SKEW BRACE の加法群と乗法群の関係性について

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

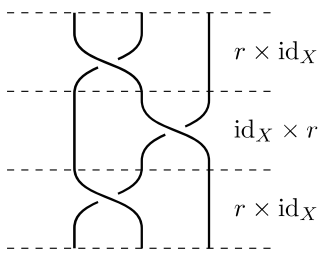
1　はじめに

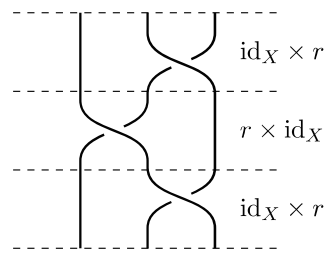
Skew brace は Yang-Baxter 方程式の非退化集合論的解を研究するために導入された代数的構造である．まずは，skew brace の生まれた経緯と背景について簡単に述べる．

Yang-Baxter 方程式は理論物理学や結び目理論といった諸分野に応用があり，多くの人々の興味を惹き盛んに研究されてきた．その中で，1992年に Drinfeld [10] が集合論的解というものを提唱した．Yang-Baxter 方程式の集合論的解とは，集合 X および

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

を満たす全単射 $r : X \times X \longrightarrow X \times X$ のなすペア (X, r) のことである．r は braiding とも呼ばれ，隣接する二つのストランドを交差する操作として解釈できる．すると，上式はくみひも群のくみひも関係式と同様に，以下のように図示できる．





また，r の値 $r(x, y)$ の第一成分と第二成分をそれぞれ y と x の関数として見なし，

$$r(x, y) = (\sigma_x(y), \tau_y(x))$$

と書くことにする．(X, r) が非退化であるとは，すべての $x \in X$ に対して σ_x も τ_x も全単射であるときにいう．(X, r) が involutive であるとは，$r^2 = \mathrm{id}_{X \times X}$ が成り立つときにいう．

Etingof-Schedler-Soloviev [11] の影響もあり，involutive な非退化解の研究が特に注目を集めていた．その一環として，2007 年に Rump [18] が brace を導入し，brace は involutive な非退化集合論的解と対応することを証明した．その後，2017 年に Guarnieri-Vendramin [12]

が involutive でない解も網羅できるよう， brace の定義を skew brace に一般化し，skew brace はすべての非退化集合論的解と対応すると示すことに成功した．したがって，skew brace の構造を調べることで，Yang-Baxter 方程式の非退化集合論的解について情報を得ることができる．例えば，非退化集合論的解 (X, r) が multipermutation か否かは対応する skew brace の冪零性と関連することが知られている [14].

Skew brace は群の holomorph の正則部分群とも対応することが知られており [12]，後者は有限ガロア拡大上のホップ・ガロア構造とも関連する [8]．したがって，skew brace の応用範囲は Yang-Baxter 方程式に留まらず置換群やホップ・ガロア理論にまで及んでいる．例えば，ホップ・ガロア構造におけるホップ・ガロア対応が全射か否かは対応する skew brace の左イデアルと関連することが知られている [19]．近年では，Yang-Baxter 方程式の研究者の他に，群論や代数的整数論の研究者も skew brace に対して興味を持つようになり，skew brace の研究が急速に進んでいる．

本論文では，第 2 節で brace および skew brace の定義や具体例を述べたあとに，第 3 節で skew brace と holomorph の正則部分群の対応について説明する．一つの skew brace において加法群と乗法群と呼ばれる二つの群が関わっており，その関係性を調べるのは自然なことである．この課題の研究において，群の分解を用いる場面が多々ある．第 4 節では，群の分解がどのように応用されてきたかを中心に，skew brace の加法群と乗法群の関係性に関する先行研究および著者の研究成果を紹介する．

2 Brace と Skew brace

まずは，brace を定義する．

定義 2.1. Brace とは，二つの二項演算 $+$ と $\circ$ を備えた集合 $A = (A, +, \circ)$ であって，

(1) $(A, +)$ はアーベル群である．

(2) $(A, \circ)$ は群である．

(3) 任意の $a, b, c \in A$ に対して，$a \circ (b + c) = (a \circ b) - a + (a \circ c)$ が成り立つ．
この関係式は (左) brace relation とも呼ばれる．

を満たすものである．$(A, +)$ を A の加法群，$(A, \circ)$ を A の乗法群と呼ぶ．$(A, +)$ と $(A, \circ)$ の単位元が一致するのは容易に確かめられ，それを 0 と表記する．

Brace は二つの二項演算を備えた代数的構造であり，その定義は環を連想させるところがある．例えば，brace relation は環における分配法則と類似する．実際，brace は radical 環の一般化として導入されたものである．

任意の環 $R=(R,+,\cdot)$ において，adjoint operation と呼ばれる二項演算

$$a\circ b=a+b+a\cdot b$$

が定められる．$(R,\circ)$ は monoid であり，R の零元 0_R が $(R,\circ)$ の単位元となるのは容易に確かめられる．$(R,\circ)$ が実際に群をなすとき，R が radical であるという．ちなみに，自明でない単位的環は radical になることはない．R の単位元の加法逆元 -1_R が $\circ$ について逆元を持たないからである．

例 2.2. 任意の radical 環 $R=(R,+,\cdot)$ に対して，$(R,+,\circ)$ は brace である．ただし，$\circ$ は R の adjoint operation である．$(R,+)$ がアーベル群であるのは環の定義から，$(R,\circ)$ が群であるのは radical の定義から従う．また，任意の $a,b,c\in A$ に対して，

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

が成り立つため，brace relation も満たされる．

実は，radical 環は例 2.2 によって両側 brace と一対一対応する [18]．Brace $A=(A,+,\circ)$ が両側であるとは，任意の $a,b,c\in A$ に対して，左 brace relation に加えて右 brace relation

$$(b+c)\circ a=(b\circ a)-a+(c\circ a)$$

も成り立つときにいう．このことから，brace は radical 環の一般化として見なせる．

次は，skew brace を定義する．Skew brace は brace の一般化であり，加法群がアーベル群である条件を任意の群に緩めたものである．

定義 2.3. Skew brace とは，二つの二項演算 $\cdot$ と $\circ$ を備えた集合 $A=(A,\cdot,\circ)$ であって，

(1) $(A,\cdot)$ は群である．

(2) $(A,\circ)$ は群である．

(3) 任意の $a,b,c\in A$ に対して，$a\circ(b\cdot c)=(a\circ b)\cdot a^{-1}\cdot(a\circ c)$ が成り立つ．

この関係式は (左) brace relation または (左) skew brace relation とも呼ばれる．

を満たすものである．Brace のときと同様に，$(A,\cdot)$ を A の加法群，$(A,\circ)$ を A の乗法群と呼ぶ．$(A,\cdot)$ と $(A,\circ)$ の単位元が一致するのは容易に確かめられ，それを 1 と表記する．

次の例から解るように，skew brace は群の一般化として考えられる．

例 2.4. 任意の群 $A = (A, \cdot)$ に対して，$(A, \cdot, \cdot)$ も $(A, \cdot, \cdot^{\mathrm{op}})$ も skew brace である．ただし，$\cdot^{\mathrm{op}}$ は $\cdot$ の opposite operation，すなわち，$a \cdot^{\mathrm{op}} b = b \cdot a$ を満たす二項演算である．$(A, \cdot)$ も $(A, \cdot^{\mathrm{op}})$ も群であるのは明らかである．Brace relation について，$(A, \cdot, \cdot)$ においては

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

と書き直せて，$(A, \cdot, \cdot^{\mathrm{op}})$ においては

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

と書き直せる．どちらも群 $(A, \cdot)$ の結合法則より従う．

例 2.4 からなる skew brace は，一つの二項演算だけで記述できるため，本質的には群とさほど変わらない．このことから，任意の skew brace $A = (A, \cdot, \circ)$ に対して，備えている二つの二項演算 $\circ$ と $\cdot$ が等しいときは A が trivial であるといい，互いに opposite operation となっているときは A が almost trivial であるという．

最後に，skew brace と Yang-Baxter 方程式の非退化集合論的解との関連性を示す定理を紹介する [12]．$A = (A, \cdot, \circ)$ を skew brace とする．このとき，各 $a \in A$ に対して，

$$\gamma_a : A \longrightarrow A;\ \ \gamma_a(x) = a^{-1} \cdot (a \circ x) \tag{2.1}$$

は $(A, \cdot)$ の自己同型となるのは容易に確かめられる．また，

$$\gamma : (A, \circ) \longrightarrow \mathrm{Aut}(A, \cdot);\ \ a \mapsto \gamma_a \tag{2.2}$$

が群の準同型となるのも知られている．この写像は λ と表記されることが多いが，次の節では左正則表現を λ と表すため，本論文では [6] に従って写像 (2.2) を γ と書くことにする．

定理 2.5. 任意の skew brace $A = (A, \cdot, \circ)$ に対して，

$$r_A : A \times A \longrightarrow A \times A;\ \ r_A(a, b) = (\gamma_a(b), \gamma^{-1}_{\gamma_a(b)}((a \circ b)^{-1} \cdot a \cdot (a \circ b)))$$

は Yang-Baxter 方程式の非退化集合論的解となる．また，r_A が involutive であるのは，A が brace であるとき，かつそのときに限る．

逆に，Yang-Baxter 方程式の非退化集合論的解 (X, r) が与えられたとき，ある普遍性を満たす skew brace を構成することができる．詳細は [12] を参照のこと．

3 Holomorph の正則部分群との対応

本節では，$A = (A, \cdot)$ を群とする．$(A, \cdot, \circ)$ が skew brace となるような二項演算 $\circ$ が A の holomorph の正則部分群と一対一対応することについて簡単に説明する．

まず，A の対称群の部分群 R が正則であるとは，R の A への自然な作用が正則，つまり，推移的かつ自由であるときにいう．例えば，ρ と λ をそれぞれ A の右正則表現と左正則表現とすると，すなわち，各 $a \in A$ に対して

$$\begin{cases} \rho(a) : A \longrightarrow A; \quad \rho(a)(x) = xa^{-1} \\ \lambda(a) : A \longrightarrow A; \quad \lambda(a)(x) = ax \end{cases}$$

とすると，$\rho(A)$ と $\lambda(A)$ は正則部分群となる．A の holomorph は，A の対称群における $\rho(A)$ または $\lambda(A)$ と A の自己同型群 $\mathrm{Aut}(A)$ の内部半直積

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

として定義される．$\mathrm{Hol}(A)$ において，任意の $a, b \in A$ と $\varphi, \psi \in \mathrm{Aut}(A)$ に対して，

$$(\rho(a)\varphi)(\rho(b)\psi) = \rho(a\varphi(b))\varphi\psi, \ \ (\rho(a)\varphi)^{-1} = \rho(\varphi^{-1}(a^{-1}))\varphi^{-1} \tag{3.1}$$

が成り立つことに注意しておく．また，$\mathrm{Aut}(A)$ は A の単位元を動かさないため，$\mathrm{Hol}(A)$ に含まれる任意の正則部分群は，明らかにある写像 $\gamma : A \longrightarrow \mathrm{Aut}(A)$ を用いて

$$R_\gamma = \{\rho(a)\gamma_a : a \in A\}$$

と表せる．ここでは $\gamma(a)$ を γ_a と書く．しかし，一般の写像 $\gamma : A \longrightarrow \mathrm{Aut}(A)$ に対して，R_γ が $\mathrm{Hol}(A)$ の部分群となるためには γ は一定の条件を満たさなければならない．

命題 3.1. 任意の写像 $\gamma : A \longrightarrow \mathrm{Aut}(A)$ に対して，R_γ が $\mathrm{Hol}(A)$ の部分群となるのは，

$$\forall a, b \in A : \ \gamma_{a\gamma_a(b)} = \gamma_a\gamma_b \tag{3.2}$$

が成り立つとき，かつそのときに限る．このとき R_γ が正則部分群となるのは自明である．

証明. 式 (3.1) を鑑みて，R_γ が $\mathrm{Hol}(A)$ の部分群となるのは，

- (単位元を含む) $\gamma_1 = \mathrm{id}_A$
- (演算に関して閉じている) 任意の $a, b \in A$ に対して $\gamma_{a\gamma_a(b)} = \gamma_a\gamma_b$
- (逆元に関して閉じている) 任意の $a \in A$ に対して $\gamma_{\gamma_a^{-1}(a^{-1})} = \gamma_a^{-1}$

がすべて成り立つとき，かつそのときに限る．式 (3.2) に $a = b = 1$ と $b = \gamma_a^{-1}(a^{-1})$ をそれぞれ代入すれば $\gamma_1 = \mathrm{id}_A$ と $\gamma_{\gamma_a^{-1}(a^{-1})} = \gamma_a^{-1}$ が得られるため，この命題が従う． □

次の二つの定理は [12] によるものである．

定理 3.2. $(A, \cdot, \circ)$ が skew brace となるような二項演算 $\circ$ は $\mathrm{Hol}(A)$ の正則部分群 R_γ と一対一対応する．具体的に，この対応は関係式

$$\forall a, b \in A : a \circ b = a\gamma_a(b) \tag{3.3}$$

によって与えられる．また，このとき $(A, \circ)$ と R_γ は同型である．

証明. $(A, \cdot, \circ)$ が skew brace となるような二項演算 $\circ$ が与えられたとき，(3.3) によって定められる写像 γ_a は (2.1) に一致する．写像 (2.2) が群の準同型であるため，(3.2) が成り立って R_γ は $\mathrm{Hol}(A)$ の正則部分群である．また，$(A, \circ)$ は $a \mapsto \rho(a)\gamma_a$ により R_γ と同型である．逆に，$\mathrm{Hol}(A)$ の正則部分群 R_γ が与えられたとき，(3.3) によって定められる二項演算 $\circ$ について，$(A, \cdot, \circ)$ が skew brace となるのは簡単に確かめられるため，詳細を省略する． □

定理 3.2 の対応において，skew brace の同型類は正則部分群の共役類と対応する．ここで，skew brace の構造は備えている二つの二項演算によってすべて決まるため，skew brace の準同型は両方の演算を保つ写像として自然と定義される．

定理 3.3. $(A, \cdot, \circ), (A, \cdot, \circ')$ が skew brace となるような二項演算 $\circ, \circ'$ について，それぞれに対応する $\mathrm{Hol}(A)$ の正則部分群を $R_\gamma, R_{\gamma'}$ とすると，$(A, \cdot, \circ)$ と $(A, \cdot, \circ')$ が skew brace として同型であることは，R_γ と $R_{\gamma'}$ が $\mathrm{Aut}(A)$ の元によって共役であることと同値である．

証明. $(A, \cdot, \circ)$ と $(A, \cdot, \circ')$ の間に存在する skew brace の同型は $A = (A, \cdot)$ の自己同型でなければならないため，$\mathrm{Aut}(A)$ の元のみ考えればよい．また，任意の $\varphi \in \mathrm{Aut}(A)$ に対して，

$$\varphi R_\gamma \varphi^{-1} = \{\rho(\varphi(a))\varphi\gamma_a\varphi^{-1} : a \in A\}$$

である．このことから，$\varphi R_\gamma \varphi^{-1} = R_{\gamma'}$ となるのは，すべての $a \in A$ について $\gamma'_{\varphi(a)} = \varphi\gamma_a\varphi^{-1}$ が成り立つとき，かつそのときに限ることがわかる．しかし，任意の $a, b \in A$ に対して，

$$(\gamma'_{\varphi(a)}\varphi)(b) = \varphi(a)^{-1} \cdot (\varphi(a) \circ' \varphi(b))$$
$$(\varphi\gamma_a)(b) = \varphi(a)^{-1} \cdot \varphi(a \circ b)$$

である．よって，$\varphi R_\gamma \varphi^{-1} = R_{\gamma'}$ が成り立つのは，φ が乗法群の演算も保つ，つまり $(A, \cdot, \circ)$ から $(A, \cdot, \circ')$ への skew brace の同型であることと同値であり，定理が従う． □

注 3.4. $\mathrm{Hol}(A)$ の任意の正則部分群 R_γ について，$\mathrm{Aut}(A)$ による共役類は $\mathrm{Hol}(A)$ による共役類と一致する [1]．なぜならば，$x \in A$ と $\varphi \in \mathrm{Aut}(A)$ に対して，$y = \varphi^{-1}(x^{-1})$ とすると，

$$\rho(x)\varphi\rho(y)\gamma_y = \rho(x\varphi(y))\varphi\gamma_y = \varphi\gamma_y$$

が成り立つ．$\widetilde{y} := \rho(y)\gamma_y \in R_\gamma$ のため，$\mathrm{Hol}(A)$ の元 $\widetilde{x} := \rho(x)\varphi$ の R_γ に対する共役作用は，

$$\widetilde{x}R_\gamma\widetilde{x}^{-1} = \widetilde{x}(\widetilde{y}R_\gamma\widetilde{y}^{-1})\widetilde{x}^{-1} = (\widetilde{x}\widetilde{y})R_\gamma(\widetilde{x}\widetilde{y})^{-1}$$

のように $\mathrm{Aut}(A)$ の元 $\widetilde{x}\widetilde{y} = \varphi\gamma_y$ の共役作用として実現できる．

例 2.4 で述べたように，$(A, \cdot, \cdot)$ も $(A, \cdot, \cdot^{\mathrm{op}})$ も skew brace である．定理 3.2 の (3.3) による対応において，前者 (trivial skew brace) は $\rho(A)$，後者 (almost trivial skew brace) は $\lambda(A)$ と対応する．また，$\rho(A)$ と $\lambda(A)$ が等しいのは A がアーベル群であるとき，かつそのときに限ることに注意しよう．$\rho(A)$ も $\lambda(A)$ も $\mathrm{Aut}(A)$ の共役作用で不変であるため，定理 3.3 によると，$(A, \cdot, \cdot)$ と $(A, \cdot, \cdot^{\mathrm{op}})$ が skew brace として同型であることは，A がアーベル群であることと同値となる．この事実は，定理 3.3 を用いらなくても容易に示せる．

4　加法群と乗法群の関係性

本節では，群の分解を用いた研究手法に触れつつ，skew brace の加法群と乗法群の同型類を比較した先行研究および著者の研究成果を紹介する．定理 3.2 の対応より，本節のタイトルに関する研究は，群とその holomorph の正則部分群の同型類を調べることに帰着する．

以降，$A = (A, \cdot)$ を群とする．その holomorph は，

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

のように半直積として二通りに表せる．それぞれの分解による $\mathrm{Aut}(A)$ への射影を

$$\begin{cases} \pi_\rho : \mathrm{Hol}(A) \longrightarrow \mathrm{Aut}(A); \quad \pi_\rho(\rho(a)\varphi) = \varphi \ \ (a \in A,\ \varphi \in \mathrm{Aut}(A)) \\ \pi_\lambda : \mathrm{Hol}(A) \longrightarrow \mathrm{Aut}(A); \quad \pi_\lambda(\lambda(a)\varphi) = \varphi \ \ (a \in A,\ \varphi \in \mathrm{Aut}(A)) \end{cases}$$

とおく．以下の命題は [21] によるものであり容易に示せる．

命題 4.1. $\mathrm{Hol}(A)$ の任意の正則部分群 R に対して，$\rho(A) \rtimes \pi_\rho(R) = R \cdot \pi_\rho(R)$ が成り立つ．

次の定理は最初に [4] 或いは [17] によって示されたが，ここでは [21] に従い，命題 4.1 を用いた証明で示す．

定理 4.2. $(A,\cdot,\circ)$ が skew brace であるとする．乗法群 $(A,\circ)$ がアーベル群であれば，加法群 $(A,\cdot)$ はメタアーベル群である．

証明. 定理 3.2 と命題 4.1 より，$\mathrm{Hol}(A)$ において $(A,\circ)$ と同型な正則部分群 R が存在し，

$$\rho(A) \rtimes \pi_\rho(R) = R \cdot \pi_\rho(R) \tag{4.1}$$

が成り立つ．$(A,\circ)$ がアーベル群であるとすると，アーベル群の商群もまたアーベル群であるため，$\pi_\rho(R)$ もアーベル群となる．また，Itô の定理 [13] によると，二つのアーベル部分群によって分解される群はメタアーベル群である．したがって，群 (4.1) はメタアーベル群であり，メタアーベル群の部分群もまたメタアーベル群であるため，$\rho(A) \simeq A$ もメタアーベル群となる．以上より，$A = (A,\cdot)$ がメタアーベル群であることが示された． □

群の分解の理論において，Itô の定理の他に Douglas の定理と Kegel-Wielandt の定理もよく知られている．Douglas の定理 [9] によると，二つの巡回部分群によって分解される有限群は超可解群である．また，Kegel-Wielandt の定理 [15] によると，二つの冪零部分群によって分解される有限群は可解群である．次の定理は [21] による結果である．

定理 4.3. $(A,\cdot,\circ)$ が有限 skew brace であるとする．

(a) 乗法群 $(A,\circ)$ が巡回群であれば，加法群 $(A,\cdot)$ は超可解群である．

(b) 乗法群 $(A,\circ)$ が冪零群であれば，加法群 $(A,\cdot)$ は可解群である．

証明. Itô の定理の代わりに，Douglas および Kegel-Wielandt の定理を用いれば，定理 4.2 と全く同じ議論で証明できる． □

注 4.4. $(A,\cdot,\circ)$ が有限 skew brace であり，乗法群 $(A,\circ)$ が巡回群であるとき，加法群 $(A,\cdot)$ となり得る群の同型類は著者によってすべて特定されている．詳細は [24] を参照のこと．

定理 4.2 と定理 4.3 では，skew brace の乗法群が巡回群，アーベル群，そして冪零群である場合を考えた．次に，skew brace の乗法群が非可解群である場合を考えよう．これに関して，以下のことが予想されている．

予想 4.5. $(A,\cdot,\circ)$ が有限 skew brace であるとする．乗法群 $(A,\circ)$ が非可解群であれば，加法群 $(A,\cdot)$ も非可解群である．

予想 4.5 を完全に証明するのは非常に困難であると思われ，有限単純群の分類定理が必要不可欠であろう．進展 [5,21] はあるものの，いまだに未解決問題である．乗法群が特定の非可解群である場合では成り立つことが知られており，関連する結果を少し紹介しよう．

まず，構造が最も簡単な非可解群は非アーベル単純群である．次の定理は [3] によるものであり，のちに著者によって任意の quasisimple 群に一般化された [23]．ただし，quasisimple 群とは，完全群であって，中心による商群が非アーベル単純群となる群である．

定理 4.6. $(A,\cdot,\circ)$ が有限 skew brace であるとする．乗法群 $(A,\circ)$ が非アーベル単純群であれば，$(A,\cdot,\circ)$ は trivial または almost trivial な skew brace である．したがって，加法群 $(A,\cdot)$ は $(A,\circ)$ と同型であり，特に非可解群である．

非アーベル単純群を除き，5 次以上の対称群が最も馴染みのある非可解群の一つであろう．Skew brace の乗法群が対称群であるとき，加法群になり得る群の同型類は既に著者によってすべて特定されている [20]．詳しくは述べないが，この結果はある程度，socle の指数が素数であるような任意の almost simple に拡張することができる [22]．ただし，almost simple 群とは，ある非アーベル単純群の内部自己同型群と自己同型群の間に埋め込める群である．

定理 4.7. $(A,\cdot,\circ)$ が有限 skew brace であり，乗法群 $(A,\circ)$ が n 次対称群 S_n であるとする．ただし，n は 5 以上の自然数とする．

(a) $n\neq 6$ のとき，加法群 $(A,\cdot)$ は S_n または $A_n\times C_2$ と同型である．

(b) $n=6$ のとき，加法群 $(A,\cdot)$ は S_6, $A_6\times C_2$ または M_{10} と同型である．

したがって，どちらの場合においても加法群 $(A,\cdot)$ は非可解群である．

注 4.8. 定理 4.7 の証明において，最初は加法群 $(A,\cdot)$ の可能性を $A_n\times C_2$ または A_n を socle に持つ almost simple 群に絞った．$n\neq 6$ のとき，$\mathrm{Out}(S_n)$ は自明であるため，後者になり得る群は S_n のみである．一方で $n=6$ のとき，$\mathrm{Out}(S_6)\simeq C_2\times C_2$ であり，後者になり得る群は S_6 と M_{10} の他には $\mathrm{PGL}_2(9)$ もある．しかし，[7] の最後のところで述べられたように，乗法群 $(A,\circ)$ が S_6 であるとき，加法群 $(A,\cdot)$ が $\mathrm{PGL}_2(9)$ になることはない．

予想 4.5 の真偽がまだ明らかにされていないのに対して，その逆は成り立たないことが知られている．つまり，加法群 $(A,\cdot)$ は非可解群であって乗法群 $(A,\circ)$ は可解群となるような有限 skew brace $(A,\cdot,\circ)$ が存在する．具体例は群の分解を用いて作ることができる．正確に言うと，有限非可解群が存在して，共通部分が自明となるような二つの可解部分群によって分解されるとき，以下の命題を用いれば作れる．

命題 4.9. $A=BC$ が部分群 B, C によって分解され，かつ $B\cap C=1$ が成り立つとする．任意の $b_1,b_2\in B$, $c_1,c_2\in C$ に対して $(b_1c_1)\circ(b_2c_2)=b_1\cdot(b_2c_2)\cdot c_1$ とおくと，$(A,\cdot,\circ)$ が skew brace となり，その乗法群 $(A,\circ)$ は $bc^{-1}\leftarrow\!\shortmid(b,c)$ によって $B\times C$ と同型である．特に，B, C が共に可解群であるとき，乗法群 $(A,\circ)$ も可解群である．

証明. 仮定より A の元は $b \in B$, $c \in C$ を用いて bc と一意に書けて，$\gamma_{bc} = \mathrm{conj}(c^{-1})$ とおく．ただし，A の任意の元 a に対して，$\mathrm{conj}(a) = (x \mapsto axa^{-1})$ は a による内部自己同型を表す．任意の $b_1, b_2 \in B$, $c_1, c_2 \in C$ に対して，

$$\begin{aligned}\gamma_{b_1c_1}\gamma_{b_1c_1}(b_2c_2) &= \gamma_{b_1c_1\cdot c_1^{-1}b_2c_2c_1} \\ &= \mathrm{conj}((c_2c_1)^{-1}) \\ &= \mathrm{conj}(c_1^{-1})\mathrm{conj}(c_2^{-1}) \\ &= \gamma_{b_1c_1}\gamma_{b_2c_2}\end{aligned}$$

が成り立つため，条件 (3.2) は満たされる．したがって，命題 3.1 と定理 3.2 より，

$$(b_1c_1)\circ(b_2c_2) = b_1c_1\gamma_{b_1c_1}(b_2c_2) = b_1\cdot(b_2c_2)\cdot c_1$$

とおくと，$(A, \cdot, \circ)$ は skew brace となる．$(A, \circ) \simeq B \times C$ は容易に確かめられる． □

例 4.10. $A_5 = A_4\langle(1\,2\,3\,4\,5)\rangle$ および $A_4 \cap \langle(1\,2\,3\,4\,5)\rangle = 1$ が成り立つため，命題 4.9 によると，加法群 $(A, \cdot)$ は非アーベル単純群の A_5 であって乗法群 $(A, \circ)$ は可解群 $A_4 \times C_5$ と同型となるような skew brace $(A, \cdot, \circ)$ が存在する．

群の分解の理論をさら応用し，乗法群 $(A, \circ)$ が可解群となるような有限 skew brace $(A, \cdot, \circ)$ の加法群 $(A, \cdot)$ になり得る非アーベル単純群も特定できる．要となるのは次の二つの命題である [25].

命題 4.11. $\mathrm{Hol}(A)$ の任意の正則部分群 R に対して，$\pi_\rho(R)\pi_\lambda(R)$ は部分群であり，

$$\mathrm{Inn}(A) \le \pi_\rho(R)\pi_\lambda(R) \le \mathrm{Aut}(A),\ \ \pi_\rho(R)\mathrm{Inn}(A) = \pi_\lambda(R)\mathrm{Inn}(A)$$

が成り立つ．注: R が可解群であるとき，$\pi_\rho(R)$ も $\pi_\lambda(R)$ も可解群となる．

命題 4.12. A の中心が自明であるとする．$\mathrm{Aut}(A)$ の任意の部分群 P, Q に対して，PQ は部分群であり，P は $P \cap \mathrm{Inn}(A)$ 上に分裂し，かつ

$$\mathrm{Inn}(A) \le PQ \le \mathrm{Aut}(A),\ \ P\mathrm{Inn}(A) = Q\mathrm{Inn}(A),\ \ P \cap Q = 1$$

が成り立つとき，$\mathrm{Hol}(A)$ において $P \cap \mathrm{Inn}(A)$ と Q の半直積と同型となるような正則部分群 R が存在する．注: P も Q も可解群であるとき，R も可解群となる．

以下の定理は [25] による結果である．その証明の概略を簡単に説明する．

定理 4.13. A が有限非アーベル単純群であるとする．$(A,\cdot,\circ)$ が skew brace であって乗法群 $(A,\circ)$ が可解群となるような二項演算 $\circ$ が存在するのは，$A=(A,\cdot)$ が以下の非アーベル単純群のどれかと同型であるとき，かつそのときに限る．

(1) $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSL}_3(8)$, $\mathrm{PSU}_3(8)$, $\mathrm{PSU}_4(2)$, M_{11};

(2) $\mathrm{PSL}_2(q)$, $q\neq 2,3$ は素数冪である．

証明の概略. 定理 3.2 より，$(A,\cdot,\circ)$ が skew brace であって乗法群 $(A,\circ)$ が可解群となるような二項演算 $\circ$ が存在することは，$\mathrm{Hol}(A)$ において可解な正則部分群が存在することと同値である．後者の条件で考える．

まず，$\mathrm{Hol}(A)$ において可解な正則部分群 R が存在するとする．命題 4.11 において，$\pi_\rho(R)$ も $\pi_\lambda(R)$ も可解群となり，$\pi_\rho(R)\pi_\lambda(R)$ は $\mathrm{Inn}(A)\simeq A$ を socle に持つ有限 almost simple 群となる．二つの可解部分群によって分解できる有限 almost simple 群は既に知られており [16]，その socle は (1), (2) の非アーベル単純群のどれかと同型でなければならない．

逆に，A が (1), (2) の非アーベル単純群のどれかと同型であるとする．$\mathrm{Aut}(A)$ において，命題 4.12 の条件を満たす可解部分群 P, Q が存在すればよい．(2) の場合は，Singer cycle と一次元の部分空間の安定化群にすればよく，このときの積が $\mathrm{PGL}_2(q)$ となる．詳細は [25] を参照のこと．(1) の場合は，Magma [2] を用いて確かめればよく，$A\simeq\mathrm{PSU}_3(8)$ のときを除いて上述のような P, Q が実際に存在する．$A\simeq\mathrm{PSU}_3(8)$ の場合は命題 4.12 では不十分であるため，ここでは詳しく述べないことにする． □

実は，定理 4.13 と同様に，命題 4.11 と命題 4.12 を用いて乗法群 $(A,\circ)$ が可解群となるような有限 skew brace $(A,\cdot,\circ)$ の加法群 $(A,\cdot)$ になり得る almost simple 群も特定できる．詳細はプレプリント arXiv:2312.15745 を参照のこと．

参考文献

[1] V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav, *Computing skew left braces of small orders*, Internat. J. Algebra Comput. 30 (2020), no. 4, 839–851.

[2] 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.

[3] N. P. Byott, *Hopf-Galois structures on field extensions with simple Galois groups*, Bull. London Math. Soc. 36 (2004), no. 1, 23–29.

[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] A. Caranti, *Bi-skew braces and regular subgroups of the holomorph*, J. Algebra 562 (2020), 647–665.

[7] S. Carnahan and L. Childs, *Counting Hopf Galois structures on non-abelian Galois field extensions*, J. Algebra 218 (1999), no. 1, 81–92.

[8] L. N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, 80. American Mathematical Society, Providence, RI, 2000.

[9] J. Douglas, *On the supersolvability of bicyclic groups*, Proc. Nat. Acad. Sci. U.S.A 47 (1961), 1493–1495.

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

[11] P. Etingof, T. Schedler, and A. Soloviev. *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. 100 (1999), no. 2, 169–209.

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

[13] N. Itô, *Über das Produkt von zwei abelschen Gruppen*, Math. Z. 62 (1955), 400–401.

[14] E. Jespers, A. Van Antwerpen, and L. Vendramin, *Nilpotency of skew braces and multipermutation solutions of the Yang-Baxter equation*, Commun. Contemp. Math. 25 (2023), no. 9, Paper No. 2250064, 20 pp.

[15] O. H. Kegel, *Produkte nilpotenter Gruppen*, Arch. Math. (Basel) 12 (1961), 90–93.

[16] C. H. Li and B. Xia, *Factorizations of almost simple groups with a solvable factor, and Cayley graphs of solvable groups*, Mem. Amer. Math. Soc. 279 (2022), no. 1375, v+99 pp.

[17] T. Nasybullov, *Connections between properties of the additive and the multiplicative groups of a two-sided skew brace*, J. Algebra 540 (2019), 156–167.

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

[19] L. Stefanello and S. Trappeniers, *On the connection between Hopf-Galois structures and skew braces*, Bull. Lond. Math. Soc. 55 (2023), no. 4, 1726–1748.

[20] C. Tsang, *Hopf-Galois structures on a Galois S_n-extension*, J. Algebra 531 (2019), 349–361.

[21] 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.

[22] C. Tsang, *Hopf-Galois structures on finite extensions with almost simple Galois group*, J. Number Theory 214 (2020), 286–311.

[23] C. Tsang, *Hopf-Galois structures on finite extensions with quasisimple Galois group*, Bull. Lond. Math. Soc. 53 (2021), no. 1, 148–160.

[24] C. Tsang, *Hopf-Galois structures on cyclic extensions and skew braces with cyclic multiplicative group*, Proc. Amer. Math. Soc. Ser. B 9 (2022), 377–392.

[25] 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.

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

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