Simple Skew Braces

Nigel Byott

University of Exeter

Omaha, 1 June 2023

§1 Definitions

Definition: A **skew brace** $B = (B, +, \circ)$ consists of a set B and two operations $+$, $\circ$ so that

- $(B, +)$ is a group (the additive group of B);
- $(B, \circ)$ is a group (the multiplicative group of B);
- $a \circ (b + c) = (a \circ b) - a + (a \circ c)$ for all a, b, $c \in B$.

Its **opposite skew brace** B^{op} is $(B, +^{\mathrm{op}}, \circ)$. This might or might not be isomorphic to B.

B is a **brace** if $(B, +)$ is abelian.

§1 Definitions

Definition: A **skew brace** $B = (B, +, \circ)$ consists of a set B and two operations $+$, $\circ$ so that

- $(B, +)$ is a group (the additive group of B);
- $(B, \circ)$ is a group (the multiplicative group of B);
- $a \circ (b + c) = (a \circ b) - a + (a \circ c)$ for all a, b, $c \in B$.

Its **opposite skew brace** B^{op} is $(B, +^{\mathrm{op}}, \circ)$. This might or might not be isomorphic to B.

B is a **brace** if $(B, +)$ is abelian.

There is a homomorphism of groups $\lambda : (B, \circ) \to \mathrm{Aut}(B, +)$ given by

$$a \mapsto \lambda_a \text{ where } \lambda_a(b) = -a + a \circ b.$$

§1 Definitions

Definition: A **skew brace** $B = (B, +, \circ)$ consists of a set B and two operations $+$, $\circ$ so that

- $(B, +)$ is a group (the additive group of B);
- $(B, \circ)$ is a group (the multiplicative group of B);
- $a \circ (b + c) = (a \circ b) - a + (a \circ c)$ for all a, b, $c \in B$.

Its **opposite skew brace** B^{op} is $(B, +^{\mathrm{op}}, \circ)$. This might or might not be isomorphic to B.

B is a **brace** if $(B, +)$ is abelian.

There is a homomorphism of groups $\lambda : (B, \circ) \to \mathrm{Aut}(B, +)$ given by

$$a \mapsto \lambda_a \text{ where } \lambda_a(b) = -a + a \circ b.$$

Definition: An **ideal** in a skew brace B is a subset I of B such that

- $(I, +) \lhd (B, +)$,
- $(I, \circ) \lhd (B, \circ)$,
- $\lambda_a(I) \subseteq I$ for all $a \in B$.

This is what we need to define a quotient skew brace B/I.

Definition: A skew brace $B \neq \{0\}$ is **simple** if it has no quotient skew braces except $\{0\}$ and B, i.e. if it has no ideal I with $\{0\} \subsetneq I \subsetneq B$.

Definition: A skew brace $B \neq \{0\}$ is **simple** if it has no quotient skew braces except $\{0\}$ and B, i.e. if it has no ideal I with $\{0\} \subsetneq I \subsetneq B$.

We would like to understand/classify all finite simple skew braces, since these are the "building blocks" from which all finite skew braces are built up.

Definition: A skew brace $B \neq \{0\}$ is **simple** if it has no quotient skew braces except $\{0\}$ and B, i.e. if it has no ideal I with $\{0\} \subsetneq I \subsetneq B$.

We would like to understand/classify all finite simple skew braces, since these are the "building blocks" from which all finite skew braces are built up.

As with finite simple groups, we cannot expect the answer to be easy!

§2 Some Examples

(a) For each prime p, the (trivial) brace of order p is a simple skew brace. These are the only simple *braces* of prime power order.

(b) **Simple braces**:
Many examples have been constructed by Bachiller and by Cedó, Jespers and Okniński using matched pairs of braces.
It is known that every finite abelian group is a *subgroup* of the multiplicative group of a simple brace.
As far as I know, there are no classification results for simple braces going beyond (a).

(c) If B is a skew brace with either $(B,+)$ or $(B,\circ)$ a nonabelian simple group, then we get for free that B is simple.

(i) $(B,+)$ is nonabelian simple:
If G is a non-abelian simple group with an exact factorisation $G = HJ$, $H \cap J = \{1\}$, then we can construct a skew brace B with $(B,+) \cong G$ and $(B,\circ) \cong H \times J$. For example, if $n \geq 5$ then we can have

$$(B,+) \cong A_n, \qquad (B,\circ) \cong C_n \times A_{n-1}.$$

When $n = 5$ this gives an example with $(B,+)$ nonabelian simple and $(B,\circ)$ solvable.
Cindy Tsang has found all instances of this phenomenon.

(c) If B is a skew brace with either $(B,+)$ or $(B,\circ)$ a nonabelian simple group, then we get for free that B is simple.

(i) $(B,+)$ is nonabelian simple:
If G is a non-abelian simple group with an exact factorisation $G = HJ$, $H \cap J = \{1\}$, then we can construct a skew brace B with $(B,+) \cong G$ and $(B,\circ) \cong H \times J$. For example, if $n \geq 5$ then we can have

$$(B,+) \cong A_n, \qquad (B,\circ) \cong C_n \times A_{n-1}.$$

When $n = 5$ this gives an example with $(B,+)$ nonabelian simple and $(B,\circ)$ solvable.
Cindy Tsang has found all instances of this phenomenon.

(ii) $(B,\circ)$ is nonabelian simple:
The only possibilities are the trivial skew brace $(B,+,+)$ and its opposite $(B,+^{\mathrm{op}},+)$.
[This is a reinterpretation of an old result on Hopf-Galois structures (NB, 2004): a Galois extension whose Galois group is a nonabelian simple group G admits only two Hopf-Galois structures, and these are both of type G.]

(d) Computer calculations.
Leandro Vendramin (2022, unpublished) found that there are two simple skew braces of order 12 (up to isomorphism). These are the smallest simple skew braces which are not braces. Both have

$$(B, +) \cong A_4 \cong (C_2 \times C_2) \rtimes C_3, \qquad (B, \circ) \cong C_3 \rtimes C_4.$$

(d) Computer calculations.
Leandro Vendramin (2022, unpublished) found that there are two simple skew braces of order 12 (up to isomorphism). These are the smallest simple skew braces which are not braces. Both have

$$(B,+) \cong A_4 \cong (C_2 \times C_2) \rtimes C_3, \qquad (B,\circ) \cong C_3 \rtimes C_4.$$

Question (Vendramin): Is there an infinite family of simple skew braces into which these two examples of order 12 fit?

(d) Computer calculations.
Leandro Vendramin (2022, unpublished) found that there are two simple skew braces of order 12 (up to isomorphism). These are the smallest simple skew braces which are not braces. Both have

$$(B,+) \cong A_4 \cong (C_2 \times C_2) \rtimes C_3, \qquad (B,\circ) \cong C_3 \rtimes C_4.$$

Question (Vendramin): Is there an infinite family of simple skew braces into which these two examples of order 12 fit?

Aim for the rest of the talk: I will give a more-or-less explicit construction for such a family ...

(d) Computer calculations.
Leandro Vendramin (2022, unpublished) found that there are two simple skew braces of order 12 (up to isomorphism). These are the smallest simple skew braces which are not braces. Both have

$$(B,+) \cong A_4 \cong (C_2 \times C_2) \rtimes C_3, \qquad (B,\circ) \cong C_3 \rtimes C_4.$$

Question (Vendramin): Is there an infinite family of simple skew braces into which these two examples of order 12 fit?

Aim for the rest of the talk: I will give a more-or-less explicit construction for such a family ...

... but first I need to explain what I mean by "construction".

If $(B, +, \circ)$ is a skew brace, we have the homomorphism

$$\lambda : (B, \circ) \to \mathrm{Aut}(B, +), \qquad a \mapsto \lambda_a,$$

so we have an injection

$$(B, \circ) \to \mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +), \qquad b \mapsto [b, \lambda_b]$$

which embeds $(B, \circ)$ as a regular subgroup of $\mathrm{Hol}(B, +)$.

If $(B, +, \circ)$ is a skew brace, we have the homomorphism

$$\lambda : (B, \circ) \to \mathrm{Aut}(B, +), \qquad a \mapsto \lambda_a,$$

so we have an injection

$$(B, \circ) \to \mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +), \qquad b \mapsto [b, \lambda_b]$$

which embeds $(B, \circ)$ as a regular subgroup of $\mathrm{Hol}(B, +)$.

Conversely, given a group N and a regular subgroup G of $\mathrm{Hol}(N)$, we obtain a skew brace B with $(B, +) \cong N$ and $(B, \circ) \cong G$.

If $(B, +, \circ)$ is a skew brace, we have the homomorphism

$$\lambda : (B, \circ) \to \mathrm{Aut}(B, +), \qquad a \mapsto \lambda_a,$$

so we have an injection

$$(B, \circ) \to \mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +), \qquad b \mapsto [b, \lambda_b]$$

which embeds $(B, \circ)$ as a regular subgroup of $\mathrm{Hol}(B, +)$.

Conversely, given a group N and a regular subgroup G of $\mathrm{Hol}(N)$, we obtain a skew brace B with $(B, +) \cong N$ and $(B, \circ) \cong G$.

So will shall consider finding a regular subgroup in $\mathrm{Hol}(N)$ as equivalent to constructing a skew brace.

If $(B, +, \circ)$ is a skew brace, we have the homomorphism

$$\lambda : (B, \circ) \to \mathrm{Aut}(B, +), \qquad a \mapsto \lambda_a,$$

so we have an injection

$$(B, \circ) \to \mathrm{Hol}(B, +) = (B, +) \rtimes \mathrm{Aut}(B, +), \qquad b \mapsto [b, \lambda_b]$$

which embeds $(B, \circ)$ as a regular subgroup of $\mathrm{Hol}(B, +)$.

Conversely, given a group N and a regular subgroup G of $\mathrm{Hol}(N)$, we obtain a skew brace B with $(B, +) \cong N$ and $(B, \circ) \cong G$.

So will shall consider finding a regular subgroup in $\mathrm{Hol}(N)$ as equivalent to constructing a skew brace.

Then looking for skew braces with a given additive group is pretty much the same thing as looking for Hopf-Galois structures of a given type (after reformulating the Greither-Pareigis theorem in terms of holomorphs, and leaving aside "counting questions").

§3 Constructing Some Simple Skew Braces

Let p, q be primes such that q divides $\dfrac{p^p - 1}{p - 1}$, e.g.

- $p = 2$, $q = 3$;
- $p = 3$, $q = 13$;
- $p = 5$, $q = 11$ or 71.

§3 Constructing Some Simple Skew Braces

Let p, q be primes such that q divides $\dfrac{p^p - 1}{p - 1}$, e.g.

- $p = 2$, $q = 3$;
- $p = 3$, $q = 13$;
- $p = 5$, $q = 11$ or 71.

We will construct a simple skew brace B of order $p^p q$.

- for $p = 2$, we have $|B| = 2^2 \cdot 3 = 12$;
- for $p = 3$, we have $|B| = 3^3 \cdot 13 = 351$;
- for $p = 5$, we have $|B| = 5^5 \cdot 11 = 34\,374$ or $5^5 \cdot 71 = 221\,875$.

(i) Construction of N

Let V be an elementary abelian group of order p^p, which we view as the vector space $\mathbb{F}_p^p$ of column vectors over the field $\mathbb{F}_p$ of p elements.
Let

$$J = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \in \mathrm{GL}_p(\mathbb{F}_p) = \mathrm{Aut}(V).$$

Thus J is a single Jordan block with eigenvalue 1, and $(J - I)^p = 0$, so $J^p = I$.

Claim:

There is a matrix M in $\mathrm{GL}_p(\mathbb{F}_p)$ of order q such that $JMJ^{-1} = M^p$.

Claim:

There is a matrix M in $\mathrm{GL}_p(\mathbb{F}_p)$ of order q such that $JMJ^{-1} = M^p$.

Sketch of Proof:
(This is the only point where are construction is not completely explicit.)

Claim:

There is a matrix M in $\mathrm{GL}_p(\mathbb{F}_p)$ of order q such that $JMJ^{-1} = M^p$.

Sketch of Proof:
(This is the only point where are construction is not completely explicit.)

We use some results on central simple algebras.

Claim:

There is a matrix M in $\mathrm{GL}_p(\mathbb{F}_p)$ of order q such that $JMJ^{-1} = M^p$.

Sketch of Proof:
(This is the only point where are construction is not completely explicit.)

We use some results on central simple algebras.

Let $M_0 \in \mathrm{GL}_p(\mathbb{F}_p)$ have order q. (Take $\omega \in \mathbb{F}_{p^p}^\times$ of order q and take M_0 to be the companion matrix of the minimal polynomial of ω over $\mathbb{F}_p$.)

Claim:

There is a matrix M in $\mathrm{GL}_p(\mathbb{F}_p)$ of order q such that $JMJ^{-1} = M^p$.

Sketch of Proof:
(This is the only point where are construction is not completely explicit.)

We use some results on central simple algebras.

Let $M_0 \in \mathrm{GL}_p(\mathbb{F}_p)$ have order q. (Take $\omega \in \mathbb{F}_{p^p}^\times$ of order q and take M_0 to be the companion matrix of the minimal polynomial of ω over $\mathbb{F}_p$.)

Consider the subalgebra $A = \mathbb{F}_p[M_0]$ of the matrix algebra $\mathcal{M}_p(\mathbb{F}_p)$. By the Double Centraliser Theorem, A is its own centraliser in $\mathcal{M}_p(\mathbb{F}_p)$.

Claim:

There is a matrix M in $\mathrm{GL}_p(\mathbb{F}_p)$ of order q such that $JMJ^{-1} = M^p$.

Sketch of Proof:
(This is the only point where are construction is not completely explicit.)

We use some results on central simple algebras.

Let $M_0 \in \mathrm{GL}_p(\mathbb{F}_p)$ have order q. (Take $\omega \in \mathbb{F}_{p^p}^\times$ of order q and take M_0 to be the companion matrix of the minimal polynomial of ω over $\mathbb{F}_p$.)

Consider the subalgebra $A = \mathbb{F}_p[M_0]$ of the matrix algebra $\mathcal{M}_p(\mathbb{F}_p)$. By the Double Centraliser Theorem, A is its own centraliser in $\mathcal{M}_p(\mathbb{F}_p)$.

Since $A \cong \mathbb{F}_{p^p}$, its automorphism group is generated by the Frobenius map $M_0 \mapsto M_0^p$, which has order p. By the Skolem-Noether Theorem, there is a matrix J_0 such that $J_0 M_0 J_0^{-1} = M_0^p$. Multiplying J_0 by an element of the centraliser of A, we may assume that J_0 has order p. Then conjugation by J_0 cannot fix any proper subspace of V, so J_0 is conjugate to a single Jordan block. We can therefore make a change of basis transforming J_0 to J and M_0 to the required matrix M.

Now form the group of $(p+1) \times (p+1)$ matrices

$$N = \left\{ \left(\begin{array}{c|c} M^k & v \\ \hline 0 & 1 \end{array} \right) : 0 \leq k \leq q-1, v \in V \right\}.$$

This will be the additive group of our simple skew brace.

Now form the group of $(p+1) \times (p+1)$ matrices

$$N = \left\{ \left(\begin{array}{c|c} M^k & v \\ \hline 0 & 1 \end{array} \right) : 0 \leq k \leq q-1, v \in V \right\}.$$

This will be the additive group of our simple skew brace.

N is a nonabelian group of order $p^p q$, and its only normal subgroups are $\{I\}$, V, N.

(ii) Construction of G

Inside $\mathrm{Hol}(N)$, we will construct a regular subgroup $G \cong C_q \rtimes P$, where P is a certain group of order p^p and exponent p^2, acting nontrivially on C_q. Thus G has no normal subgroup of order p^p.

(ii) Construction of G

Inside $\mathrm{Hol}(N)$, we will construct a regular subgroup $G \cong C_q \rtimes P$, where P is a certain group of order p^p and exponent p^2, acting nontrivially on C_q. Thus G has no normal subgroup of order p^p.

Then G corresponds to a skew brace $(B, +, \circ)$ with $(B, +) \cong N$ and $(B, \circ) \cong G$.

(ii) Construction of G

Inside $\mathrm{Hol}(N)$, we will construct a regular subgroup $G \cong C_q \rtimes P$, where P is a certain group of order p^p and exponent p^2, acting nontrivially on C_q. Thus G has no normal subgroup of order p^p.

Then G corresponds to a skew brace $(B, +, \circ)$ with $(B, +) \cong N$ and $(B, \circ) \cong G$.

Then B must be simple since $(B, +)$ only has normal subgroups of order 1, p^p, $p^p q$ and $(B, \circ)$ does not have a normal subgroup of order p^p.

[When $p = 2$, $q = 3$ we have $N \cong \mathbb{F}_2^2 \rtimes C_3 \cong A_4$ and $N \cong C_3 \rtimes C_4$, as in Vendramin's example.]

To work with $\mathrm{Hol}(N)$, we first need to understand $\mathrm{Aut}(N)$. The group

$$N = \left\{ \left(\begin{array}{c|c} M^k & v \\ \hline 0 & 1 \end{array} \right) : 0 \le k \le q-1, v \in V \right\}$$

has trivial centre, so $\mathrm{Aut}(N)$ contains a copy of N (acting by conjugation). In fact

$$\mathrm{Aut}(N) = \left\{ \left(\begin{array}{c|c} A & v \\ \hline 0 & 1 \end{array} \right) : A \text{ normalises } \langle M \rangle, v \in V \right\}$$

(acting by conjugation).

In particular, we can take $A = M^k$ for $k \in \mathbb{Z}$, or $A = J$.

Write elements of $\mathrm{Hol}(N)$ as $[\eta, \alpha]$ with $\eta \in N$, $\alpha \in \mathrm{Aut}(N)$.

Let $e_1, \ldots, e_p$ be the standard basis of $V = \mathbb{F}_p^p$.

We will define certain elements of $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$.

Let

$$X = \left[\left(\begin{array}{c|c} M & 0 \\ \hline 0 & 1 \end{array} \right), \mathrm{conj} \left(\begin{array}{c|c} I & 0 \\ \hline 0 & 1 \end{array} \right) \right], \; Y = \left[\left(\begin{array}{c|c} I & e_p \\ \hline 0 & 1 \end{array} \right), \mathrm{conj} \left(\begin{array}{c|c} J & -e_p \\ \hline 0 & 1 \end{array} \right) \right],$$

$$Z_v = \left[\left(\begin{array}{c|c} I & v \\ \hline 0 & 1 \end{array} \right), \mathrm{conj} \left(\begin{array}{c|c} I & -v \\ \hline 0 & 1 \end{array} \right) \right] \text{ for each } v \in V.$$

These move 0_N to M, e_p, v respectively, and satisfy the relations

$$X^q = I, \qquad YXY^{-1} = X^p, \qquad Y^p = Z_{e_1}, \qquad Z_v X = X Z_v,$$

$$Z_v Z_w = Z_{v+w}, \qquad Y Z_v Y^{-1} Z_v^{-1} = Z_{Jv-v}$$

so that, in particular

$$Y Z_{e_i} Y^{-1} Z_{e_i}^{-1} = Z_{e_{i-1}} \text{ for } 2 \le i \le p.$$

Let $P = \langle Y, Z_{e_{p-1}} \rangle = \langle Y, Z_{e_{p-1}}, Z_{e_{p-2}}, \ldots, Z_{e_1} = Y^p \rangle$.

Let $P = \langle Y, Z_{e_{p-1}} \rangle = \langle Y, Z_{e_{p-1}}, Z_{e_{p-2}}, \ldots, Z_{e_1} = Y^p \rangle$.

The group P acts regularly on V, has exponent p^2 and has derived length 2 since $\langle Z_{e_{p-1}}, Z_{e_{p-2}}, \ldots, Z_{e_1} \rangle$ is an abelian normal subgroup of index p, but P has nilpotency class $p-1$. In particular, P is abelian only when $p = 2$. So P is a subgroup of $\mathrm{Hol}(V) \leq \mathrm{Hol}(N)$ of order p^p which is regular on V.

Let $P = \langle Y, Z_{e_{p-1}} \rangle = \langle Y, Z_{e_{p-1}}, Z_{e_{p-2}}, \ldots, Z_{e_1} = Y^p \rangle$.

The group P acts regularly on V, has exponent p^2 and has derived length 2 since $\langle Z_{e_{p-1}}, Z_{e_{p-2}}, \ldots, Z_{e_1} \rangle$ is an abelian normal subgroup of index p, but P has nilpotency class $p-1$. In particular, P is abelian only when $p = 2$. So P is a subgroup of $\mathrm{Hol}(V) \leq \mathrm{Hol}(N)$ of order p^p which is regular on V.

Finally, $G = \langle X, Y, Z_{e_{p-1}} \rangle \cong C_q \rtimes P$ does what we want.

§4 Opposite skew braces

We sketch a proof that the skew brace B we have constructed is not isomorphic to its opposite skew brace. Thus for each pair p, q as above, we have get two simple skew braces.

§4 Opposite skew braces

We sketch a proof that the skew brace B we have constructed is not isomorphic to its opposite skew brace. Thus for each pair p, q as above, we have get two simple skew braces.

We have made the group $(N, +)$ into a skew brace $(N, +, \circ)$ by constructing a regular subgroup

$$G = \{g_\eta : \eta \in N\} \leq \mathrm{Hol}(N, +)$$

where $g_\eta = [\eta, \alpha_\eta]$ for $\alpha_\eta \in \mathrm{Aut}(N, +)$, and then defining $\circ$ so that $g_{\eta \circ \mu} = g_\eta g_\mu$.

It is not obvious how to find a regular subgroup of $\mathrm{Hol}(N, +)$ corresponding to $(N, +^{\mathrm{op}}, \circ)$.

Instead, we look for a bijection $\Phi : N \to N$ such that

(i) Φ is an antihomomorphism of $(N, +)$,

(ii) Φ is an automorphism of $(N, \circ)$.

Instead, we look for a bijection $\Phi : N \to N$ such that

(i) Φ is an antihomomorphism of $(N, +)$,

(ii) Φ is an automorphism of $(N, \circ)$.

Then (i) is equivalent to

$$\text{there exists } \alpha \in \mathrm{Aut}(N, +) \text{ with } \Phi(\eta) = -\alpha(\eta) \quad \forall \eta \in N.$$

Instead, we look for a bijection $\Phi : N \to N$ such that

(i) Φ is an antihomomorphism of $(N, +)$,

(ii) Φ is an automorphism of $(N, \circ)$.

Then (i) is equivalent to

$$\text{there exists } \alpha \in \mathrm{Aut}(N, +) \text{ with } \Phi(\eta) = -\alpha(\eta) \quad \forall \eta \in N.$$

We know α must be conjugation by

$$\left(\begin{array}{c|c} A & w \\ \hline 0 & 1 \end{array}\right)$$

for some A with $AMA^{-1} = M^j$ where $\gcd(j, q) = 1$, and some $w \in V$.

Instead, we look for a bijection $\Phi : N \to N$ such that

(i) Φ is an antihomomorphism of $(N, +)$,

(ii) Φ is an automorphism of $(N, \circ)$.

Then (i) is equivalent to

$$\text{there exists } \alpha \in \mathrm{Aut}(N, +) \text{ with } \Phi(\eta) = -\alpha(\eta) \quad \forall \eta \in N.$$

We know α must be conjugation by

$$\left(\begin{array}{c|c} A & w \\ \hline 0 & 1 \end{array}\right)$$

for some A with $AMA^{-1} = M^j$ where $\gcd(j, q) = 1$, and some $w \in V$.

By making the bijection $\eta \mapsto g_\eta$ explicit, we can check (via a messy calculation) that no choice of A, w makes Φ an automorphism of $(N, \circ)$.

Instead, we look for a bijection $\Phi : N \to N$ such that

(i) Φ is an antihomomorphism of $(N, +)$,

(ii) Φ is an automorphism of $(N, \circ)$.

Then (i) is equivalent to

$$\text{there exists } \alpha \in \mathrm{Aut}(N, +) \text{ with } \Phi(\eta) = -\alpha(\eta) \quad \forall \eta \in N.$$

We know α must be conjugation by

$$\left(\begin{array}{c|c} A & w \\ \hline 0 & 1 \end{array}\right)$$

for some A with $AMA^{-1} = M^j$ where $\gcd(j, q) = 1$, and some $w \in V$.

By making the bijection $\eta \mapsto g_\eta$ explicit, we can check (via a messy calculation) that no choice of A, w makes Φ an automorphism of $(N, \circ)$.

Hence the simple skew brace we have constructed is not isomorphic to its opposite skew brace.

§5 Some Open Questions:

- For the groups N and G we have constructed, are there only two simple skew braces B (up to isomorphism) with $(B,+) \cong N$ and $(B,\circ) \cong G$?
- For primes p, q with q dividing $(p^p - 1)/(p-1)$, are there only two simple skew braces B (up to isomorphism) with $|B| = p^p q$?