, 位数 n の socle nilpotent でない skew brace が存在すればよい. しかし, socle nilpotent でない skew brace と任意の skew brace の直積は明らかに socle nilpotent でないため, 素数 p, q に対して

$$(i) \ n = p^3, \quad (ii) \ n = pq \ (q \mid p-1), \quad (iii) \ n = p^2q \ (q \mid p^2-1)$$

において, 位数 n の socle nilpotent でない skew brace が存在すればよい. (ii),(iii) の場合は, 位数 n の非冪零群が存在するため除外できる. (i) の場合は, $p = 2$ のときは [1, Theorem 3.1] より存在し, $p \geq 3$ のときは命題 4.3 (2) を用いて以下のように例を構成できる. $\square$

例 5.6. 任意の奇素数 p に対して, 命題 4.3 (2) において,

$$B = (\mathbb{F}_p^2, +), \quad C = (\mathbb{F}_p, +)$$

とする. また, $\text{Aut}(B) = \text{GL}_2(\mathbb{F}_p)$ と同一視し, $P := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $E := \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ とおき,

$$\alpha : C \longrightarrow \text{Aut}(B); \quad c \mapsto \alpha_c := P^{-2c}$$

$$\beta : C \longrightarrow \text{Aut}(B); \quad c \mapsto \beta_c := EP^cE^{-1}$$

$$\lambda : C \longrightarrow \text{Aut}(B); \quad c \mapsto \lambda_c := P^c$$

とする. これらは明らかに (4.5) の一つ目の式を満たし, 二つ目の式も満たすのは,

$$\forall c \in C : \lambda_c \beta_c^{-1} = \frac{1}{2} \begin{bmatrix} -c^2 - c + 2 & c^2 + 3c \\ -c & c + 2 \end{bmatrix}$$

を使って簡単に示せる. このとき, 命題 4.3 (2) を用いて $\mathbb{F}_p^2 \times \mathbb{F}_p$ に対して, 演算 $\cdot$ と $\circ$ を定めて位数 p^3 の skew brace を構成できる. この skew brace について, socle が単位元 $(\vec{0}, 0)$ しか含まないことを証明できたら, socle nilpotent でないとも言える.

ここで, $((\alpha_c \lambda_c)(\vec{b}), c)$ を socle の元とすると, 任意の $\vec{x} \in \mathbb{F}_p^2$, $y \in \mathbb{F}_p$ に対して

$$((\alpha_c \lambda_c)(\vec{b}), c) \cdot ((\alpha_y \lambda_y)(\vec{x}), y) = (\alpha_c(\lambda_c(\vec{b}) + (\alpha_y \lambda_y)(\vec{x})), c + y)$$

$$((\alpha_c \lambda_c)(\vec{b}), c) \circ ((\alpha_y \lambda_y)(\vec{x}), y) = ((\alpha_{c+y} \lambda_{c+y})(\beta_y^{-1}(\vec{b}) + \vec{x}), c + y)$$

が一致することとなる. $y = 0$ を代入して比較すれば, $c \in \ker(\lambda)$ が得られる. λ は単射であるため $c = 0$ となる. また, $\vec{x} = \vec{0}$, $y = 1$ を代入して比較すれば, $(\alpha_1 \lambda_1 \beta_1^{-1})(\vec{b}) = \vec{b}$ であることも分かる. $\alpha_1 \lambda_1 \beta_1^{-1} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 & -1 \\ -1 & 1 \end{bmatrix}$ が正則行列であるため $\vec{b} = \vec{0}$ となる. 以上より, socle において単位元 $(\vec{0}, 0)$ しか存在しない.

したがって, 上記の五つ組 $(B, C, \alpha, \beta, \lambda)$ を用いて命題 4.3 (2) から構成できる skew brace は socle nilpotent ではない.

謝辞

本研究は JSPS 科研費 24K16891 の助成を受けたものである.

参考文献

- [1] D. Bachiller, *Classification of braces of order p^3* , J. Pure Appl. Algebra 219 (2015), no. 8, 3568–3603.

- [2] A. Ballester-Bolínches, R. Esteban-Romero, P. Jiménez-Seral, V. Pérez-Calabuig, *Constructing skew left braces whose additive group has trivial centre*, Canad. Math. Bull. 68 (2025), no. 3, 797–804.
- [3] W. Bosma, J. Cannon, and C. Playoust, *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.
- [4] N. P. Byott, *Solubility criteria for Hopf-Galois structures*, New York J. Math. 21 (2015), 883–903.
- [5] N. P. Byott, *On insoluble transitive subgroups in the holomorph of a finite soluble group*, J. Algebra 638 (2024), 1–31.
- [6] L. E. Dickson, *Definitions of a group and a field by independent postulates*, Trans. Amer. Math. Soc. 6 (1905), no. 2, 198–204. Erratum, *ibid.* no. 4, 547.
- [7] M. Ferrara, M. Trombetti, C. Tsang, *On cardinalities whose arithmetical properties determine the structure of solutions of the Yang-Baxter equation*, arXiv:2509.11001v1.
- [8] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. 86 (2017), no. 307, 2519–2534.
- [9] W. Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra 307 (2007), no. 1, 153–170.
- [10] A. Smoktunowicz, L. Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra 2 (2018), no. 1, 47–86.
- [11] C. Tsang, *Non-abelian simple groups which occur as the type of a Hopf-Galois structure on a solvable extension*, Bull. Lond. Math. Soc. 55 (2023), no. 5, 2324–2340.
- [12] C. Tsang, *A generalization of Ito’s theorem to skew braces*, J. Algebra 642 (2024), 367–399.
- [13] C. Tsang, *Analogues of the lower and upper central series in skew braces: a survey*, Commun. Math. 33 (2025), no. 3, Paper No. 11, 30 pp.
- [14] C. Tsang, *Factorizations of groups and skew braces*, to appear in “Group Theory”, Springer Proc. Math. Stat., 543, Springer (2026).
- [15] C. Tsang and C. Qin, *On the solvability of regular subgroups in the holomorph of a finite solvable group*, Internat. J. Algebra Comput. 30 (2020), no. 2, 253–265.

Email address: tsang.sin.yi@ocha.ac.jp

URL: <http://sites.google.com/site/cindysinyitsang/>