Finite skew braces with solvable additive group

Ilya Gorshkov, Timur Nasybullov

Abstract

A. Smoktunowicz and L. Vendramin conjectured that if $A$ is a finite skew brace with solvable additive group, then the multiplicative group of $A$ is solvable. In this short note we make a step towards positive solution of this conjecture proving that if $A$ is a minimal finite skew brace with solvable additive group and non-solvable multiplicative group, then the multiplicative group of $A$ is not simple. On the way to obtaining this result, we prove that the conjecture of A. Smoktunowicz and L. Vendramin is correct in the case when the order of $A$ is not divisible by 3.

Keywords: skew brace, solvable group, simple group.

Mathematics Subject Classification: 20F16, 20D05, 20N99, 16T25.

1 Introduction

A skew brace $A = (A, \oplus, \odot)$ is an algebraic system with two binary algebraic operations $\oplus, \odot$ such that $A_\oplus = (A, \oplus), A_\odot = (A, \odot)$ are groups and the equality

$$a \odot (b \oplus c) = (a \odot b) \oplus a \odot (a \odot c)$$

holds for all $a, b, c \in A$, where $\ominus a$ denotes the inverse to $a$ element with respect to the operation $\oplus$ (we denote by $a^{-1}$ the inverse to $a$ element with respect to $\odot$). The group $A_\oplus$ is called the additive group of a skew brace $A$, and the group $A_\odot$ is called the multiplicative group of a skew brace $A$. If $A_\oplus$ is abelian, then $A$ is called a classical brace.

Classical braces were introduced by Rump in [17] in order to study non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation. Skew braces were introduced by Guarnieri and Vendramin in [9] in order to study non-degenerate set-theoretic solutions of the Yang-Baxter equation which are not necessarily involutive. Skew braces have connections with other algebraic structures such as groups with exact factorizations, Zappa-Szép products, triply factorized groups and Hopf-Galois extensions [18]. Some algebraic aspects of skew braces are studied in [6,7,10,14,16,18]. Thanks to its relations with the Yang-Baxter equation skew braces can be applied for constructing representations of virtual braid groups and invariants of virtual links [2,4]. A big list of problems concerning skew braces is collected in [21].

Equality (1) makes the additive group $A_\oplus$ and the multiplicative group $A_\odot$ of a skew brace $A$ strongly connected with each other. For example, the following problems formulated in the Kourovka notebook [15 Problem 19.90] tell about some of such connections.

1. Does there exist a (finite) skew brace with nilpotent multiplicative group but non-solvable additive group?

2. Does there exist a (finite) skew brace with solvable additive group but non-solvable multiplicative group?

The first problem from the list above was studied, for example, in [5,16,18,20]. The most general result about this question is obtained in [20], where it is proved that the answer to this question is
negative in the case of finite skew braces. The second problem from the list above was studied, for example, in \[16,18\]. It is known \[16,\ Example 3.2\] that there exists an infinite skew brace which gives a positive answer to this question. So, in general, the answer to the second question from the list above is positive. In this short note we make a step towards negative answer to the second question from the list above for finite skew braces. More precisely, we prove the following theorem.

**Theorem 3.1.** Let \( A \) be a minimal finite skew brace, such that \( A_{\oplus} \) is solvable, and \( A_\ominus \) is not solvable. Then \( A_\ominus \) is not simple.

On the way to obtaining this result, we prove the following statement which proves that the answer to the second question from the list above is negative for some finite skew braces.

**Corollary 2.2.** Let \( A \) be a finite skew brace such that the additive group \( A_{\oplus} \) is solvable. If \( |A| \) is not divisible by 3, then \( A_\ominus \) is solvable.

**Acknowledgment.** The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation.

## 2 Preliminaries

In this section we formulate and prove the necessary preliminary results.

Let \( A \) be a skew brace. Equality (11) implies that the unit element of \( A_{\oplus} \) coincides with the unit element of \( A_\ominus \), we denote this element by \( 1 \). For \( a \in A \) the map \( \lambda_a : x \mapsto \ominus a \oplus (a \odot x) \) is an automorphism of the group \( A_\ominus \). Moreover, the map \( a \mapsto \lambda_a \) gives a homomorphism \( A_\ominus \to \text{Aut}(A_{\oplus}) \).

From the definition of \( \lambda_a \) follows that for all \( a, b \in A \) the equality

\[
a \odot b = a \oplus \lambda_a(b)
\]

holds. From this equality follows, in particular, that for each \( a \in A \) the element \( a^{-1} \) has the following form

\[
a^{-1} = \ominus \lambda_a^{-1}(a).
\]

**Lemma 2.1.** Let \( G \) be a finite group, and \( p \) be a prime divisor of the index \( |G : [G,G]| \). Then there exists a characteristic subgroup \( H \) of \( G \) such that \( G/H = \mathbb{Z}_p^n \) for some \( n > 0 \).

**Proof.** Let \( |G : [G,G]| = p^k m \), where \( k > 0 \) and \( (p, m) = 1 \). Denote by \( A \) the subset

\[
A = \{ x \in G \mid x^m \in [G,G] \}
\]

of \( G \). It is clear that \( A \) is a subgroup of \( G \) such that \([G,G] \subseteq A\) and \( |G : A| = p^k \). Let \( \varphi \) be an automorphism of \( G \), and \( x \) be an element from \( A \). Then \( x^m \in [G,G] \), and therefore \( \varphi(x)^m \in [G,G] \), i.e. \( \varphi(x) \) is an element from \( A \), so, \( A \) is a characteristic subgroup of \( G \).

Denote by \( B = \{ x^p \mid x \in G/A \} \) the subgroup of \( G/A \). Since \( G/A \) is abelian \( p \)-group, it is clear that \( B \neq G/A \). Let \( H \) be the preimage of \( B \) in \( G \)

\[
H = \{ x^p a \mid x \in G, h \in A \}.
\]

It is clear that \( H \) is a subgroup of \( G \) such that \( [G,G] \leq A \subseteq H \). Let \( \varphi \) be an automorphism of \( G \), and \( x \) be an element from \( H \). Then \( x = y^p a \) for some \( y \in G, a \in A \), and therefore \( \varphi(x)^m = \varphi(y)^p \varphi(a) \).

Since \( A \) is characteristic in \( G \), the element \( \varphi(x) \) belongs to \( H \), so, \( H \) is a characteristic subgroup of \( G \).
Since $[G, G] \leq A \leq H$, the quotient $G/H$ is a finite abelian group. Since for every $x \in G$ the element $x^p$ belongs to $H$, every element from $G/H$ is of order $p$, therefore, $G/H = \mathbb{Z}_p^n$. Since $B = H/A \neq G/A$, the index $|G : H|$ is equal to

$$|G : H| = |G : A|/|H : A| \neq 1,$$

therefore $n > 0$.

**Corollary 2.2.** Let $A$ be a finite skew brace such that the additive group $A_\oplus$ is solvable. If $|A|$ is not divisible by 3, then $A_\circ$ is solvable.

**Proof.** Suppose that the statement is not correct and let $(A, \oplus, \circ)$ be a counter example of minimal order. Since $A_\oplus$ is solvable, the index $|A_\oplus : [A_\oplus, A_\oplus]|$ is divisible by some prime number $p$. From Lemma 2.1 follows that in $A_\oplus$ there exists a characteristic subgroup $H$ of index $p^n$. Consider arbitrary elements $a, b \in H$. Since $\lambda_a$ is an automorphism of $A_\oplus$, and $H$ is a characteristic subgroup of $A_\oplus$, the element $\lambda_a(b)$ belongs to $H$, and the element $a \circ b = a \oplus \lambda_a(b)$ belongs to $H$. Therefore the set $H$ is a subgroup of $A_\circ$, and hence $H$ is a skew subbrace of $A$. Since $A$ is a minimal finite skew brace, such that $A_\oplus$ is solvable, and $A_\circ$ is not solvable, and $H$ is a proper skew subbrace of $A$, the group $H_\circ$ is solvable. Let $P$ be a Sylow $p$-subgroup of $A_\circ$. This group is a $p$-group, therefore, $P$ is solvable. Since $|A_\circ : H_\circ| = p^n$ and $|A_\circ : P|$ are relatively prime, we have $A_\circ = H_\circ \circ P$. Therefore $A_\circ$ is a product of two solvable subgroups. Since $A_\circ$ is not divisible by 3, from [19] Lemma 2 follows that $A_\circ$ is solvable, what contradicts the choice of $A$.

Let $G$ be a finite group, and $p$ be a prime number. Recall that a subgroup $H$ of $G$ is said to be a $p$-complement if the index $|G : H|$ is a power of $p$, and the order $|H|$ is relatively prime with $p$. The following statement proved in [12] Theorem 7 states when a finite simple group has a $p$-complement.

**Lemma 2.3.** Let $G$ be a finite simple group, and $p$ be a prime divisor of $|G|$. If $G$ has a $p$-complement, then one of the following statements hold

1. $G = A_p$;
2. $G = \text{PSL}_n(q)$, where $q^a - 1$ is a power of $p$;
3. $G = \text{PSL}_2(11)$, $p = 11$;
4. $G = M_p$, $p = 11$ or $p = 23$.

Lemma 2.3 has the following corollary.

**Lemma 2.4.** Let $G$ be a finite group, and $p$ be a prime divisor of $|G|$. If $G$ has a solvable $p$-complement, then each non-abelian composition factor of $G$ is one of

1. $\text{PSL}_2(q)$, where $q + 1$ is a power of $p$;
2. $\text{PSL}_2(7)$, where $p = 7$;
3. $\text{PSL}_3(3)$, where $p = 13$.

**Proof.** Since $G$ has a solvable $p$-complement, each composition factor of $G$ also has a solvable $p$-complement. Since composition factors of $G$ are simple, from Lemma 2.3 follows that each non-abelian composition factor is one of

1. $A_p$,
2. $\text{PSL}_n(q)$, where $q^a - 1$ is a power of $p$,
3. $\text{PSL}_2(11)$, $p = 11$,
4. $M_p$, $p = 11$ or $p = 23$.

Let us check which cases from the list above are possible. It is clear that the $p$-complement in the alternating group $A_p$ is isomorphic to $A_{p-1}$. From the condition that the $p$-complement is solvable follows that $A_{p-1}$ is either $A_2$, or $A_3$, or $A_4$, so, $p \in \{3, 4, 5\}$. The group $A_3$ is abelian (but the statement of the lemma is about non-abelian composition factors), the group $A_4$ is not simple (but composition factors are simple), therefore the only possible case is that the composition factor is isomorphic to $A_5$, and $p = 5$. Since $A_5$ is isomorphic to $PSL_2(4)$, and $(4^2 - 1)/(4 - 1) = 5$, the composition factor is isomorphic to $PSL_2(q)$, where $q^2 - 1 = q + 1$ is a power of $p$.

Suppose that the group $PSL_2(11)$ has a solvable $11$-complement $A$. This complement is contained in some maximal subgroup $B$ of $PSL_2(11)$. Since $|PSL_2(11) : A|$ is a power of 11, and

$$|PSL_2(11) : A| = |PSL_2(11) : B||B : A|,$$

the indices $|PSL_2(11) : B|$, $|B : A|$ are powers of 11. Since $|PSL_2(11) : B|$ is a power of 11, according to the atlas [3] Page 7 the group $B$ is isomorphic to $A_5$, and $|PSL_2(11) : B| = 11$. Since $|B : A|$ is a power of 11, and $|B| = |PSL_2(11)|/11 = 60$ is not divisible by 11, we have $A = B$, therefore $A$ is not solvable. This contradiction shows that the case $PSL_2(11)$, $p = 11$ is impossible.

Suppose that the group $M_{11}$ has a solvable $11$-complement $A$. This complement is contained in some maximal subgroup $B$ of $M_{11}$. Since $|M_{11} : A|$ is a power of 11, and

$$|M_{11} : A| = |M_{11} : B||B : A|,$$

the indices $|M_{11} : B|$, $|B : A|$ are powers of 11. Since $|M_{11} : B|$ is a power of 11, according to the atlas of finite groups [3] Page 18 the group $B$ is isomorphic to $M_{10}$ which is the extension of $A_6$ by the graph automorphism, and $|M_{11} : B| = 11$. Since $|B : A|$ is a power of 11, and $|B| = |M_{11}|/11 = 2^33^25$ is not divisible by 11, we have $A = B$, therefore $A$ is not solvable. This contradiction shows that the case $M_{11}$, $p = 11$ is impossible.

Suppose that the group $M_{23}$ has a solvable $23$-complement $A$. This complement is contained in some maximal subgroup $B$ of $M_{23}$. Since $|M_{23} : A|$ is a power of 23, and

$$|M_{23} : A| = |M_{23} : B||B : A|,$$

the indices $|M_{23} : B|$, $|B : A|$ are powers of 23. Since $|M_{23} : B|$ is a power of 23, according to the atlas of finite groups [3] Page 105 the group $B$ is isomorphic to $M_{22}$, and $|M_{23} : B| = 23$. Since $|B : A|$ is a power of 23, and $|B| = |M_{23}|/23 = 2^7\cdot3^2\cdot5\cdot7\cdot11$ is not divisible by 23, we have $A = B$, therefore $A = M_{22}$ is not solvable. This contradiction shows that the case $M_{23}$, $p = 23$ is impossible.

Hence, the only possible composition factors of $G$ are the groups isomorphic to $PSL_n(q)$, where $(q^n - 1)/(q - 1)$ is a power of $p$. Let $A$ be a solvable $p$-complement in $PSL_n(q)$. The group $PSL_n(q)$ has a subgroup $B$ isomorphic to $PSL_{n-1}(q)$. The order of $B$ is relatively prime with $(q^n - 1)/(q - 1)$, and since $(q^n - 1)/(q - 1)$ is a power of $p$, the order of $B$ is relatively prime with $p$. Therefore the subgroup $B$ of $PSL_n(q)$ is contained in some $p$-complement $C$ of $PSL_n(q)$. Since $A$ and $C$ are two $p$-complements in $PSL_n(q)$, according to [4] Proposition 1 there exists an automorphism $\varphi$ of $PSL_n(q)$ such that $\varphi(A) = C$, in particular, $C$ is a solvable $p$-complement. Since $B$ is a subgroup of $C$, the group $B$ is solvable. Since $B$ is isomorphic to $PSL_{n-1}(q)$, and $PSL_{n-1}(q)$ is solvable only in the cases when $PSL_{n-1}(q) = PSL_1(q)$, $PSL_{n-1}(q) = PSL_2(2)$, or $PSL_{n-1}(q) = PSL_2(3)$, the non-abelian composition factor of $G$ which is isomorphic to $PSL_n(q)$, where $(q^n - 1)/(q - 1)$ is a power of $p$, is one of the following three

1. $PSL_2(q)$, where $q + 1$ is a power of $p$;
2. $PSL_3(2)$, where $p = 7$;
3. PSL₂(3), where \( p = 13 \).

Since PSL₂(2) is isomorphic to PSL₂(7), the lemma is proved. \( \square \)

The following statement is contained in [13, Table 5.3.A].

**Lemma 2.5.** Let \( p, q \) be powers of different primes, and \( q \neq 4,9 \). If there exists a faithful representation \( \text{PSL}_2(q) \to \text{GL}_n(p) \), then \( n \geq (q - 1)/(2, q - 1) \), where \( (2, q - 1) \) denotes the greatest common divisor of 2 and \( q - 1 \).

### 3 Proof of the main theorem

In this section we prove the following main theorem of the paper.

**Theorem 3.1.** Let \( A \) be a minimal finite skew brace, such that \( A_\circ \) is solvable, and \( A_\circ \) is not solvable. Then \( A_\circ \) is not simple.

**Proof.** Since \( A_\circ \) is solvable, the index \( |A_\circ : [A_\circ, A_\circ]| \) is greater than 1. Let \( p \) be a prime divisor of \( |A_\circ : [A_\circ, A_\circ]| \). From Lemma 2.4 follows that one of the following cases holds.

3. \( A \)

Since \( A_\circ \) is not solvable, the multiplicative group \( A_\circ \) acts on \( A_\circ/H = \mathbb{Z}_p^n \), for some \( n > 0 \). Therefore there is a homomorphism

\[ \varphi : A_\circ \to \text{Aut}(A_\circ/H) = \text{Aut}(\mathbb{Z}_p^n) = \text{GL}_n(p), \]

which maps an element \( a \in A_\circ \) to the automorphism \( \lambda_a \) of \( A/H \).

Suppose by contrary that \( A_\circ \) is simple. In this case the kernel of \( \varphi \) is either trivial, or coincides with \( A_\circ \). Suppose that \( \ker(\varphi) = A_\circ \). It means that for all \( a, b \in A \) we have \( \lambda_a(b \circ H) = b \circ H \), or \( \lambda_a(b) = b \circ h \) for some \( h \in H \) (\( h \) depends on \( a, b \)). Hence, from formula [3] follows that for every element \( a \in A \) we have \( a^{-1} = \bigoplus \lambda_a^{-1}(a) = \bigoplus(a \circ h_1) \), where \( h_1 \) is an element from \( H \) (which depends on \( a \)). Using these equalities, for arbitrary element \( a, b \in H \) we have

\[
\begin{align*}
a^{-1} \circ b \circ a &= a^{-1} \bigoplus \lambda_a^{-1}(b \circ a) \\
&= \bigoplus(a \circ h_1) \bigoplus (b \circ a) \bigoplus h_2 \\
&= \bigoplus h_1 \bigoplus a \bigoplus b \bigoplus \lambda_a(a) \bigoplus h_2 \\
&= \bigoplus h_1 \bigoplus a \bigoplus b \bigoplus a \bigoplus h_3 \bigoplus h_2 \\
&= \bigoplus h_1 \bigoplus (\bigoplus a \bigoplus b \bigoplus a) \bigoplus h_3 \bigoplus h_2
\end{align*}
\]

and since \( \bigoplus a \bigoplus b \bigoplus a \) belongs to \( H \), we conclude that \( H \) is a normal subgroup of \( A_\circ \). Since \( |A_\circ : H| = p^n \) for \( n > 0 \), the subgroup \( H \) is a proper normal subgroup of \( A_\circ \), what contradicts to the simplicity of \( A_\circ \). Therefore, the case \( \ker(\varphi) = A_\circ \) is impossible, and we have a faithful representation

\[ \varphi : A_\circ \to \text{GL}_n(p). \] (4)

Since \( \lambda_a \) is an automorphism of \( A_\circ \), and \( H \) is a characteristic subgroup of \( A_\circ \), for all \( a, b \in H \) the element \( \lambda_a(b) \) belongs to \( H \), and the element \( a \circ b = a \bigoplus \lambda_a(b) \) belongs to \( H \). Therefore \( H \) is a subgroup of \( A_\circ \), and hence \( H \) is a skew brace of \( A \). Since \( A \) is a minimal finite skew brace, such that \( A_\circ \) is solvable, and \( A_\circ \) is not solvable, the multiplicative group \( H_\circ \) is solvable, therefore by Hall theorem [11, Theorem 20.1.1] it contains a \( p \)-complement \( P \) (which is solvable). Since \( |A_\circ : H| = p^n \), and \( P \) is a solvable \( p \)-complement in \( H \), the group \( P \) is a solvable \( p \)-complement in \( A_\circ \). Since \( A_\circ \) is simple, from Lemma 2.4 follows that one of the following cases hold:

1. \( A_\circ = \text{PSL}_2(q) \), where \( q + 1 \) is a power of \( p \);
2. \( A_\odot = \text{PSL}_2(7) \), where \( p = 7 \);

3. \( A_\odot = \text{PSL}_3(3) \), where \( p = 13 \).

If we show that no of these cases possible, then we show that \( A_\odot \) cannot be simple. We will prove that no of the three cases above possible considering the cases collected in the following table.

| Case | Description |
|------|-------------|
| 1) | \( A_\odot = \text{PSL}_2(q) \), \( q + 1 \) is a power of \( p \) |
| 1.1) | \( q \) odd, \( \text{In this case } p = 2 \) |
| 1.1.1) | \( q = 3 \) |
| 1.1.2) | \( q = 7 \) |
| 1.1.3) | \( q > 7 \) |
| 1.2) | \( q \) even, \( \text{In this case } p \) odd |
| 1.2.1) | \( q = 2 \) |
| 1.2.2) | \( q = 4 \) |
| 1.2.3) | \( q > 4 \) |
| 2) | \( A_\odot = \text{PSL}_2(7) \), \( p = 7 \) |
| 3) | \( A_\odot = \text{PSL}_3(3) \), \( p = 13 \) |

**Case 1:** \( A_\odot = \text{PSL}_2(q) \), where \( q + 1 \) is a power of \( p \).

**Case 1.1:** \( q \) odd. In this case \( q + 1 \) is even, and therefore \( p = 2 \).

**Case 1.1.1:** \( A_\odot = \text{PSL}_2(3) \). This case is impossible since the group \( A_\odot = \text{PSL}_2(3) \) is solvable, but by the condition of the theorem the group \( A_\odot \) is not solvable.

**Case 1.1.2:** \( A_\odot = \text{PSL}_2(7) \). Since \( A_\odot / H = \mathbb{Z}_2^3 \) and \( |A_\odot| = |A_\odot| = |\text{PSL}_2(7)| = 2^3 \cdot 3 \cdot 7 \), the number \( n \) is either 1, 2, or 3. From formula (1) follows that there exists a faithful representation

\[
A_\odot \to \text{GL}_n(2).
\]

Since \( |\text{GL}_1(2)| = 1 \), \( |\text{GL}_2(2)| = 6 \) and \( |A_\odot| = |\text{PSL}_2(7)| = 168 \), the cases \( n = 1, 2 \) are impossible, hence, \( n = 3 \), and \( |H| = 3 \cdot 7 = 21 \).

Let \( X \) be a Sylow 7-subgroup of \( H \). This group is a cyclic group of order 7. By Sylow theorem, \( X \) is a unique Sylow 7-subgroup of \( H \), therefore \( X \) is a characteristic subgroup of \( H \). Since \( H \) is a characteristic subgroup of \( A_\odot \), and \( X \) is a characteristic subgroup of \( H \), the group \( X \) is a characteristic subgroup of \( A_\odot \). Denote by \( G = A_\odot \times A_\odot = A_\odot \times \text{PSL}_2(7) \), where \( A_\odot = \text{PSL}_2(7) \) acts on \( A_\odot \) by automorphisms \( \lambda_a \) for \( a \in A_\odot \).

Since \( X \) is characteristic in \( A_\odot \), and \( A_\odot = \text{PSL}_2(7) \) acts on \( A_\odot \), the group \( A_\odot = \text{PSL}_2(7) \) acts on \( X \), therefore \( X \) is a normal subgroup of \( G \). Let \( C = C_G(X) \) be the centralizer of \( X \) in \( G \). Since \( X \) is a normal subgroup of \( G \), the group \( C \) is also a normal subgroup of \( G \). Since \( X \) is cyclic, the group \( \text{Aut}(X) \) is abelian, and since \( A_\odot = \text{PSL}_2(7) \) is simple, the group \( A_\odot = \text{PSL}_2(7) \) acts trivially on \( X \), so, \( A_\odot = \text{PSL}_2(7) \) is a subgroup of \( C \).

Since \( C \) is a normal subgroup of \( G \), the group \( CH/H \) is a normal subgroup of \( G/H = (A_\odot / H) \rtimes A_\odot = (\mathbb{Z}_2)^3 \rtimes \text{PSL}_2(7) \).

Moreover, since \( A_\odot = \text{PSL}_2(7) \) is a subgroup of \( C \), we have the following inclusions

\[
\text{PSL}_2(7) \leq CH/H \leq (\mathbb{Z}_2)^3 \rtimes \text{PSL}_2(7).
\]

From this inclusions follows that \( CH/H = B \rtimes \text{PSL}_2(7) \), where \( B \) is a subgroup of \( \mathbb{Z}_2^3 \). If \( B \) is a proper subgroup of \( \mathbb{Z}_2^3 \), then the semidirect product

\[
(A_\odot / H) \rtimes A_\odot = (\mathbb{Z}_2)^3 \rtimes \text{PSL}_2(7)
\]

is a direct product (since \( \text{PSL}_2(7) \) cannot act nontrivially on \( B < \mathbb{Z}_2^3 \)). Therefore, the homomorphism

\[
\varphi : A_\odot \to \text{Aut}(A_\odot / H) = \text{GL}_3(2),
\]
which maps an element $a \in A_7$ to the automorphism $\lambda_a$ of $A/H$ is trivial, what contradicts formula $[1]$. Hence $B$ cannot be a proper subgroup of $B$, i.e. either $CH/H = \text{PSL}_2(7)$ or $CH/H = (\mathbb{Z}_2)^3 \times \text{PSL}_2(7)$. Let us prove that no of these cases is possible.

If $CH/H = \text{PSL}_2(7)$, then due to the fact that $CH/H$ is normal in $G/H = (\mathbb{Z}_2)^3 \times \text{PSL}_2(7)$, the semidirect product $(A_7/H) \times A_7 = (\mathbb{Z}_2)^3 \times \text{PSL}_2(7)$ is a direct product. Therefore, the homomorphism $\varphi : A_7 \rightarrow \text{Aut}(A_7/H) = \text{GL}_3(2)$, which maps an element $a \in A_7$ to the automorphism $\lambda_a$ of $A/H$ is trivial, what contradicts formula $[1]$. Hence, the case $CH/H = \text{PSL}_2(7)$ is impossible, and we have $CH/H = G/H$, or equivalently $CH = G$. Here we have two cases: either $C \cap A_7 = A_7$ or $C \cap A_7 \neq A_7$.

If $C \cap A_7 = A_7$, then $A_7$ normalizes $X$, therefore $A_7 = X \times D$, where $D$ is a Hall $\{2,3\}$-subgroup of $A_7$. Since $A_7 = X \times D$, where $D$ is a Hall $\{2,3\}$-subgroup of $A_7$, the group $D$ is characteristic in $A_7$. Therefore the group $\text{PSL}_2(7)$ acts on $A_7/D$. Since the group $A_7/D$ has order $|A_7/D| = |A_7|/|D| = |X| = 7$, it is a cyclic group, and $|\text{Aut}(A_7/D)|$ is abelian. Since $A_7 = \text{PSL}_2(7)$ is simple, the group $A_7 = \text{PSL}_2(7)$ acts trivially on $A_7/D$. It means that for all $a, b \in A$ we have $\lambda_a(b \oplus d) = b \oplus d$, or $\lambda_a(b) = b \oplus d$ for some $d \in D$ ($d$ depends on $a, b$). Hence, from formula $[3]$ follows that for every element $a \in A$ we have $a^{-1} = \ominus \lambda_a^{-1}(a) = \ominus(a \oplus d_1)$, where $d_1$ is an element from $D$ (which depends on $a$). Using these equalities, for arbitrary element $a \in A$, $b \in D$ we have

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

$$= \ominus(a \oplus d_1) \circ (b \circ a) \circ d_2$$

$$= \ominus d_1 \circ a \circ b \circ \lambda_b(a) \circ d_2$$

$$= \ominus d_1 \circ (a \oplus b) \circ a \circ d_3 \circ d_2$$

$$= \ominus d_1 \circ (a \oplus b \circ a) \circ d_3 \circ d_2$$

and since $\ominus a \circ b \circ a$ belongs to $D$, we conclude that $D$ is a normal subgroup of $A_7$. Since $|A_7 : D| = 7$, the subgroup $D$ is a proper normal subgroup of $A_7$, what contradicts to the simplicity of $A_7$. So, the case $C \cap A_7 = A_7$ is impossible.

If $C \cap A_7 \neq A_7$, then since $CH = G$, the group $C$ contains a Sylow 2-subgroup of $A_7$. Since $C \cap A_7 \neq A_7$, and $C \cap A_7$ contains both Sylow 7-subgroup $X$ of $A_7$ and Sylow 2-subgroup of $A_7$, the group $C \cap A_7$ is a Hall $\{2,7\}$-subgroup of $A_7$. Since $C, A_7$ are normal subgroups of $G$, the group $C \cap A_7$ is a normal subgroup of $G$. Therefore, the group $A_7$ acts on $C \cap A_7$, and hence $C \cap A_7$ is a skew subbrace of $A$, in particular, $C \cap A_7$ is a Hall $\{2,7\}$-subgroup of $A_7$. So, the group $A_7$ has a 2-complement $H$, and a 3-complement $C \cap A_7$, therefore by [1] Corollary 4.4 the group $A_7$ is solvable, what contradicts the choice of $A$.

**Case 1.1.3:** $A_7 = \text{PSL}_2(q)$, where $q > 7$. The order of the group $A_7 = \text{PSL}_2(q)$ is equal to

$$|\text{PSL}_2(q)| = \frac{(q-1)q(q+1)}{2}.$$

Therefore the maximal power of 2 which divides $|\text{PSL}_2(q)|$ is equal to $(q+1)$ ($(q+1)$ is a power of 2, $q$ is odd, and $q-1$ is divisible by 2, but not divisible by 4). From formula $[4]$ follows that there exists a faithful representation

$$\text{PSL}_2(q) \rightarrow \text{GL}_n(2),$$

where $n \leq \log_2(q+1)$. From the other side from Lemma $[2]$ follows that if there exists a faithful representation $\text{PSL}_2(q) \rightarrow \text{GL}_n(2)$, then $n \geq (q-1)/2$. From these two inequalities follows that $\log_2(q+1) \leq (q-1)/2$ or $q+1 \geq 2^{(q-1)/2}$. This inequality is impossible for $q > 7$, therefore the case $A_7 = \text{PSL}_2(q)$, where $q+1$ is a power of $p$, and $q > 7$ is impossible.

**Case 1.2:** $q$ is even.

**Case 1.2.1:** $A_7 = \text{PSL}_2(2)$. This case is impossible since the group $A_7 = \text{PSL}_2(2)$ is solvable, but by the condition of the theorem the group $A_7$ is not solvable.
Case 1.2.2: $A_\odot = \text{PSL}_2(4)$. In this case $p = 5$. Since the order of $A_\odot = \text{PSL}_2(4)$ is equal to $|\text{PSL}_2(4)| = 2^2 \cdot 3 \cdot 5$, and $|A_\odot : H| = p^n = 5^n$, we conclude that $n = 1$. From formula (3) follows that there exists a faithful representation
\[ \varphi: \text{PSL}_2(4) \to \text{GL}_1(5). \]
But such representation cannot exist due to the equalities $|\text{PSL}_2(4)| = 2^2 \cdot 3 \cdot 5$, $\text{GL}_1(5) = 4$. Hence, the case $A_\odot = \text{PSL}_2(4)$, $p = 5$ is impossible.

Case 1.2.3: $A_\odot = \text{PSL}_2(q)$ for $q > 4$ is impossible. Since $q$ is even, $p$ is odd, hence $p \geq 3$. The order of the group $A_\odot = \text{PSL}_2(q)$ is equal to
\[ |\text{PSL}_2(q)| = (q-1)q(q+1). \]
Therefore the maximal power of $p$ which divides $|\text{PSL}_2(q)|$ is equal to $(q+1)$ ($(q+1)$ is a power of $p$, and $q(q-1)$ is relatively prime with $p$). From formula (4) follows that there exists a faithful representation
\[ \text{PSL}_2(q) \to \text{GL}_n(p), \]
where $n \leq \log_p(q + 1)$. From the other side from Lemma 2.3 follows that if there exists a faithful representation $\text{PSL}_2(q) \to \text{GL}_n(p)$, then $n \geq (q-1)$. From these two equalities follows that
\[ \log_p(q + 1) \geq (q-1) \]
or $(q + 1) \geq p^{q-1} \geq 3^{q-1}$. This inequality is impossible for $q > 4$, therefore the case $A_\odot = \text{PSL}_2(q)$, where $q + 1$ is a power of $p$, and $q > 4$ is impossible.

Case 2: $A_\odot = \text{PSL}_3(3)$, $p = 13$. Since the order of $A_\odot = \text{PSL}_3(3)$ is equal to $|\text{PSL}_3(3)| = 2^4 \cdot 3 \cdot 13$, and $|A_\odot : H| = p^n = 13^n$, we conclude that $n = 1$. From formula (4) follows that there exists a faithful representation
\[ \varphi: \text{PSL}_3(3) \to \text{GL}_1(13). \]
But such representation cannot exist due to the equalities $|\text{PSL}_3(3)| = 2^4 \cdot 3 \cdot 13$, $\text{GL}_1(13) = 12$. Hence, the case $A_\odot = \text{PSL}_3(3)$, $p = 13$ is impossible.

Case 3: $A_\odot = \text{PSL}_2(7)$, $p = 7$. Since the order of $A_\odot = \text{PSL}_2(7)$ is equal to $|\text{PSL}_2(7)| = 2^3 \cdot 3 \cdot 7$, and $|A_\odot : H| = p^n = 7^n$, we conclude that $n = 1$. From formula (4) follows that there exists a faithful representation
\[ \varphi: \text{PSL}_2(7) \to \text{GL}_1(7). \]
But such representation cannot exist due to the equalities $|\text{PSL}_2(7)| = 2^3 \cdot 3 \cdot 7$, $\text{GL}_1(7) = 6$. Hence, the case $A_\odot = \text{PSL}_2(7)$, $p = 7$ is impossible.

\[ \square \]

References

[1] Z. Arad, M. Ward, New criteria for the solvability of finite groups, J. Algebra, V. 77, N. 1, 1982, 234–246.
[2] V. Bardakov, T. Nasybullov, Multi-switches and representations of braid groups, ArXiv:Math/1907.09230.
[3] V. Bardakov, T. Nasybullov, Multi-switches and virtual knot invariants, ArXiv:Math/2001.09711.
[4] A. Buturlakin, D. Revin, On $p$-complements of finite groups, Sib. Electron. Math. Rep., V. 10, 2013, 414–417.
[5] N. Byott, Solubility criteria for Hopf-Galois structures, New York J. Math., V. 21, 2015, 883–903.
[6] F. Cedó, A. Smoktunowicz, L. Vendramin, Skew left braces of nilpotent type, Proc. London Math. Soc., V. 118, N. 6, 2019, 1367–1392.
[7] L. N. Childs, Skew braces and the Galois correspondence for Hopf Galois structures, J. Algebra, V. 511, 2018, 270–291.
[8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups: maximal subgroups and ordinary characters for simple groups, Oxford [Oxfordshire]: Clarendon Press; New York: Oxford University Press, 1985.
[9] L. Guarnieri, L. Vendramin, Skew braces and the Yang-Baxter equation, Math. Comp., V. 86, N. 307, 2017, 2519–2534.
[10] E. Jespers, L. Kubat, A. Van Antwerpen, L. Vendramin, Factorizations of skew braces, Math. Annalen, V. 375. N. 3-4, 2019, 1649–1663.
[11] M. Kargapolov, Ju. Merzljakov, Fundamentals of the theory of groups, Translated from the second Russian edition by Robert G. Burns. Graduate Texts in Mathematics 62. Springer-Verlag, New York-Berlin, 1979.
[12] L. Kazarin, On the product of finite groups (Russian), Dokl. Akad. Nauk SSSR, V. 269, N. 3, 1983, 528–531.
[13] P. Kleidman, M. Liebeck, The subgroup structure of the finite classical groups, Cambridge University Press, 1990.
[14] A. Konovalov, A. Smoktunowicz, L. Vendramin, On skew braces and their ideals, ArXiv:Math/1804.04106.
[15] The Kourovka notebook, Unsolved problems in group theory. Edited by V. D. Mazurov and E. I. Khukhro, 19-th. ed.. Russian Academy of Sciences Siberian Division. Institute of Mathematics, Novosibirsk, 2018.
[16] T. Nasybullov, Connections between properties of the additive and the multiplicative groups of a two-sided skew brace, J. Algebra, V. 540, 2019, 156–167.
[17] W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra, V. 307, N. 1, 2007, 153–170.
[18] A. Smoktunowicz, L. Vendramin, On skew braces (with an appendix by N. Byott and L. Vendramin), J. Comb. Algebra, V. 2, N. 1, 2018, 47–86.
[19] S. Syskin, On a question of R. Baer (Russian), Sib. Mat. Zh., V. 20, 1979, 679–681.
[20] C. Tsang, Q. Chao, On the solvability of regular subgroups in the holomorph of a finite solvable group, Int. J. Algebra Comput., V. 30, N. 2, 2020, 253–265.
[21] L. Vendramin, Problems on skew left braces, Advances in Group Theory and Applications, V. 7, 2019, 15–37.

Ilya Gorshkov
Sobolev Institute of Mathematics, Acad. Koptyug avenue 4, 630090 Novosibirsk, Russia
ilygor8@gmail.com

Timur Nasybullov
Sobolev Institute of Mathematics, Acad. Koptyug avenue 4, 630090 Novosibirsk, Russia
Novosibirsk State University, Pirogova 1, 630090 Novosibirsk, Russia
ntr@math.nsc.ru