The study of braces and the Yang-Baxter equation

Dennis Acreman, Sophie Bleau,
Alicia Taggart

Year 4 Project
School of Mathematics
University of Edinburgh
17th March 2023

Abstract

In this paper, we will discuss set theoretic solutions to the Yang-Baxter Equation. This equation states that for a set X and a function $r : X \times X \to X \times X$, we have

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

We will discuss the knot and braid theoretic applications to the Yang-Baxter equation.

We will find that Jacobson radical rings provide set theoretic solutions to the Yang-Baxter equation. Our following discussions will uncover the relation between these and braces.

Our focus at the final chapter of the report will be devoted to the attempt to classify braces of different kinds.

Declaration

I declare that this thesis was composed by myself and that the work contained therein is my own, except where explicitly stated otherwise in the text.

(*Dennis Acreman, Sophie Bleau,*
Alicia Taggart)

To the rational approximation support group,
who have been there for me 22/7.

Contents

Abstract **ii**

Contents **v**

1 Set theoretic solutions to the Yang-Baxter equation **3**

1.1 Knot and braid theory . . . 3

1.2 The Yang-Baxter switch . . . 7

1.3 Types of set-theoretic solutions . . . 10

1.3.1 Examples of set theoretic solutions to the Yang-Baxter equation . . . 10

2 Jacobson radical rings **13**

2.1 Definitions . . . 13

2.2 The structure group . . . 17

3 Brace yourself **20**

3.1 Definitions . . . 20

3.1.1 Category theoretic description . . . 26

3.2 The holomorph of a group . . . 26

3.3 How do braces relate to the Yang-Baxter equation? . . . 28

4 Classifying braces **31**

4.1 Braces of certain order . . . 31

4.1.1 Skew braces of cardinality n for $(n, \phi(n)) = 1$ . . . 31

4.1.2 Skew braces of cardinality pq . . . 32

4.1.3 Braces of prime order . . . 33

4.2 Finding dihedral braces . . . 35

4.2.1 Braces with adjoint group D_p . . . 38

4.2.2 Braces with adjoint group D_{p^i} . . . 46

4.2.3 Braces with adjoint group D_n (n odd) . . . 52

Introduction

> Algebra is like French Pastry: wonderful, but cannot be learned without putting one's hands to the dough.
>
> *Pierre Grillet*

Chen-Ning Yang (also known as Frank), whilst studying the system with delta function repulsive potential, and Rodney James Baxter, whilst studying an 8-vertex model in statistical mechanics, came together to analyse solutions to an equation that would become the motivation for the study of braces; the Yang-Baxter equation. The equation also has applications to quasi-triangular Hopf algebra, quantum computation, differential geometry, cryptography and quadratic algebras.

We will establish the link between this equation and brace theory, which will be the main focus of the paper. We will also state results classifying braces of different forms, including specifications on their cardinality and the structure of the adjoint group. In this way, we hope to put a smile on your face - without the orthodontic suffering one would usually associate with braces.

The diagrams in this report are our own.

Notation

Symbol/expression	Meaning
m, n, i, j, k	integer indices
p, q	primes
na	multiplication of some a by an integer index n
$\ast, \star$	both used for ring multiplication
$(R, +, \ast)$	a ring
$(A, \cdot, \circ)$	a skew brace
$(B, +, \circ)$	a brace with abelian additive group
$(0, +, \circ)$	the zero brace
$(B_1 \circledast B_2, +, \circ)$	the product brace of $(B_1, +, \circ)$ and $(B_2, +, \circ)$
$a^{\star(-1)}$	the inverse of a under operation $\star$
$a^{\star(n)}$	some operation $\star$ applied to some element a some n times

Here, $\circ$ will have order of dominance over integer multiplication, which will in turn have order of dominance over $\ast$ and $\star$, which will have order of dominance over $\cdot$ and $+$.

Chapter 1

Set theoretic solutions to the Yang-Baxter equation

In the study of brace theory, we first wish to motivate why one would come up with such a thing as a brace. Indeed, the brace is the long sought after solution to a problem: is there a set X and a function $r : X \times X \to X \times X$ such that

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r) \tag{1.1}$$

is satisfied? Well, yes there is, and as promised the answer is all about braces. Equation (1.1) is the Yang-Baxter equation, and in this section we will show its implications in knot theory and show some examples of set theoretic solutions.

1.1 Knot and braid theory

We begin by giving an impression of how the rules work in knot and braid theory.

Definition 1.1. (Section 3.1, [30]) A **link diagram** with n components is the image of a smooth map

$$\underbrace{S^1 \sqcup \cdots \sqcup S^1}_{n} \to \mathbb{R}^2$$

such that at each crossing point of two loops - S^1 - the intersecting branches are distinguished by which one passes over the other.

Remark 1.2. *Ambient isotopy* in knot theory and braid theory is loosely described as a continuous distortion of a knot, which bends or stretches the 'rope' without breaking it. For the knot theory that follows, we consider equivalence up to ambient isotopy.

Definition 1.3 (Section 5, [13])**.** Two link diagrams are **equivalent** if there exists a finite number of Reidemeister moves taking one to the other, where we show the three Reidemeister moves below.

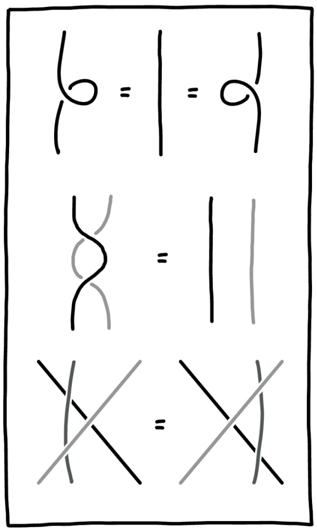

Figure 1.1: The figure shows the three Reidemeister moves.

Example 1.4. (p170, [13]) Looking at a section of a link diagram, we can analyse how the three edges can be arranged under the Reidemeister moves.

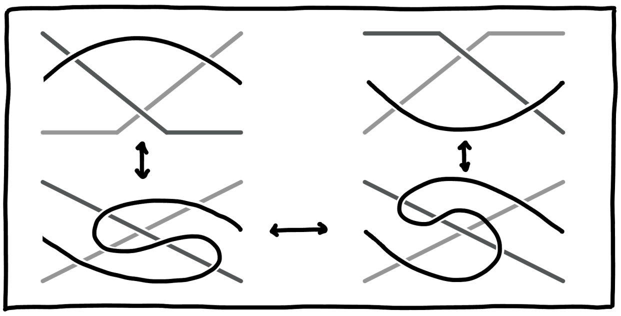

Figure 1.2: The figure shows how the Reidemeister moves can act on a section of a link diagram.

Remark 1.5. In [13], it is shown that we may choose to orientate the crossings in a link diagram by giving each circle a direction. Although oriented link diagrams are a profitable field of study, we will not apply this here.

Definition 1.6. The n-strand **braid group**, B_n, is the group of n-strand braids, whose identity is composed of n vertical strands with no intersections, and whose nontrivial elements are each given by a composition of operations σ_i for $1 \leq i \leq n$, where σ_k swaps the bottom of the kth strand over the bottom of the $k+1$th strand.

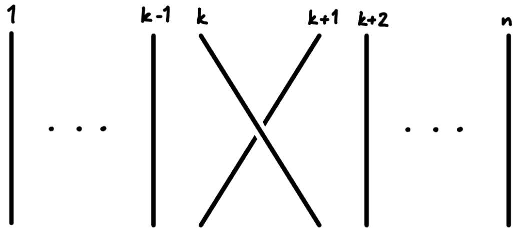

Figure 1.3: The figure shows the action of σ_k on an n-braid.

Likewise, σ_k^{-1} swaps the kth strand under the $k+1$th.

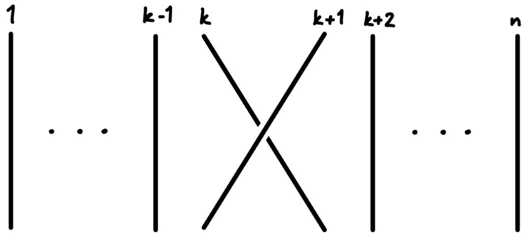

Figure 1.4: The figure shows the action of σ_k^{-1} on an n-braid.

In this way,

$$\sigma_k \sigma_k^{-1} \sim \mathrm{id} \sim \sigma_k^{-1} \sigma_k,$$

so each element of B_n is an equivalence class under $\sim$. It is useful to imagine that you are identifying the end of the strand in the ith place at the bottom with the beginning of the strand in the ith place at the top. By doing so we generate a series of loops as described in Definition 1.1.

We can compose these operations together sequentially.

Definition 1.7. A composition of σ-operations is called a **braid word**.

Notation. For an n-braid, we denote the set of n strands by $\{1, \dots, n\}$.

Definition 1.8. The **strand domain** of a braid operation is the set of strands acted on by the operation. For example, σ_i would have strand domain $\{i, i+1\}$.

Lemma 1.9. For $|k - \ell| > 1$ with $1 \leq k, \ell \leq n$ we have

$$\sigma_k \sigma_\ell = \sigma_\ell \sigma_k.$$

Proof. We know that swapping the order of disjoint operations has no effect on the composite operation. So, to prove this we need only show that the strand domains of σ_k and σ_ℓ have empty intersection. With $|k - \ell| > 1$, we know that $k + 1 < \ell$ or $\ell + 1 < k$, so

$$\{k, k+1\} \cup \{\ell, \ell + 1\} = \varnothing,$$

as required. □

Lemma 1.10. For all k with $1 \leq k \leq n$ we have

$$\sigma_k \sigma_{k+1} \sigma_k = \sigma_{k+1} \sigma_k \sigma_{k+1}$$

Proof. Examining the following diagrams, we see that the equation is a formulaic representation of the third Reidmeister move, and therefore the equation is satisfied in B_n.

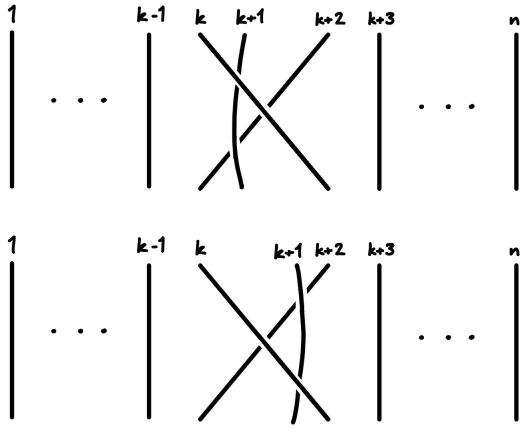

Figure 1.5: The figure shows the action of $\sigma_k \sigma_{k+1} \sigma_k$ and $\sigma_{k+1} \sigma_k \sigma_{k+1}$ on an n-braid, respectively.

□

There are several interesting results we can get to via the path of braid theory. We will not prove these here, as they require background information which might qualify as too great a digression, but here they are, to give you a hint as to the utility and span of braid theory.

Theorem 1.11. (Section 6, [14]) The braid group B_n is the fundamental group of the configuration space E^{2n} of n points on a plane. This is to say, it is the number of genera[1] in the collection of unordered n-tuples in $\Bbbk^2$, for some field $\Bbbk$.

Theorem 1.12. (Corollary 1, [14]) The braid group B_n has no elements of finite order.

These entirely nonobvious and strong statements will hopefully persuade you of the power of braid theory. We now relate the theory discussed thus far to the main focus of the paper.

Definition 1.13. (Definition 2.1, [13]) For a set X, denote by $P_n(X)$ the group of permutations of the n-fold Cartesian product, X^n. A **switch** on X is an element $r \in P_2(X)$ satisfying

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

[1] A **genus** is an equivalence class of loops in a topological space.

where the order of bracket multiplication here is right to left, such that

$$(AB)(x) = A(B(x)),$$

as is customary.

Remark 1.14. Notice that although r is a switch acting on 2 elements, the formulae $(r \times \mathrm{id}_X)(\mathrm{id}_X \times r)(r \times \mathrm{id}_X)$ and $(\mathrm{id}_X \times r)(r \times \mathrm{id}_X)(\mathrm{id}_X \times r)$ act on 3 elements, so constitute as a member of $P_3(X)$.

Lemma 1.15. (p158, [13]) A switch r on X defines a representation of B_n into the group $P_n(X)$ which sends

$$\sigma_i \mapsto r_i = (\mathrm{id}_X)^{i-1} \times r \times (\mathrm{id}_X)^{n-i-1}.$$

Proof. Omitted. (See [13]) □

Notation. We may denote $(r \times \mathrm{id}_X)$ as $r_{12} : X^3 \to X^3$ and $(\mathrm{id}_X \times r)$ as $r_{23} : X^3 \to X^3$.

Using the above notation, we obtain the fundamental relation

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}. \tag{1.2}$$

This is known famously as the **Yang-Baxter equation**.

1.2 The Yang-Baxter switch

A set theoretic solution to the Yang Baxter equation, originating in the field of statistical mechanics, is a tuple (X, r) for some set X and some function (often a matrix) $r : X \times X \to X \times X$, where on X^3 we have

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

The equivalent elements of the braid group B_3 corresponding to this equation are shown below.

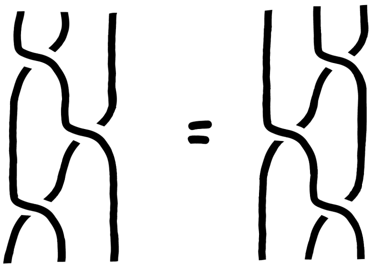

Figure 1.6: The figure shows a visual representation of the Yang Baxter equation.

Applying the r-function corresponds to swapping a pair of strands. The knot theoretic equivalent to finding set theoretic solutions to the Yang-Baxter equation is asking if the Reidemeister moves hold, since we can fix these two members of the braid group B_3 to be equivalent by the third Reidemeister move.

To get an idea of what some possible solutions can be, we define a new operation on the inputs of the switch function r.

Definition 1.16. We define the operation of **adjoint multiplication** $\circ$ as follows:

$$a \circ b := a + a * b + b. \tag{1.3}$$

Notation. We will henceforth denote

$$r(x, y) = (\lambda_x(y), \rho_y(x)) \tag{1.4}$$

as in [8], where

$$\lambda_x(y) = x \circ y - x \quad \text{and} \quad \rho_y(x) = x \circ y - y. \tag{1.5}$$

We call $\lambda_x(y)$ the **lambda function**, for use in following calculations, noticing that $\lambda_x(y) = x * y + y$ by applying the adjoint multiplication definition.

The following lemmas from [8] gives us an idea of how $\lambda_x(y)$ and $\rho_y(x)$ work, denoting the composition of functions $\lambda_a\lambda_b := \lambda_a(\lambda_b)$ which sends $x \mapsto \lambda_a(\lambda_b(x))$, and likewise for ρ.

Lemma 1.17. (Lemma 2.9, [8]) Let $(B, +)$ be an abelian group and $(B, \circ)$ be a group, possibly nonabelian, defined on the same elements. If for $a, b, c \in B$ we have **left adjoint distributivity** given by

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

then for $x, y \in B$ we have

(i) $\lambda_a(x + y) = \lambda_a(x) + \lambda_a(y)$, which is to say that λ_a is an automorphism of $(B, +)$; and

(ii) $\lambda_a\lambda_b = \lambda_{a\circ b}$, which is to say that the map $\lambda : B \to \mathrm{Sym}_B$, defined by $\lambda(a) = \lambda_a$, is a well-defined group homomorphism.

Proof. (i) For $a, x, y \in B$ we use Equation (1.5) to get

$$\begin{aligned}\lambda_a(x + y) &= a \circ (x + y) - a \\ &= a \circ x - a + a \circ y - a \\ &= \lambda_a(x) + \lambda_a(y),\end{aligned}$$

as required.

(ii) For $a, b, x \in B$ we have

$$\begin{aligned}\lambda_a\lambda_b(x) &= \lambda_a(b \circ x - b)\\ &= a \circ (b \circ x - b) - a\\ &= a \circ b \circ x - a \circ b\\ &= \lambda_{a\circ b}(x),\end{aligned}$$

as required.

□

Lemma 1.18. (Lemma 2.10, [8]) If $(B, +)$ is an abelian group and $(B, \circ)$ a group defined on the same elements where for all $a, b, c \in B$

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

then for $x, y \in B$ we have

(i) $\rho_a(x + y) = \rho_a(x) + \rho_a(y)$, which is to say that ρ is an automorphism of the abelian group $(B, +)$; and

(ii) $\rho_a\rho_b = \rho_{b\circ a}$, which is to say that the map $\rho : B \to \mathrm{Sym}_B$ defined by $\rho(a) = \rho_a$ is a group antihomomorphism, so $\rho_a\rho_b(x) = \rho_{b\circ a}(x)$.

Proof. (i) For $a, x, y \in B$ we use Equation (1.5) to get

$$\begin{aligned}\rho_a(x + y) &= (x + y) \circ a - a\\ &= x \circ a - a + y \circ a - a\\ &= \rho_a(x) + \rho_a(y),\end{aligned}$$

as required.

(ii) For $a, b, x \in B$ we have

$$\begin{aligned}\rho_a\rho_b(x) &= \rho_a(x \circ b - b)\\ &= (x \circ b - b) \circ a - a\\ &= (x \circ b) \circ a - a - b \circ a + a\\ &= x \circ (b \circ a) - (b \circ a)\\ &= \rho_{b\circ a}(x),\end{aligned}$$

as required.

□

From this we can develop the following corollary.

Corollary 1.19. (p5, [8]) For $a, b \in B$ we have

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

Proof. Omitted. (See [8]) □

We will come back to what it means for a structure like this to have these conditions.

1.3 Types of set-theoretic solutions

Definition 1.20. A set theoretic solution (X, r) to the Yang-Baxter equation is called

- **left non-degenerate** if λ_x is bijective;
- **right non-degenerate** if ρ_y is bijective;
- **non-degenerate** if it is both left and right non-degenerate;
- **involutive** if $r^2 = \mathrm{id}_{X^2}$.

1.3.1 Examples of set theoretic solutions to the Yang-Baxter equation

Example 1.21. A **twist solution** $\tau : X \times X \to X \times X$ is one in which $\tau(x, y) = (y, x)$. Indeed, for any triple $x, y, z \in X$ we have

$$\begin{aligned} \tau_{12}\tau_{23}\tau_{12}(x, y, z) &= \tau_{12}\tau_{23}(y, x, z) \\ &= \tau_{12}(y, z, x) \\ &= (z, y, x) \\ &= \tau_{23}(z, x, y) \\ &= \tau_{23}\tau_{12}(x, z, y) \\ &= \tau_{23}\tau_{12}\tau_{23}(x, y, z) \end{aligned}$$

giving the required equality $\tau_{12}\tau_{23}\tau_{12}(x, y, z) = \tau_{23}\tau_{12}\tau_{23}(x, y, z)$. This solution is particularly reminiscent of the braid pattern shown in Figure 1.6.

Example 1.22. The identity solution $i : X \times X \to X \times X$ is that where $i(x, y) = (x, y)$. Here it is clear that

$$i_{12}i_{23}i_{12}(x, y, z) = (x, y, z) = i_{23}i_{12}i_{23}(x, y, z).$$

Example 1.23. For a group G, we can have $r(g, h) = (gh, 1_G)$. Indeed for $g, h, k \in G$ we have

$$\begin{aligned} r_{12}r_{23}r_{12}(g, h, k) &= r_{12}r_{23}(gh, 1_G, k) \\ &= r_{12}(gh, k, 1_G) \\ &= (ghk, 1_G, 1_G) \\ &= r_{23}(ghk, 1_G, 1_G) \\ &= r_{23}r_{12}(g, hk, 1_G) \\ &= r_{23}r_{12}r_{23}(g, h, k) \end{aligned}$$

as required.

Example 1.24. For a set X with commutative endomorphisms f and g, **Lyubashenko solutions** define r such that

$$r(x,y) = (f(y), g(x)).$$

We find indeed that

$$\begin{aligned} r_{12}r_{23}r_{12}(x,y,z) &= r_{12}r_{23}(f(y), g(x), z) \\ &= r_{12}(f(y), f(z), g^2(y)) \\ &= (f^2(z), g(f(y)), g^2(z)) \\ &= r_{23}(f^2(z), g(x), g(y)) \\ &= r_{23}r_{12}(x, f(z), g(y)) \\ &= r_{23}r_{12}r_{23}(x,y,z) \end{aligned}$$

as required.

We use the theory from earlier in the chapter and the notation from this section to find a new way of expressing the Yang-Baxter equation.

Lemma 1.25. (p159, [13]) We can use the identity map i and the twist function τ to generate the Yang-Baxter equation. Let

$$i_k = (\mathrm{id}_X)^{k-1} \times i \times (\mathrm{id}_X)^{n-k-1} \quad \text{and} \quad \tau_k = (\mathrm{id}_X)^{k-1} \times \tau \times (\mathrm{id}_X)^{n-k-1}.$$

Setting $r_{12} = i_1\tau_1$, $r_{13} = \tau_1 i_2 \tau_2 i_1$ and $r_{23} = i_2\tau_2$, we find that the Yang-Baxter equation can also be written as

$$r_{12}r_{13}r_{23} = r_{23}r_{13}r_{12}. \tag{1.6}$$

Proof. We prove diagrammatically. To show that the equivalence

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}$$

implies the equivalence

$$r_{12}r_{13}r_{23} = r_{23}r_{13}r_{12}$$

we use the second and third Reidemeister moves, $R1$ and $R2$, respectively:

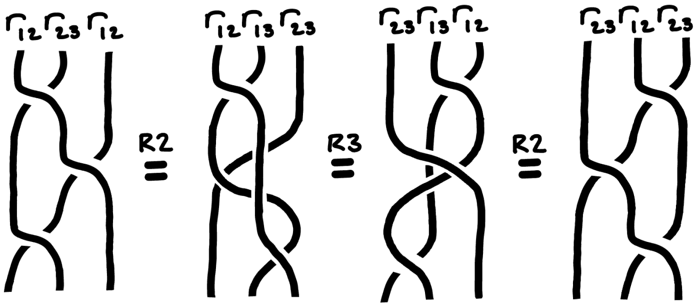

Figure 1.7: The figure shows the equivalence of the two equations via $R2$ and $R3$.

□

Lemma 1.26. Let (X, r) be a set-theoretic solution to the Yang-Baxter equation. Then (X, r) is involutive if and only if for all $x, y \in X$ we have

$$\lambda_{\lambda_x(y)}(\rho_y(x)) = x, \quad \text{and} \quad \rho_{\rho_y(x)}(\lambda_x(y)) = y. \tag{1.7}$$

Proof. We calculate

$$\begin{aligned} r^2(x, y) &= r(\lambda_x(y), \rho_y(x)) && (1.8) \\ &= (\lambda_{\lambda_x(y)}(\rho_y(x)), \rho_{\rho_y(x)}(\lambda_x(y))). && (1.9) \end{aligned}$$

Therefore $r^2(x, y) = (x, y)$ if and only if both

$$x = \lambda_{\lambda_x(y)}(\rho_y(x)) \quad \text{and} \quad y = \rho_{\rho_y(x)}(\lambda_x(y)).$$

□

In this chapter, we have examined the braid theoretic visualisations of the Yang-Baxter equations, and the methods of applying this theory to manipulating the equation. We have motivated the study of the lambda function, which will be of much use to us in Chapter 4, and given a hands on perspective as to how the lambda and rho functions from the switch function operate on elements of X. We have discussed types of solutions, and given several examples. Understanding these will allow us to proceed to the study of Jacobson radical rings.

Chapter 2

Jacobson radical rings

In this chapter, we will discuss what is required for an object to be a Jacobson radical ring, look at some examples, and prove that all nilpotent rings are Jacobson radical rings. We then establish the connection between Jacobson radical rings and braces, showing how they serve as set theoretic solutions to the Yang-Baxter equation. This leads us to look at the structure group which is defined using set theoretic solutions. Through the theory of the structure group we will define what it means for a solution to be a multipermutation solution of a certain level. We note the importance of this type of solution through the experimental observation in (p2, [16]) that more than 95% of involutive solutions with at most ten elements are multipermutation solutions.

2.1 Definitions

Before looking at Jacobson radical rings we first define the more general structure of a ring. We assume prior knowledge of basic group theory, taking the following concepts as known: groups, identity elements, commutativity, associativity, inverses, (right and left) distributivity and abelian groups.

Recall the definition of a monoid.

Definition 2.1. A **monoid** is a set M with an associative operation $*$ and an identity element e_M such that $e_M * m = m = m * e_M$ for all $m \in M$.

We use this to define a ring.

Definition 2.2. A **ring** $(R, +, *)$ is a set R equipped with two binary operations, addition $+$ and ring multiplication $*$, where

(i) $(R, +)$ is an abelian group,

(ii) $(R, *)$ is a monoid,

(iii) $*$ distributes over addition.

Remark 2.3. If $(R, *)$ is commutative then we call R a **commutative ring**, and if there exists $1_R \in R$ where for all $r \in R$ we have $1_R * r = r = r * 1_R$ we call R a **unital ring**.

Definition 2.4. For a ring $(R, +, *)$ and some $r \in R$, we define r to be **nilpotent** if and only if for some n we have

$$r^{*(n)} = \underbrace{r * \cdots * r}_{n} = 0.$$

Example 2.5. For example, in the ring $GL_2(\mathbb{Z}_2)$ of invertible matrices, if we let

$$r = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

then for $n = 2$ we have $r^{*(n)}$ is the zero matrix, so r is nilpotent in $GL_2(\mathbb{Z}_2)$.

Definition 2.6. R is a **nil ring** if and only if for every $r \in R$, there exists some $n \in \mathbb{N}$ such that $r^{*(n)} = 0$.

A stronger concept still is that of a nilpotent ring.

Definition 2.7. R is a **nilpotent ring** if for any n-tuple of R-values $(r_1, \dots, r_n)$ we have

$$r_1 * \cdots * r_n = 0.$$

Now we introduce the notion of Jacobson radical rings, which we find to be integral to our study of the set-theoretic solutions of the Yang-Baxter equations.

Definition 2.8. A ring R is a **Jacobson radical ring** if and only if for all $a \in R$ there exists some $b \in R$ such that

$$a + a * b + b = 0.$$

This is known as the *right quasiregularity condition*[1].

Remark 2.9. Note that for a Jacobson radical ring R, there is no 1_R such that $a * 1_R = a = 1_R * a$ so the ring is not unital. This is because the existence of a unit implies the existence of the additive inverse -1_R, so taking $a = -1_R$ we know there exists some $b \in R$ such that:

$$\begin{aligned} (-1_R) + (-1_R) * b + b &= 0 \\ (-1_R) - b + b &= 0 \\ -1_R &= 0 \end{aligned}$$

by the quasiregularity condition. However $-1_R = 0$ implies $1_R = 0$ in which case all elements must be 0 since for all $r \in R$ we would have $r = 1 * r = 0 * r = 0$. Hence there exists no such 1_R.

The following is a very useful and widely known result in ring theory but the proof is our own.

[1] The *left quasiregularity condition* states that for each $a \in R$ there is some $b \in R$ such that

$$b + b * a + a = 0.$$

Lemma 2.10. All nilpotent rings are Jacobson radical rings

Proof. Assume R is a nilpotent ring. Whilst not all rings contain an identity element it is common practice to embed a ring into a larger ring, $\overline{R}$, containing R and $1_{\overline{R}}$, allowing us to use the element $1_{\overline{R}}$ which we denote as 1 in this proof.

Let $a \in R$, and consider the Taylor series expansion

$$\frac{1}{1+a} = \sum_{i=0}^{\infty}(-a)^i.$$

For $a \in R$ there exists $N \in \mathbb{N}$ such that for all $n \geq N$ we have $a^n = 0$ by nilpotency, thus the sum on the right-hand side is finite. Upon rearranging we have

$$(1+a)(1-a+a^2-\dots) = 1.$$

Setting $b = (-a+a^2-\dots)$ we have

$$\begin{aligned}(1+a)(1+b) &= 1,\\ 1+a+a*b+b &= 1,\\ a+a*b+b &= 0,\end{aligned}$$

so the right quasiregularity condition required for Jacobson Radical rings is satisfied. Since neither a nor b required the existence of 1_R we know $a \in R$ and $b \in R$. Moreover, as b is a finite sum we know that for a given nilpotent ring R and some element $a \in R$, we can find $b \in R$ such that the right quasiregularity conditions holds. Hence all nilpotent rings are Jacobson Radical rings. □

Example 2.11. An example of a Jacobson radical ring is the collection of 3×3 strictly upper triangular matrices; those with empty diagonal.

Definition 2.12. As in Definition 1.16, for a ring $(R,+,*)$ with $a,b \in R$, we define the operation **adjoint multiplication**, denoted $\circ$, as follows:

$$a \circ b := a + a*b + b. \tag{2.1}$$

Corollary 2.13. For $(R,+,*)$ defined with $(\circ)$, we have

$$a\circ(b+c) = a\circ b - a + a\circ c. \tag{2.2}$$

and

$$a\circ(b-c) = a\circ b + a - a\circ c. \tag{2.3}$$

Proof. To prove (2.2) we calculate

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

and for (2.3) we calculate

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

□

Now we establish one of the key properties of adjoint multiplication in the context of Jacobson radical rings (and later, braces). Let $1_\circ$ denote the adjoint multiplicative identity and 0 denote the additive identity.

Lemma 2.14. For every brace $(B, +, \circ)$, the adjoint multiplicative identity, $1_\circ$, is equal to the additive identity, 0.

Proof. We first show that 0 suffices as the identity for the operation $\circ$. Indeed

$$a \circ 0 = a + a * 0 + 0 = a = 0 + 0 * a + a = 0 \circ a.$$

Now we show that $1_\circ$ serves as the additive identity. Let $1_\circ$ be such that $1_\circ \circ x = x = x \circ 1_\circ$ for all $x \in B$. Then

$$\begin{aligned} a + 1_\circ &= 0 \circ (a + 1_\circ) \\ &= 0 \circ a + 0 \circ 1_\circ - 0 \\ &= 0 \circ a + 0 - 0 \\ &= a \end{aligned}$$

where for the first equality we used the fact that 0 suffices as the identity for adjoint multiplication and for the third equality we used the definition of $1_\circ$ as the identity for adjoint multiplication. Hence $1_\circ$ is the identity for addition. Therefore the additive identity is equal to the adjoint multiplicative identity, giving $1_\circ = 0$ in $(B, +, \circ)$. □

Remark 2.15. As $0 = 1_\circ$, we will henceforth use 0 to refer to both the additive and adjoint multiplicative identities, unless specified otherwise.

Theorem 2.16. A ring $(R, +, *)$ is a Jacobson radical ring if and only if $(R, \circ)$ is a group.

Proof. Proving the backwards direction, we observe that if $(R, \circ)$ is a group then every element in $r \in R$ has a unique inverse s in $(\circ)$ such that

$$r \circ s = r + r * s + s = 0,$$

so $(R, +, *)$ is a Jacobson radical ring. To prove the forwards direction, assume that for all $r \in R$ there exists some $s \in R$ such that $r + r * s + s = 0$. Firstly, as in Lemma 2.14, 0 is the unique identity of the operation $\circ$. Then for $a, b, c \in R$ we calculate

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

so $\circ$ is associative in R. Finally, for all $a \in R$ there exists some $b \in R$ such that $a \circ b = a + a * b + b = 0$ since $(R, +, *)$ is a Jacobson radical ring, so there exists an inverse for every element in $(R, \circ)$. To prove this inverse is unique, assume there exists some $c \in R$ with $c \neq b$ such that $a \circ c = 0$. Then by 2.3, since $a \circ b = 0$ and $a \circ c = 0$, we have

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

so $b - c$ is the adjoint multiplicative identity, which is also the additive identity $(b - c = 0)$. Therefore $b = c$, and the inverse is unique. □

In order to connect this back to set theoretic solutions of the Yang-Baxter equation we establish the following.

Theorem 2.17. Let $(R, +, *)$ be a Jacobson radical ring and r its Yang-Baxter map. Then (R, r) are set theoretic solutions to the Yang Baxter equation.

This follows from a result in the next section, stemming from the fact that all Jacobson radical rings define a brace and that a brace (equipped with its Yang-Baxter map) is a non-degenerate involutive solution to the Yang-Baxter equation.

2.2 The structure group

Having established a class of objects that provide set-theoretic solutions to the Yang-Baxter equation, we now discuss the theory of structure groups, which focus on endowing set theoretic solutions with more structure. Moreover we provide an insight into properties of the structure group and in particular define multipermutation solutions of level m which are a particularly common type of involutive solution.

Definition 2.18. (Definition 2.1, [12]) Let (X, r) be a set theoretic solution of the Yang-Baxter equation. Then the **structure group** of (X, r), denoted $G(X, r)$, is given by

$$G(X, r) := \langle X : x \circ y = \lambda_x(y) \circ \rho_y(x) \text{ for all } x, y \in X \rangle_\circ.$$

Remark 2.19. In general the map $\iota : X \to G(X, r)$ is not injective. When ι is injective we call (X, r) an **injective solution**.

We consider an example.

Example 2.20. (p8, [12]) Consider the trivial pair (X, S), so $S(x, y) = (y, x)$. Then $G(X, r)$ is the free abelian group $\mathbb{Z}^X$ generated by X.

Recall the definition of a solvable group.

Definition 2.21. (Definition 8.1.2, [24]) A group G is **solvable** if it has a series of subgroups

$$e = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$$

such that each factor G_{i+1}/G_i is abelian.

For example, all abelian groups and all finite p-groups[2] are solvable. We now state the following theorem.

Theorem 2.22. (p2, [16]) If (X, r) is finite, involutive and non-degenerate, then the group $G(X, r)$ is solvable.

Proof. Omitted. (See Theorem 2.14, [12]) □

Definition 2.23. (p3, [26]) A solution (X, r) is a **multipermutation solution of level** m if applying the r-function m times gives a solution of cardinality 1, and m is the minimal such integer.

There are many interesting results discussing the implications of a multipermutation level being finite or otherwise. Right nilpotency was introduced by Rump to study multipermutation solutions for skew braces of abelian type, as shown in [22]. In [16] we observe the following.

Theorem 2.24. (p2, [16]) A solution (X, r) is a multipermutation solution if and only if $G(X, r)$ is right nilpotent.

Proof. Omitted. (See Theorem 2.20, [9] and Theorem 4.13, [10]) □

To generate a monoid from a group, we can simply forget about the inverses in the group. With this information, we can define a structure monoid by relaxing the requirement of inverses in its generation.

[2] We define a p-group as a group of cardinality p^k for some prime p and integer k.

Definition 2.25. Given a set-theoretic solution (X,r) of the Yang-Baxter equation, the **structure monoid** is

$$M = M(X,r) = \langle X : x \circ y = \lambda_x(y) \circ \rho_y(x) \text{ for all } x,y \in X\rangle_\circ.$$

This definition, while similar to that of the structure group, has no requirement of inverses. Indeed, we see that X is embedded in $M(X,r)$.

Note that it is not true in general that two set-theoretic solutions (X,r) and (Y,s) are isomorphic if the structure monoids $M(X,r)$ and $M(Y,s)$ are isomorphic. This is illustrated by the following example.

Example 2.26. (Example 1.1, [17]) Let $X = \{x_1, x_2, x_3\}$. Define permutations $\sigma_1 = (2,3), \sigma_2 = (1,3), \sigma_3 = (1,2)$ and consider the maps $r,s : X \times X \to X \times X$ given by

$$r(x_i, x_j) = (x_j, x_{\sigma_j(i)}) \text{ and } s(x_i, x_j) = (x_{\sigma_i(j)}, x_i).$$

Note that for distinct $i,j,k \in \{1,2,3\}$, we have $\sigma_j(i) = k$, and $\sigma_i(i) = i$. We calculate

$$\begin{aligned} r^3(x_i,x_j) &= r^2(x_j, x_{\sigma_j(i)}) = r^2(x_j, x_k) \\ &= r(x_k, x_{\sigma_k(j)}) = r(x_k, x_i) \\ &= (x_i, x_{\sigma_i(k)}) = (x_i, x_j). \end{aligned}$$

Thus $r^3 = \text{id}$, and similarly $s^3 = \text{id}$, so both (X,r) and (X,s) are bijective non-degenerate solutions to the Yang-Baxter equation. Also $M(X,r) = M(X,s)$. However, the solutions (X,r) and (X,s) are not isomorphic. To see this, suppose $f : (X,r) \to (X,s)$ was an isomorphism of solutions. Then $f \circ \sigma_x = f$ for all $x \in X$, leading to $\sigma_x = \text{id}$, a contradiction.

In this chapter we have encountered a class of objects in Jacobson radical rings and shown they include the more familiar class of objects, nilpotent rings. Furthermore, we've seen that Jacobson radical rings provide us with non-degenerate involutive solutions to the Yang-Baxter equation, and thus we have an entire well-known class of rings that provide solutions to the Yang-Baxter equation. Moreover, using such set theoretic solutions we can generate their structure groups/monoids, whose properties we have described. Specifically, we have introduced the notion of a multipermutation solution which categorises a large proportion of these set theoretic solutions. The theory discussed in this chapter concerning the structure group/monoid along with the use of algebraic tools help us study non-degenerate solutions. We use this theory in Chapter 4.

Chapter 3

Brace yourself

In this chapter we will introduce the theory of braces. We will first discuss skew braces - those with nonabelian additive group - defining the necessary requirements for brace structure. We will give an analogous definition of the lambda function defined in Equation (1.5) in terms of skew braces, and use it to find results on biskew braces and opposite skew braces.

We will then define braces with abelian additive group, and explain their relation to Jacobson radical rings. We will reconstruct the definition of ring multiplication as we know it, which we will use to prove later results. The relationship between two-sided braces and Jacobson radical rings will be discussed, as well as some category theoretic applications of brace theory. We will also show the origin of the definition of the lambda function via the concept of a holomorph, and give an explicit relationship between braces and set-theoretic solutions to the Yang-Baxter equation.

3.1 Definitions

Definition 3.1. A **skew left brace**, denoted $(A, \cdot, \circ)$, is a ring $(A, \cdot, \star)$ satisfying the following constraints.

- $(A, \cdot)$ is a group with identity $0 \in A$ and inverse elements $x^{\cdot(-1)}$ for each $x \in A$,
- $(A, \circ)$ is a group with identity $0 \in A$, and
- for $x, y, z \in A$,
$$x \circ (y \cdot z) = x \circ y \cdot x^{\cdot(-1)} \cdot x \circ z, \tag{3.1}$$
which we call left adjoint distributivity.

Remark 3.2. This last constraint takes us out of the realm of rings and into new territory. Though it may be unfamiliar to the reader, may we remind you that if you liked it then you should have put a ring on it.

We call $(A, \cdot)$ the **additive group** and $(A, \circ)$ the **adjoint group**[1] of the skew left brace. The group $(A, \circ)$ acts on the group $(A, \cdot)$ by automorphisms.

Remark 3.3. Skew right braces are defined similarly but

$$(x \cdot y) \circ z = x \circ z \cdot z^{\cdot(-1)} \cdot y \circ z \tag{3.2}$$

holds instead of Equation (3.1).

Definition 3.4. A **two-sided** skew brace has both left and right adjoint distributivity. This is to say that it is both a skew left brace and a skew right brace.

Although two-sided skew braces are more general, most of our dealings will be will skew left braces. So henceforth, where unspecified, the term 'skew brace' will refer to a skew left brace.

Example 3.5. The **trivial skew brace** has $a \cdot b = a \circ b$. That is to say $(A, \cdot) = (A, \circ)$. In this case, $(A, \circ)$ acts on $(A, \cdot)$ with the identity automorphism. We denote the adjoint group of the trivial skew brace by $\mathrm{Triv}(A, \circ)$.

Recall the definition of a lambda function in Equation (1.5). In any skew brace, we define

$$\lambda_a(b) \coloneqq a \circ b \cdot a^{\cdot(-1)}. \tag{3.3}$$

Definition 3.6. We say that a skew brace $(A, \cdot, \circ)$ is **biskew** if $(A, \circ, \cdot)$ is also a skew brace, and denote by $\lambda_{\leftrightarrow(a)} \coloneqq \lambda_a^{-1}$ the lambda function associated with $(A, \circ, \cdot)$.

Example 3.7. The trivial skew brace is biskew by observation.

Lemma 3.8. (Lemma 3.5, [28]) For a biskew brace $(A, \cdot, \circ)$, $\ker(\lambda)$ is an ideal of $(A, \cdot, \circ)$.

Proof. Instead of a trivial skew brace, let $\mathrm{Triv}(A, \circ)_{\mathrm{op}}$ have the operation $a \cdot b = b \circ a$. Then $\lambda : A \to \mathrm{Triv}(\mathrm{Aut}(A, \cdot), \circ)_{op}$ is a well-defined skew brace homomorphism, and therefore the kernel of λ satisfies the constraints of an ideal. □

Theorem 3.9. (Theorem 2.6, [28]) For a biskew brace $(A, \cdot, \circ)$, $\lambda : (A, \cdot) \to \mathrm{Aut}(A, \cdot)$ is a group antihomomorphism.

Proof. Omitted. (See [28]) □

Definition 3.10. We say that $(A, \cdot, \circ)$ is λ-homomorphic if λ is a group homomorphism.

[1] In literature, the adjoint group is often referred to as the 'multiplicative group of braces'.

Theorem 3.11. (Example 9.2, [8]) For an abelian group $(A, \circ)$, if we define $a \cdot b := a \circ b$ for $a, b \in A$, we must have

$$(b \cdot c) \circ a \cdot a = b \circ a \cdot c \circ a$$

for $a, b, c \in A$. Then $(A, \cdot, \circ)$ is a two-sided skew brace, and $\lambda_a = \mathrm{id}_A$ for all $a \in A$.

Proof. Omitted. (See [8]) □

In Lemma 3.8 we hinted at how we might define oppositeness in a brace. Thus, we now formally introduce the idea of opposite groups and opposite braces, to further analyse the mathematics surrounding skew braces.

Definition 3.12. For a group $(G, \cdot)$, we may define an operation $\square : G \times G \to G$ where for all $g, h \in G$ we have $g \square h := h \cdot g$. Then the group $(G, \square)$ is the **opposite group** of $(G, \cdot)$, denoted $(G, \cdot)^{op}$.

The concept of opposite groups is frequently exploited in the study of skew braces, as shown in the following mathematical discussion.

Lemma 3.13. (Prop 3.1 [19]) For a skew brace $(A, \cdot, \circ)$, and $(A, \square)$ defined in definition 3.12, we have that

$$(A, \square, \circ)$$

is a skew brace.

Proof. Omitted. (See [19]) □

Indeed, this skew brace we have generated has a name.

Definition 3.14. (Definition 2.4, [8]) The skew brace generated by taking the opposite group of the additive group is called the **opposite skew brace**.

Lemma 3.15. (Definition 2.4, [8]) If $(A, \cdot, \circ)$ is a skew left brace, then the opposite skew brace $(A, \square, \circ)$ is a skew right brace, and vice versa. In essence, there is a bijective correspondence between skew left braces and skew right braces.

Proof. Omitted. (See [8]) □

We now examine ideals of skew braces.

Definition 3.16. An **ideal** of a ring $(R, +, *)$ is a subset $I \subseteq R$ such that

- I contains the additive identity;
- I is closed under addition;
- for all $i \in I$, we have $-i \in I$; and
- I is closed under left and right multiplication with elements of R, so that $ir, ri \in I$.

In particular, I is a normal subgroup of $(R, +)$.

With this in mind, an ideal of a skew brace $(A, \cdot, \circ)$ is a subset $I \subseteq A$ such that $(A/I, \cdot, \circ)$ is well-defined. Upon closer inspection, we find that this implies that an ideal of a skew brace $(A, \cdot, \circ)$ is necessarily a subgroup of $(A, \cdot)$ and $(A, \circ)$.

Example 3.17. The ideals of a two-sided skew brace $(A, +, \circ)$ are precisely the ideals of the Jacobson radical ring $(A, +, *)$.

Example 3.18. The ideals of opposite braces $(A, \cdot, \circ)$ and $(A, \square, \circ)$ are the normal subgroups of $(A, \circ)$.

Example 3.19. Denote by A^2 the subgroup of A consisting of elements of the form given below:

$$A^2 := \{a * b : a, b \in A\}.$$

Here we find that A^2 is an ideal of A. Furthermore, A/A^2 is a trivial skew brace.

Remark 3.20. A skew brace does not require the additive group of the brace to be abelian.

The idea of a skew brace is a useful notion, but here we broach the usefulness of commutativity within a brace, introducing the notion of left braces. These are integral in the theory of Jacobson Radical rings and set theoretic solutions to the Yang-Baxter equation.

Definition 3.21. A **left brace**, denoted $(B, +, \circ)$, is a skew left brace with abelian additive group. We will denote abelian addition by $+$ and the inverse operation by $-$. Thus our requirements become

- $(B, +)$ is an abelian group,
- $(B, \circ)$ is a group, and
- $\circ$ has left adjoint distributivity, such that for $x, y, z \in B$,

$$x \circ (y + z) = x \circ y - x + x \circ z. \tag{3.4}$$

A right brace is defined much the same except that right adjoint distributivity given by

$$(x + y) \circ z = x \circ z - z + y \circ z$$

replaces left adjoint distributivity.

Remark 3.22. Notice that left braces satisfy the results given in Lemma 1.17, and right braces those in Lemma 1.18. Indeed, braces are a construction formulated to suit these requirements.

We will refer to left braces as braces from here on. In this project we call braces with abelian additive group **abelian braces** where there is ambiguity in order to distinguish them from skew braces.

Example 3.23. If $(R, +, *)$ is a Jacobson radical ring, necessarily $(R, +, \circ)$ is a brace with $\circ$ defined in Equation (1.16).

Proof. We know $(R,+)$ is an abelian group by the definition of a ring, and $(R,\circ)$ is a group by Theorem 2.16. So to show that $(R,+,\circ)$ is a brace, we show left adjoint distributivity: for $x,y,z \in R$

$$\begin{aligned} x\circ(y+z) &= x + x\ast(y+z) + (y+z) \\ &= x + x\ast y + x\ast z + x - x + y + z \\ &= (x + x\ast y + y) - x + (x + x\ast z + z) \\ &= x\circ y - x + x\circ z, \end{aligned}$$

as required. □

Note how for a ring $(R,+,\ast)$ we defined the notion of adjoint multiplication in Definition 2.12:

$$x\circ y := x + x\ast y + y. \tag{3.5}$$

Similarly, we can define ring multiplication inside a brace as follows.

Definition 3.24. Let $(B,+,\circ)$ be a brace. The **ring multiplication**, $\star$, of $x,y \in (B,+,\circ)$ is given by

$$x\star y := -x + x\circ y - y.$$

In this way, ring multiplication serves as a measure of the difference of $a\circ b$ and $a+b$, using the fact that $a\star b = 0$ if and only if $a+b = a\circ b$.

We give the following identity for the operation of ring multiplication that we have defined in terms of $\circ$ to showcase that it behaves like the ring multiplication we know.

Lemma 3.25. Let $\star$ be the ring multiplication of some left brace $(B,+,\circ)$. Then for $x,y,z \in B$

$$x\star(y+z) = x\star y + x\star z.$$

Proof. To prove the identity, we show that

$$\begin{aligned} x\star(y+z) &= x\circ(y+z) - x - y - z \\ &= x\circ y + x\circ z - 2x - y - z \\ &= -x + x\circ y - y - x + x\circ z - z \\ &= x\star y + x\star z, \end{aligned}$$

as required. □

Corollary 3.26. It follows from this lemma that

$$n(x\star y) = x\star(ny),$$

where n acts via the operation of integer multiplication.

Similarly to the skew brace example, we define two-sidedness for braces with abelian additive group.

Definition 3.27. A **two-sided brace** is a brace $(B, +, \circ)$ with both left and right adjoint distributivity: for all $x, y, z \in B$

$$x \circ (y + z) = x \circ y - x + x \circ z \quad \text{and} \quad (x + y) \circ z = x \circ z - z + y \circ z.$$

Lemma 3.28. If a brace $(B, +, \circ)$ has an abelian adjoint group $(B, \circ)$ then the brace is trivially two-sided, and $(B, +, \circ)$ is a nilpotent ring.

Proof. Two-sidedness follows from the fact that

$$x \circ (y + z) = (y + z) \circ x,$$

and $(B, +, \circ)$ is a ring since $(B, +)$ and $(B, \circ)$ are both abelian groups. To prove nilpotency, we let $|B| = n$ and find that for any n-tuple of elements in $(b_1, b_2, \ldots, b_i, \ldots, b_n)$, where $b_1^{\circ(-1)} = b_i$, the product

$$\begin{aligned} b_1 \circ b_2 \circ \cdots \circ b_i \circ \cdots \circ b_n &= b_1 \circ b_i \circ b_2 \circ \cdots \circ b_n \\ &= 0 \circ b_2 \circ \cdots \circ b_n \\ &= 0. \end{aligned}$$

□

Lemma 3.29. For a brace $(B, +, \circ)$ with prime cardinality, say p, both the additive group and adjoint group must be abelian, and $(B, \circ, *)$ is a ring.

Proof. Since $(B, +)$ and $(B, \circ)$ are groups with prime order, they must be cyclic and therefore abelian. We have, for $x, y \in B$,

$$x * y = -x + x \circ y - y = -y + y \circ x - x = y * x,$$

so this forces $*$ too to be abelian, giving us that $(B, \circ, *)$ is indeed a ring. $(B, +, \circ)$ is nilpotent by Lemma 3.28, and $*$ is nilpotent since $(B, *)$ is a group and so we can use a similar argument to the proof of nilpotency in Lemma 3.28. □

From Example 3.23, we see that Jacobson radical rings define braces. A natural question to ask is whether any brace can define a Jacobson radical ring, and if not, which braces have this ability. Example 3.17 gave us a clue, and we confirm our suspicions in the following lemma.

Lemma 3.30. (Example 3.1.3, [6]) For a Jacobson radical ring $(R, +, *)$ we can define a two-sided brace $(R, +, \circ)$ with $a \circ b = a + a * b + b$ for any $a, b \in R$. Conversely, for a two-sided brace $(B, +, \circ)$ we can define a Jacobson radical ring $(B, +, \star)$ with $a \star b = -a + a \circ b - b$. Indeed, we find that two-sided braces are equivalent to Jacobson radical rings, and left braces are a **generalisation** of Jacobson radical rings.

Proof. Omitted. (See [6]) □

Definition 3.31. For two left braces G, H, a map $f : G \to H$ is a **homomorphism of left braces** if for all $a, b \in G$ it satisfies

$$f(a+b) = f(a) + f(b) \quad \text{and} \quad f(a \circ b) = f(a) \circ f(b).$$

Note that the definition implies that zero is preserved, and therefore the adjoint multiplicative identity is also preserved (as $0 = 1$ by Lemma 2.14).

Remark 3.32. A homomorphism of right braces satisfies the same conditions but has right braces as its domain and codomain.

Lemma 3.33. (p5, [8]) Let f be a homomorphism of right braces. If $y \in \mathrm{Ker}(f)$ then $\rho_x(y) \in \mathrm{Ker}(f)$ for all $x \in G$.

Proof. Omitted. (See [8]) □

3.1.1 Category theoretic description

We may consider the class of braces to form a category, **Bra**, where morphisms between braces are defined as additive group homomorphisms respecting multiplication. There exist functors $F_+, F_\circ : \mathbf{Bra} \to \mathbf{Grp}$ with

$$F_+((B, +, \circ)) = (B, +) \quad \text{and} \quad F_\circ((B, +, \circ)) = (B, \circ).$$

Theorem 3.34. (p672, [23]) For brace B_1, B_2, the image of a morphism $f : B_1 \to B_2$ is a **subbrace** of B_2. This is to say $\mathrm{Im}(f) \subseteq B_2$ is an additive subgroup which is itself a brace.

Proof. Omitted. (See [23]) □

A fun proposition we will not prove is given below, showing the intersection between category theory and brace theory.

Proposition 3.35. Let G be a group with operation $+$. Then the collection of braces with $(G, +)$ as its additive group is a full subcategory of **Bra**.

The area of categorical study of braces is ripe with opportunities for further exploration, but we will not delve much deeper in this project. Instead, we strive to explore something that will be invaluable to our classifications of braces: the semi-direct product.

3.2 The holomorph of a group

The **semidirect product** of two groups can mean different things depending on context.

Definition 3.36. If $(G, \cdot)$ is a group with $N \lhd G$ and $H \leq G$ such that $N \cap H = \{\mathrm{id}_G\}$ and $G = N \times H$ (meaning that every element g of G can be expressed as $g = nh$ for $n \in N$ and $h \in H$), then G is the **inner semidirect product** of N and H, denoted

$$G := N \rtimes H = H \ltimes N.$$

Definition 3.37. For an inner semidirect product G of H on N, we define the **conjugation homomorphism** of G by

$$\sigma : H \to \operatorname{Aut}(N).$$

which takes h to an automorphism σ_h sending $\sigma_h(n) = h \cdot n \cdot h^{-1}$.

Now we ask a question posed in [21]. For some group $\mathcal{N}$, is it possible to generate a group $\mathcal{G}$ such that $\mathcal{N} \lhd \mathcal{G}$ and $\operatorname{Aut}(\mathcal{N})$ can be extended to $\operatorname{Aut}(\mathcal{G})$? Indeed, this is something called a **holomorph**. The holomorph $\mathcal{G}$ consists of elements

$$\mathcal{G} := \{n \in \mathcal{N},\ \phi \in \operatorname{Aut}(\mathcal{N})\}$$

with composition defined by

$$(n_1, \phi_1)(n_2, \phi_2) = (n_1 \phi_1^{-1}(n_2), \phi_1 \phi_2).$$

This defines the other concept of semidirect product, which we call the **outer semidirect product**. In this way,

$$\mathcal{N} \cong \{(g, h) \in \mathcal{G} : h = \mathrm{id}_{\operatorname{Aut}(\mathcal{N})}\} \quad \text{and} \quad \operatorname{Aut}(\mathcal{N}) \cong \{(g, h) \in \mathcal{G} : g = \mathrm{id}_{\mathcal{N}}\}.$$

Furthermore, by the above observations, for $n \in \mathcal{N}$ and $\phi \in \operatorname{Aut}(\mathcal{N})$ we have

$$(\mathrm{id}_{\mathcal{N}}, \phi^{-1})(n, \mathrm{id}_{\operatorname{Aut}(\mathcal{N})})(\mathrm{id}_{\mathcal{N}}, \phi) = (\phi(n), \mathrm{id}_{\operatorname{Aut}(\mathcal{N})}),$$

so $\mathcal{N}$ is normal in $\mathcal{G}$ and the automorphism group of $\mathcal{N}$ is indeed a restriction of that of $\mathcal{G}$, satisfying the constraints of our conjecture. Therefore, apart from the method of construction, the two types of semidirect product are the same, and we may write

$$\mathcal{G} = \mathcal{N} \rtimes \operatorname{Aut}(\mathcal{N}).$$

Remark 3.38. For a skew brace $(A, \cdot, \circ)$, we define the **crossed group** of $(A, \cdot, \circ)$ to be the outer semidirect product

$$\mathcal{A} = (A, \cdot) \rtimes (A, \circ)$$

Example 3.39. The dihedral group D_n is an outer semidirect product of its subgroups;

$$D_n \cong C_n \rtimes C_2.$$

Let us give a formal definition of the operations of a brace composed in this way, using the theory of semidirect products.

Definition 3.40. (Definition 2, [25]) Let $(N, +, \circ)$, $(H, +, \circ)$ be left braces and $\sigma : (H, \circ) \to \operatorname{Aut}(N, +)$ be a homomorphism (satisfying conditions in Definition 3.31) from the adjoint group of $(H, +, \circ)$ to the automorphism group of $(N, +, \circ)$, similarly to the formulation in Definition 3.36. Then the brace $N \rtimes H$, for $n_1, n_2 \in N$ and $h_1, h_2 \in H$ has $+$ defined as

$$(n_1, h_1) + (n_2, h_2) = (n_1 + n_2, h_1 + h_2),$$

and $\circ$ defined as

$$(n_1, h_1) \circ (n_2, h_2) = (n_1 \circ \sigma_{h_1}(n_2), h_1 \circ h_2).$$

Remark 3.41. Notice that this definition of $\circ$ agrees with our earlier definition of the conjugation homomorphism with multiplication in $*$; for $g_1 = n_1 * h_1$ and $g = n_2 * h_2$ we have

$$\begin{aligned} g_1 * g_2 &= n_1 * h_1 * n_2 * h_2 \\ &= n_1 * h_1 * n_2 * h_1^{-1} * h_1 * h_2 \\ &= n_1 * \sigma_{h_1}(n_2) * h_1 * h_2. \end{aligned}$$

Definition 3.42. (Section 2.1, [20]) For a group $(G, \cdot)$ with $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, we denote $g^{\cdot(\alpha)} := \alpha(g)$. Then the **holomorph** of G is given by

$$\mathrm{Hol}(G) := G \rtimes \mathrm{Aut}(G) = \{[h, \alpha] : h \in N, \alpha \in \mathrm{Aut}(N)\}. \tag{3.6}$$

Remark 3.43. Composition of automorphisms $\alpha, \beta \in \mathrm{Aut}(G)$ on some element $g \in G$ is denoted

$$\begin{aligned} (g^{\cdot(\alpha)})^{\beta} &= \beta(g^{\cdot(\alpha)}) \\ &= \beta\alpha(g) \\ &= g^{\cdot(\beta\alpha)}. \end{aligned}$$

Multiplication of elements $[g, \alpha]$ and $[h, \beta]$ in the holomorph is given by

$$[g, \alpha][h, \beta] := [g \cdot h^{\cdot(\alpha)}, \alpha\beta]. \tag{3.7}$$

We define the action of $[g, \alpha] \in \mathrm{Hol}(G)$ on $h \in G$ as

$$[g, \alpha] \cdot h := gh^{\alpha},$$

which lies in G.

We apply the holomorph to braces, taking N to be the additive group $(B, +)$ and H to be the multiplicative group $(B, \circ)$, where

$$\sigma_h(g) = \lambda_h(g) = h * g + g = h \circ g - h,$$

which gives us an explicit origin for the expression of the lambda function as an automorphism of groups in the brace. (See Chapter 2 of [4] for more details)

3.3 How do braces relate to the Yang-Baxter equation?

We claim that braces have an explicit correspondence to solutions of the Yang-Baxter equation.

Theorem 3.44. (Theorem 1.2, [11]) For a brace $(B, +, \circ)$, and a map $r : B \times B \to B \times B$ defined by

$$r(x, y) = (\lambda_x(y), \rho_y(x))$$

where $\lambda_x(y) = x \circ y - x$ and $\rho_y(x) = t \circ x - t$ for $t := \lambda_x(y)^{-1}$, then (B, r) is an involutive, non-degenerate solution of the Yang-Baxter equation.

Proof. Omitted. (See [11]) □

Definition 3.45. Let $(B, +, \circ)$ be a brace and $x, y \in B$. The **Yang-Baxter map** associated to B is the map $r : X \times X \to X \times X$ given by $r(x, y) = (\lambda_x(y), \rho_y(x))$ as defined in Theorem 3.44.

An explicit connection between braces and set theoretic solutions to the Yang-Baxter equation is shown in (p4, [19]) and (Theorem 3.1, [15]). For some skew left brace $(A, \cdot, \circ)$, let our r-function be given by

$$\begin{aligned} r_A(x, y) &= (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x \circ y)^{\cdot(-1)} \cdot x \cdot (x \circ y)) \\ &= (x^{\cdot(-1)} \cdot (x \circ y), (x^{\cdot(-1)} \cdot (x \circ y))^{\cdot(-1)} \circ x \circ y). \end{aligned}$$

By Theorem 1, [15], this is a non-degenerate solution of the Yang-Baxter equation, and r_A is involutive if and only if $a \cdot b = b \cdot a$ for all $a, b \in A$, so that $(A, \cdot)$ is abelian. We can now consider further the case of abelian additive group when classifying braces.

Lemma 3.46. (Lemma 4.1, [8]) For a left brace $(B, +, \circ)$, with $a, b \in B$, we have

- $a \circ \lambda_a^{-1}(b) = b \circ \lambda_b^{-1}(a)$;
- $\lambda_a \lambda_{\lambda_a^{-1}(b)} = \lambda_b \lambda_{\lambda_b^{-1}(a)}$; and
- the map $r(x, y) := (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x))$ is a non-degenerate set theoretic solution to the Yang Baxter equation. Furthermore, r is involutive.

Proof. Omitted. (See [8]) □

Through our coverage of the theory of braces, we have seen how skew braces operate and contribute to the plethora of study surrounding brace theory. Using the lambda function defined in Equation (3.3) for skew braces we found that $\ker(\lambda)$ is an ideal of the skew brace $(A, \cdot, \circ)$, and that λ is a group antihomomorphism for biskew braces, including the case for which λ acts as the identity homomorphism of a skew brace. Furthermore we have stated the correspondence between left and right skew braces using the theory of opposite skew braces. We concluded the theory of skew braces with some results on the ideal of a skew brace.

Having defined braces with abelian additive group, we have explained their relation to Jacobson radical rings, and found that

$$n(x * y) = x * ny$$

using what we know of adjoint and ring multiplication. Defining a two-sided brace, we found that they and Jacobson radical rings have a one-to-one correspondence as shown in [6]. After briefly discussing the category of braces and its implications in category theory, we defined the holomorph of a group and stated that the holomorph with $N := (B, +)$ and $H := (B, \circ)$ gives a brace. Finally, we showed that a skew left brace with lambda function is a set theoretic solution to the Yang-Baxter equation when paired with the switch function

$$r_A(x, y) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x \circ y)^{-1} \cdot x \cdot (x \circ y)).$$

Chapter 4

Classifying braces

We now attempt, using results from our own research and those from research in previous papers, to build braces of different types, with restrictions such as having a certain cardinality or a certain adjoint group. In each of these cases, we find the necessary constraints on how the elements of the brace interact with each other. To aid with this, we will use methods such as defining the lambda function of the brace, finding the socle of the brace, and finding Sylow subgroups of $(B, +)$ and $(B, \circ)$, among other methods. At the end of this chapter, we specialise to the case of braces with dihedral adjoint group.

To discuss braces of different cardinalities, we first introduce the group theoretical building blocks: Sylow subgroups. In the interest of brevity, let us state, without proof, the three Sylow theorems as stated in Theorems 4.1.2-4, [24]. Let G be a group of order n with some prime $p \,|\, n$, and write $n = p^m r$ with $p \nmid r$.

Theorem 4.1. (Sylow I) There exists at least one subgroup of order p^m. We call such a subgroup a **Sylow p-subgroup**.

Theorem 4.2. (Sylow II) Let P be a Sylow p-subgroup, and H a subgroup of G of order p^k for some $k \leq n$. Then there exists x with

$$H \subseteq xPx^{-1}.$$

This is to say that if H is a Sylow p-subgroup, then P and H are conjugate.

Theorem 4.3. (Sylow III) If there are n_p Sylow p-subgroups of G then

$$n_p \,|\, r \quad \text{and} \quad n_p \cong 1 \mod p.$$

4.1 Braces of certain order

4.1.1 Skew braces of cardinality n for $(n, \phi(n)) = 1$

Theorem 4.4. (Theorem A.8, [27]) Let $n \in \mathbb{N}$. There is a unique skew brace of cardinality n if and only if n and $\phi(n)$ are coprime, where ϕ denotes Euler's totient function.

The proof of this fact is rooted in Hopf-Galois theory, so we will not include a formal one, but instead an informal sketch of it. While a skew brace correlates to some number of Hopf-Galois extensions, a Hopf-Galois extension can only give one skew brace, implying that there are many more Hopf-Galois extensions than there are skew braces. Then, since we know that there is exactly one Hopf-Galois extension with Galois group of cardinality n for $(n, \phi(n)) = 1$, there can only be one skew brace.

4.1.2 Skew braces of cardinality pq

For primes p, q where $p > q$ and $p \ncong 1 \mod q$, the only skew brace of cardinality pq is the trivial brace using Theorem 4.4, noticing that $\phi(pq) = (p-1)(q-1)$ which is coprime to pq. So let's consider the converse of this case in search of a more interesting outcome.

Theorem 4.5. (p2, [1]) For primes p, q where $p \cong 1 \mod q$, there are $2q+2$ possible structures of skew brace with order pq up to isomorphism. In this case, for some element $g \in \mathbb{Z}_p$ with multiplicative order q, we have the following skew braces:

- For $(A, \cdot) \cong \mathbb{Z}_p \times \mathbb{Z}_q$ such that $\begin{pmatrix} n \\ m \end{pmatrix} \cdot \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} n \cdot s \\ m \cdot t \end{pmatrix}$, we may have
  - $(A, \cdot, \circ)$ is the trivial skew brace over $\mathbb{Z}_p \times \mathbb{Z}_q$ with $\begin{pmatrix} n \\ m \end{pmatrix} \circ \begin{pmatrix} s \\ t \end{pmatrix} := \begin{pmatrix} n \\ m \end{pmatrix} \cdot \begin{pmatrix} s \\ t \end{pmatrix}$; or
  - $(A, \cdot, \circ)$ is biskew with $\begin{pmatrix} n \\ m \end{pmatrix} \circ \begin{pmatrix} s \\ t \end{pmatrix} := \begin{pmatrix} n \cdot g^m s \\ m \cdot t \end{pmatrix}$.
- For $(A, \cdot) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$ such that $\begin{pmatrix} n \\ m \end{pmatrix} \cdot \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} n \cdot g^m s \\ m \cdot t \end{pmatrix}$ we may have
  - $(A, \cdot, \circ)$ is the trivial skew brace over $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ with $\begin{pmatrix} n \\ m \end{pmatrix} \circ \begin{pmatrix} s \\ t \end{pmatrix} := \begin{pmatrix} n \\ m \end{pmatrix} \cdot \begin{pmatrix} s \\ t \end{pmatrix}$;
  - $(A, \cdot, \circ)$ is skew with $\begin{pmatrix} n \\ m \end{pmatrix} \circ \begin{pmatrix} s \\ t \end{pmatrix} := \begin{pmatrix} g^t n \cdot g^m s \\ m \cdot t \end{pmatrix}$;
  - $A_\gamma = (A, \cdot, \circ)$ is biskew where $1 < \gamma \leq q$ and $\begin{pmatrix} n \\ m \end{pmatrix} \circ \begin{pmatrix} s \\ t \end{pmatrix} := \begin{pmatrix} n \cdot (g^\gamma)^m s \\ m \cdot t \end{pmatrix}$;
  - $A_\mu = (A, \cdot, \circ)$ is a skew brace where $1 < \mu \leq q$ and $\begin{pmatrix} n \\ m \end{pmatrix} \circ \begin{pmatrix} s \\ t \end{pmatrix} := \begin{pmatrix} g^t n \cdot (g^\mu)^m s \\ m \cdot t \end{pmatrix}$.

Proof. Omitted. (See [1]) □

4.1.3 Braces of prime order

Skew braces of prime order

Definition 4.6. (p3, [4]) A **regular subgroup** of a holomorph $\mathrm{Hol}(B)$ is a subgroup $H \leq \mathrm{Hol}(B)$ where for any $b \in B$ we have a unique $(c, \sigma) \in H$ as the adjoint multiplicative inverse to b, meaning that

$$(c, \sigma) \circ b = b + \sigma(c) = 0.$$

Corollary 4.7. (Prop. 2.3 [4]) Let $(B, +)$ be an abelian group. Let pr_1 be projection of a pair onto the first element, $\mathrm{pr}_1(c, \sigma) = c$, pr_2 be a projection onto the second element, $\mathrm{pr}_2(c, \sigma) = \sigma$, and $\tau : B \to \mathrm{Aut}(B)$, with $\tau(b) = \mathrm{pr}_2(\mathrm{pr}_1^{-1}(b))$.

- For a left brace $(B, +, \circ)$, with additive group $(B, +)$,

  $$\{(b, \lambda_b) : b \in B\}$$

  is a regular subgroup of the holomorph $\mathrm{Hol}(B)$. We also have the converse; if H is a regular subgroup of $\mathrm{Hol}(B)$, then $\mathrm{pr}_1(H) = B$. Furthermore, we can define the adjoint product by

  $$a \circ b := a + \tau(a)(b),$$

  with which $(B, +, \circ)$ defines a left brace such that $(B, \circ) \cong H$.

- We can thus define a bijection between left braces with $(B, +)$ as their additive group and regular subgroups of $\mathrm{Hol}(B)$.

Proof. Omitted. (See [4]) □

Theorem 4.8. (Example A.7, [27]) There are n skew braces of order p^n up to isomorphism.

Proof. For a skew brace $(A, \cdot, \circ)$ of order p^n, if the holomorph $\mathrm{Hol}(A)$ has an element of order p^n then $(A, \circ)$ must be cyclic. This implies that all skew braces of this form have $(A, \circ) \cong \mathbb{Z}_{p^n}$ and also $(A, \cdot) \cong \mathbb{Z}_{p^n}$. Then for some generator $a \in A$, the automorphism group is populated with automorphisms α_i which send $a \mapsto a^i$, for each i coprime to p.

Let H be a regular subgroup of $\mathrm{Hol}(A)$. Then for each i, H must have a unique element of the form (a, α_i) that generates H since $(A, \circ)$ is cyclic. We also know that $i \cong 1 \mod p$ since $\alpha_i(a) = a^i$ has maximal order so as to generate $\mathbb{Z}_{p^n}$. This implies that there exist p^{n-1} possibilities for i, and therefore p^{n-1} distinct regular subgroups.

So how many skew braces does this give us? Following closely the method in (Ex A.7, [27]), we consider the orbit of H under conjugacy of automorphisms. Given $H = \langle (a, \alpha_i) \rangle$, then the composition $\alpha_j H \alpha_j^{-1}$ is generated by (a^j, α_i), meaning that there exists some k such that (a, α_k) also generates $\alpha_j H \alpha_j^{-1}$. All that we require is that both $i - 1 \,|\, p^m$

and $k - 1 \mid p^m$ for the same such m. Therefore we have n skew braces, each determined by its generator:

$$i = 1, \quad i = 1 + p, \quad \dots, \quad i = 1 + p^{n-1}.$$

□

Abelian braces of prime order

Definition 4.9. (p673 & p681, [23]) We define a brace $(B, +, \circ)$ to be **cyclic** if $(B, +)$ is cyclic. We define $(B, +, \circ)$ to be a **primary cyclic brace** if $|B| = p^n$ for some prime p and $n \in \mathbb{N}$.

Theorem 4.10. (p55, [6]) If $(B, +, \circ)$ is a primary cyclic brace with $p > 2$ then the adjoint group has the isomorphism $(B, \circ) \cong \mathbb{Z}_{p^n}$, and so $(B, +, \circ)$ is two-sided. There are exactly n brace structures on $(B, +, \circ)$ up to isomorphism, where the ith brace structure is defined by the adjoint multiplication

$$a \circ b = a + b + p^i (a * b). \tag{4.1}$$

Proof. Omitted. (See [23]) □

Braces of order 2^m

Definition 4.11. The **index** of a subgroup H of some group G is the number of left cosets of H in G.

For Theorem 4.10, we cover the cases of primary cyclic braces for all primes except 2. Now we follow a proposition from [23] to cover this case too.

Theorem 4.12. (Proposition 11, [23]) Let G be a group of order 2^n with a cyclic subgroup of index 2. Then G fall into one of the following cases.

1. G is cyclic;
2. G is abelian and non-cyclic for $n \geq 2$ with
$$G \cong C_2 \times C_{2^{n-1}};$$
3. G is dihedral for $n \geq 3$ with
$$G \cong \langle g, h : g^{2^{n-1}} = h^2 = 1,\ gh = hg^{-1} \rangle;$$
4. G is a generalized quaternion[1] for $n \geq 3$ with
$$G \cong \langle g, h : g^{2^{n-1}} = 1, h^2 = g^{2^{n-1}}, gh = hg^{-1} \rangle;$$

[1] A **quaternion** $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ exists in a four-dimensional noncommutative extension of the complex plane, where $i^2 = j^2 = k^2 = ijk = -1$.

5. for $n \geq 4$
$$G \cong \langle g, h : g^{2^{n-1}} = 1, h^2 = 1, hgh^{-1} = g^{-1+2^{n-1}} \rangle;$$

6. for $n \geq 4$
$$G \cong \langle g, h : g^{2^{n-1}} = 1, h^2 = 1, hgh^{-1} = g^{1+2^{n-1}} \rangle.$$

Proof. Omitted. (See [23]) □

Later we will discuss in detail the constraints to obtain a brace with an adjoint group of dihedral structure. Here we state a relevant result for a brace with $(B, +) \cong \mathbb{Z}_{2^m}$.

Braces of order p^2

To classify braces of order p^2, we turn to [3].

Theorem 4.13. (Proposition 2.4, [3]) Let $|B| = p^2$ with $x_1, x_2, y_1, y_2 \in B$ and $p > 2$. Then there are four possible brace structures on $(B, +, \circ)$ up to isomorphism.

For additive group isomorphic to $\mathbb{Z}_{p^2}$, we either have

1. $x_1 \circ x_2 := x_1 + x_2$, so $(B, +, \circ)$ is the trivial brace with $(B, \circ) \cong \mathbb{Z}_{p^2}$; or
2. $x_1 \circ x_2 := x_1 + x_2 + px_1 * x_2$, so either
   - $p = 2$, in which case $(B, \circ) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$; or
   - $p > 2$, giving $(B, \circ) \cong \mathbb{Z}_{p^2}$.

Then for the case where the additive group is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, we either have

1. $(x_1, y_1) \circ (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$, so $(B, +, \circ)$ is the trivial brace with $(B, \circ) \cong \mathbb{Z}_p \times \mathbb{Z}_p$; or
2. $(x_1, y_1) \circ (x_2, y_2) := (x_1 + x_2 + y_1 * y_2, y_1 + y_2)$, so either
   - $p = 2$, in which case $(B, \circ) \cong \mathbb{Z}_4$; or
   - $p > 2$, giving $(B, \circ) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. Omitted. (See [3]) □

4.2 Finding dihedral braces

We can find interesting results by choosing groups and assigning their structure to the adjoint group of a brace. We show an example, assigning the structure of the Dihedral group of order 6 to the adjoint group. We then generalise to dihedral braces of prime order, prime power order and odd order.

The following example was the result of collaboration with Scott Warrander during project discussions, and uses ideas from a previous project (See Example 4.1.7, [18]).

Example 4.14. (D_3) We seek a brace satisfying the following properties:

- the adjoint group $(B, \circ)$ is isomorphic to the dihedral group D_3, given by
$$D_3 = \langle g, h : g^{\circ(3)} = h^{\circ(2)} = e, h \circ g = g^{\circ(-1)} \circ h\rangle_\circ, \quad \text{and} \tag{4.2}$$
- the additive group $(B, +)$ is isomorphic to the cyclic group $\mathbb{Z}_6$, given by $\mathbb{Z}_6 = \langle x : x^{+(6)} = 0\rangle_+$.

To find a brace $(B, +, \circ)$ of cardinality 6, the abelian group $(B, +)$ must be the cyclic group $\mathbb{Z}_6$ and the adjoint group $(B, \circ)$ can either be D_3 or $\mathbb{Z}_6$. Taking $(B, \circ) = \mathbb{Z}_6$, we find that the adjoint group is cyclic, so is not dihedral. So consider a different construction. Define $\lambda_a : B \to B$ to be the map

$$b \mapsto a \circ b - a.$$

The action $a \to \lambda_a$ is a group homomorphism taking $(B, \circ) \to \mathrm{Aut}(B, +)$, where, since the only elements of order 6 are 1 and 5, the only possible automorphisms are

- that which sends the generator to $1 \in \mathbb{Z}_6$ $(x \mapsto x)$, and
- that which sends the generator to $-1 \in \mathbb{Z}_6$ $(x \mapsto 5x)$.

The square of the second map is clearly the identity, so the automorphisms of $(B, \circ)$ are isomorphic to $\mathbb{Z}_2$, which we will write $\mathbb{Z}_2 = \langle -1\rangle_*$. To define λ_a we need to find a way to map $D_3 \to \mathbb{Z}_2$. There is the trivial map, sending everything to 1, but to attempt to find a surjective map we observe that if ϕ is our homomorphism then $|D_3| = |\ker(\phi)||\mathrm{im}(\phi)| = 6$, giving us that the kernel of our homomorphism must be a normal subgroup of D_3 with 3 elements. The only homomorphism that suffices here is the sign map $x \mapsto (-1)^x$, sending an element of even order to 1 and an element of odd order to -1, as used in (Example 3.1.3(c),[6]). So we have

$$\mathrm{Hom}(D_3, \mathbb{Z}_2) = \{1, (-1)^x\}$$

where 1 is the trivial map sending everything to $1 \in \mathbb{Z}_2$. Taking the trivial map yields $a \circ b = a + b$ for all $a, b \in B$, so the group $(B, \circ)$ is abelian, and therefore cannot be isomorphic to the dihedral group.

So take $\lambda_a = (-1)^a$. By our definition of λ_a, we have that

$$a \circ b = a + (-1)^a b.$$

We now assign values to elements of $(B, \circ)$ and $(B, +)$ to see how they interact. Notice first that if $(-1)^a = 1$ then $a \circ b = a + b$, giving an abelian subgroup. The group D_3 has exactly one non-trivial normal subgroup, and it is the rotational subgroup $\langle g\rangle_\circ \cong \mathbb{Z}_3$. This subgroup will therefore be isomorphic to the abelian group $\mathbb{Z}_3 = \{0, 2, 4\} < \mathbb{Z}_6$.

We send the identity element $e \in D_3$ to 0 and arbitrarily assign the remaining elements of $\mathbb{Z}_3$ as follows:

$$\phi(e) = 0, \quad \phi(g) = 2, \quad \phi(g^{\circ(2)}) = 4.$$

We remark that, up to isomorphism, assigning $\phi(g) = 4$ and $\phi(g^{\circ(2)}) = 2$ will make no difference to the brace obtained.

Now we compose our other elements to see where they place in the group homomorphism. For instance, given that $\{h, g \circ h, g^{\circ(2)} \circ h\}$ all have order two, we can arbitrarily assign $\phi(h) = 1$. Using the fact that $a \circ b = a + b$ when $(-1)^a = 1$, we have that

$$2 + 1 = \phi(g) \circ \phi(h) = \phi(g \circ h) = 3, \quad \text{and} \quad 4 + 1 = \phi(g^{\circ(2)}) \circ \phi(h) = \phi(g^{\circ(2)} \circ h) = 5.$$

Hence, we have the group homomorphism ϕ with

$e \mapsto 0$	$g \mapsto 2$	$g^{\circ(2)} \mapsto 4$
$h \mapsto 1$	$g \circ h \mapsto 3$	$g^{\circ(2)} \circ h \mapsto 5$

Then $(B, +) \cong \mathbb{Z}_6$ and $(B, \circ) \cong D_3$, as we wished to show. □

Remark 4.15. Neither left nor right distributivity of adjoint multiplication over addition of the elements of D_3 as defined in the above example is satisfied in the traditional sense. This is to say that we do not have

$$a \circ (b + c) = a \circ b + a \circ c \quad \text{or} \quad (a + b) \circ c = a \circ c + b \circ c.$$

In fact we expect this outcome due to the left adjoint distributivity condition, particularly that $a \circ (b + c)$ and $a \circ b + a \circ c$ differ by a. To exemplify the failure of left distributivity, we define the operation $(+_\phi)$ by $a \,(+_\phi)\, b := \phi^{-1}(\phi(a) + \phi(b))$ and find

$$\begin{aligned} h \circ (h \,(+_\phi)\, h) &= h \circ \phi^{-1}(1 + 1) \\ &= h \circ \phi^{-1}(2) \\ &= h \circ g \\ &= g^{\circ(2)} \circ h, \end{aligned}$$

and

$$\begin{aligned} h \circ h \,(+_\phi)\, h \circ h &= e \,(+_\phi)\, e \\ &= \phi^{-1}(0 + 0) \\ &= \phi^{-1}(0) \\ &= e, \end{aligned}$$

so $h \circ (h \,(+_\phi)\, h) \neq h \circ h \,(+_\phi)\, h \circ h$, and therefore $(B, +, \circ)$ does not qualify as a ring. We can use a similar example to show failure of right ring distributivity of $\circ$ over $+$.

Now let us try to generalise this result. We can examine what happens when our adjoint group is the dihedral group of order

- $2p$, for p prime;
- $2p^i$, for p prime and $i \in \mathbb{N}$; and
- $2n$, for n odd.

4.2.1 Braces with adjoint group D_p

Similarly to D_3, let us set the abelian group $(B,+)$ to have structure $\mathbb{Z}_{2p}$ for prime $p > 3$, and let the lambda function be

$$\lambda_a(b) = (-1)^a b$$

as in the D_3 case, for $a, b \in B$. Then

$$a \circ b = a + (-1)^a b.$$

Does this suffice to define a brace? We know that the additive group is abelian, and since $a + b$ defines the composition of group elements a and b, we can check associativity and identity of $(\circ)$:

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

where the fourth equality holds by considering a even, in which case $a + b = a + (-1)^a b$, and then considering a odd:

- for a, b both odd, we have

  $$(-1)^{a+b} = 1 = (-1)^{a+(-1)^a b},$$

  and

- for a odd and b even, we have

  $$(-1)^{a+b} = -1 = (-1)^{a+(-1)^a b}.$$

This satisfies the requirement of associativity. Furthermore, 0 acts as the identity, which gives us that $(B, \circ)$ is a group. Finally we check that Equation (3.4) is satisfied:

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

Then we may conclude that $(B, +, \circ)$ is a left brace. However, by the logic in Example 4.14, $(B, +, \circ)$ is not a Jacobson radical ring. It follows that the adjoint group is the dihedral group D_p. Indeed, this agrees with the result of Example 3.1.3(c) in [6].

Remark 4.16. For D_3 we noticed that the subgroup of rotational elements was the only nontrivial normal subgroup of D_3, and this extends to D_p where p is prime. However, the automorphism group inside $\mathbb{Z}_{2p}$ consists of more than just 2 elements, so there may be more than two homomorphisms.

Theorem 4.17. (Theorem 1, [26]) A brace $(B, +, \circ)$ is left nilpotent if and only if its adjoint group $(B, \circ)$ is nilpotent.

Proof. Omitted. (See [26]) □

We now define a piece of notation.

Notation. For braces $(B_1, +, \circ)$ and $(B_2, +, \circ)$, we can define their sum to be

$$(B_1 + B_2, +) = (B_1, +) + (B_2, +),$$

which is to say that every element of $(B_1 + B_2, +)$ is a sum of elements in $(B_1, +)$ and $(B_2, +)$.

Theorem 4.18. (Theorem 1, [26]) If $(B, +, \circ)$ has cardinality $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ for distinct primes p_i and natural indices $\alpha_i \in \mathbb{N}$, then

$$(B, +) = (B_1, +) + (B_2, +) + \dots + (B_k, +)$$

where each $(B_i, +)$ is a subgroup of $(B, +)$ of cardinality $p_i^{\alpha_i}$, and each $(B_i, +, \circ)$ is a subbrace.

Proof. Omitted. (See [26]) □

Lemma 4.19. For all $g \in (B_p, +, \circ)$, we have $g * g = 0$.

Proof. Suppose that $g * g = \alpha g$ for some $\alpha \in \mathbb{N}$. Then $g^{*(m)} = \alpha^{m-1} g$ for all $m \in \mathbb{N}$. By the nilpotency of finite braces, $(B_p, +, *)$ is a nilpotent ring of cardinality p, so there exists m such that

$$\underbrace{g * \dots * g}_{k} = 0,$$

so $\alpha^{k-1} g = 0$. Furthermore, since the order of $(B_p, +, \circ)$ is p, g has order p under the operation of $*$, so $p \,|\, \alpha^{k-1}$. As p is prime, this means that $p \,|\, \alpha$, and therefore $\alpha \cong 0 \mod p$ in $(B_p, +, \circ)$. So $g * g = 0$, as required. □

Definition 4.20. For braces $(B_1, +, \circ), (B_2, +, \circ)$ we define their **product brace**, denoted $(B_1 \circledast B_2, +, \circ)$, as follows:

$$(B_1 \circledast B_2, +, \circ) := (\langle a * b : a \in B_1, b \in B_2 \rangle_+, +, \circ)\,. \qquad (4.3)$$

This is to say that $(B_1, +, \circ), (B_2, +, \circ)$ are subbraces of $B_1 \circledast B_2$.

Notation. We write $B^{n+1} = B \circledast B^n$ for a brace raised to the $n+1$th power by left multiplication, and $B^{(n+1)} = B^{(n)} \circledast B$ for a brace raised to the $n+1$th power by right multiplication.

We now define nilpotency for braces.

Definition 4.21. We define $(B, +, \circ)$ to be **left nilpotent** if $B^n = 0$ for some n. Likewise, we define $(B, +, \circ)$ to be **right nilpotent** if $B^{(n)} = 0$ for some n.

Definition 4.22. A brace $(B, +, \circ)$ is **strongly nilpotent**[2] if it is both left and right nilpotent.

We now make a claim on the nilpotency of the Sylow p-subgroup $(B_p, +, \circ)$ of the prime dihedral brace.

Lemma 4.23. The cyclic subgroup of the adjoint group of the prime dihedral brace is strongly nilpotent.

Proof. Let $(B, +, \circ)$ be a brace where $(B, \circ) \cong D_p$ for some prime p. From Lemma 4.18 we have

$$(B, +) = (B_2, +) + (B_p, +),$$

where both $(B_2, +, \circ)$ and $(B_p, +, \circ)$ are subbraces of $(B, +, \circ)$. We find that

$$(B_2, +) = \{0, h : h + h = 0, h * h = 0\}$$

by definition of the reflective subgroup of D_p, and

$$(B_p, +) = \{0, g, g + g, \ldots, (p-1)g : g * g = 0\},$$

using the definition of D_p and Lemma 4.19. This is to say that $(B_p, +, *)$ is a nilpotent ring. We now show that $(B_p, +, \circ)$ is strongly nilpotent.

Theorem 4.24. Let $(R_1, +, \circ), (R_2, +, \circ)$ be finite subrings of some $(R, +, \circ)$ with $|R_1| = i$ and $|R_2| = j$. Then $(i, j) = 1$ if and only if $R_1 \circledast R_2 = 0$.[3]

Proof. We prove the forward direction, and omit the converse proof. Assume otherwise. For $a \in R_1, b \in R_2$ we have $(ia) * b = 0$, and $a * (jb) = 0$ from the cardinalities of R_1 and R_2. Assume $a * b = \alpha$ for some $\alpha \neq 0$. By the distributivity of $*$ in rings, we also have that $ja * b = a * (jb)$ meaning that b has order j. By Bézout's identity, we have

$$1 = (i, j) = si + tj \quad \Rightarrow \quad a * b = (si + tj)(a * b) = 0$$

[2] An equivalent definition is given in Definition 2.10 of [16].

[3] We write $(s, t) = c$ when c is the greatest common divisor of s and t.

for $s, t \in \mathbb{Z}$. Then $a * b = 0$ for all $a \in R_1$, $b \in R_2$, and

$$\begin{aligned} R_1 \circledast R_2 &= \left\langle \sum_i a_i * b_i : a_i \in B_1, b_i \in B_2 \right\rangle_+ \\ &= \left\langle \sum_i 0 \right\rangle_+ \\ &= 0, \end{aligned}$$

so $R_1 \circledast R_2 = 0$. □

Remark 4.25. Note that $R_1 \circledast R_2 \subseteq R_2$. This is because $j(a * b) = a * (jb) = a * 0 = 0$ by Corollary 3.26. This implies that every element of $R_1 * R_2$ has order at most j.

Theorem 4.26. (Theorem 5, [25]) Let $(B, +, \circ)$ be a left brace with Sylow subgroups $(B_p, +)$ and $(B_q, +)$ of cardinality p^m and q^n respectively (for p, q prime). Then if p doesn't divide $q^t - 1$ for any $1 \leq t \leq m$, we have

$$B_p \circledast B_q = 0.$$

Proof. Omitted. (See [25]) □

From this, we obtain the fact that $B_p \circledast B_2 = 0$. Therefore, we have that

$$\begin{aligned} B_p \circledast B_p &= 0 \\ B_p \circledast B_2 &= 0 \\ B_2 \circledast B_2 &= 0. \end{aligned}$$

What about $B_2 \circledast B_p$? For this we take $a \in B$ of form $a = b + c$ for $b \in B_2$ and $c \in B_p$. For $d \in B_2$ we use that

$$(x + y + x * y) * z = x * z + y * z + x * (y * z),$$

and that $c * d = 0$ to show that

$$\begin{aligned} a * d &= (b + c) * d \\ &= (b + c + c * d) * d \\ &= b * d + c * d + c * (b * d) \\ &= 0, \end{aligned}$$

as $b * d \in B_2 \circledast B_2 = 0$ and $c * d \in B_p \circledast B_2 = 0$. Alternatively, for $e \in B_p$ we have $c * e = 0$ and $b * e \in B_p$, so

$$\begin{aligned} a * e &= (b + c) * e \\ & (b + c + c * e) * e \\ &= b * e + c * (b * e) \\ &= b * e \in B_p \end{aligned}$$

since $c * (b * e) \in B_p \circledast B_p = 0$. Then we take the only nontrivial product $B_2 \circledast B_p$, and conclude that since it is contained in B_p we must have

$$(B_2 \circledast B_p) \circledast (B_2 \circledast B_p) = 0.$$

This is to say that $(B_p, +, \circ)$ is strongly nilpotent. □

Notice that Theorem 4.17 implies that $(B, +, \circ)$ is not strongly nilpotent. Indeed, although $(B, +, \circ)$ is right nilpotent, left nilpotency fails. We can see this by observing that $(B_p \circledast B_2) \circledast (B_p \circledast B_2) \subseteq B_p$, so

$$(B_p \circledast B_2) \circledast ((B_p \circledast B_2) \circledast (B_p \circledast B_2)) \subseteq B_p.$$

This is to say that no matter how many times we multiply the brace by itself, the most information we can get is that the product will land in B_p.

Definition 4.27. (Definition 2.3, [28]) Let $(B, +, \circ)$ be a brace.

- A **left ideal** of B is a subgroup I of $(B, +)$ such that $\lambda_a(I) \subseteq I$ for all $a \in B$.
- An **ideal** of B is a left ideal I normal in both $(B, +)$ and $(B, \circ)$.

Remark 4.28. By the definition of $(\circ)$, we necessarily have that a left ideal I of B is a subgroup of $(B, \circ)$, giving us that $(I, +, \circ)$ is a subbrace.

Definition 4.29. (Definition 2.4, [5]) A **simple left brace** is a left brace with no ideals except the trivial ideal and the brace itself.

In this way, we use the idea of an ideal as in [28] to define the quotient of a brace.

Definition 4.30. We define the **socle** as

$$\mathrm{Soc}(B) := \{a \in B : a * b = 0 \text{ for all } b \in B\}.$$

Remark 4.31. This definition is equivalent to that given by

$$\mathrm{Soc}(B) = \{a \in B : \lambda_a = \mathrm{id}\} = \{a \in B : a \circ b = a + b \text{ for all } b \in B\}$$

as in [8], p16.

We define the socle of a skew brace similarly.

Definition 4.32. (Definition 2.4, [15]) For a skew left brace $(A, \cdot, \circ)$, the socle is given by

$$\mathrm{Soc}(A) = \{a \in A : a \circ b = a \cdot b,\, b \cdot (b \circ a) = (b \circ a) \cdot b \text{ for all } b \in A\}.$$

We state the following lemma for skew braces, so that it can be applied whether or not the additive group is abelian.

Lemma 4.33. For some skew brace $(A, \cdot, \circ)$, $\mathrm{Soc}(A)$ is a normal subgroup of the ring multiplicative group of $(A, \cdot, \circ)$.

Proof. We follow the proof from (Lemma 2.5, [15]). Firstly, to show that $\mathrm{Soc}(A)$ is a subgroup of $(A,\circ)$ we have the unit of adjoint multiplication since $1_\circ = 1_* \in \mathrm{Soc}(A)$ by Lemma 2.14 and closure under $\circ$ since $x, y \in \mathrm{Soc}(A)$ implies that

$$\begin{aligned}(x \circ y) \circ z &= x \circ (y \circ z)\\ &= x \circ (y \cdot z)\\ &= x \cdot (y \cdot z)\\ &= (x \cdot y) \cdot z\\ &= (x \circ y) \cdot z\end{aligned}$$

for all $z \in A$. Finally, we show that $a^{\circ(-1)} \in \mathrm{Soc}(A)$, since

$$\begin{aligned}a^{\circ(-1)}b &= a^{\circ(-1)}(a * a^{\circ(-1)}) \circ b \text{ since } 1_* = 1_\circ \text{ by Lemma 2.14}\\ &= a^{\circ(-1)} \circ b,\end{aligned}$$

so $\mathrm{Soc}(A) \leq (A,\circ)$. Then, using the lambda function defined as $\lambda_a : A \to A$ with $b \mapsto a^{\circ(-1)} \cdot (b \circ a)$ and using the fact that $a \in \mathrm{Soc}(A)$ implies $a \circ b = a \cdot b$ and $b \cdot (b \circ a) = (b \circ a) \cdot b$ for $b \in A$, we have

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

which gives us that $\mathrm{Soc}(A)$ is a normal subgroup of $(A,\circ)$. We get for free here that $\mathrm{Soc}(A)$ is a subgroup of $(A,\cdot)$ also. Furthermore, we may use the equation above to redefine the socle in terms of the lambda function:

$$\mathrm{Soc}(A) = \{a \in A : a \circ b = a \cdot b,\ \lambda_b(a) \circ b = b \circ a\}.$$

Then we find that for $a \in \mathrm{Soc}(A)$ and $b, c \in A$,

$$\begin{aligned}\lambda_c \lambda_b(a) \circ c &= \lambda_{c\circ b}(a) \circ c \text{ by Lemma 1.17}\\ &= (c \circ b) \circ a \circ (c \circ b)^{\circ(-1)} \circ c\\ &= c \circ \lambda_b(a) \circ c^{\circ(-1)} \circ c\\ &= c \circ \lambda_b(a),\end{aligned}$$

and

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

giving us that for any $b\in A$ we have

$$\lambda_b(\mathrm{Soc}(A))\subseteq \mathrm{Soc}(A).$$

Then, for $a\in\mathrm{Soc}(A)$, $b\in A$,

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

Left multiplication by b gives us $a\cdot b = b\cdot a$, so $\mathrm{Soc}(A)$ is in the centraliser of A, meaning that $\mathrm{Soc}(A)$ is a normal subgroup of $(A,\cdot)$. □

Corollary 4.34. The socle of a left brace $(B,+,\circ)$ is an ideal of $(B,+,\circ)$.

Proof. We shall give a proof as can be found in (Chapter 6, [8]). Let $(B,+,\circ)$ be a left brace. For $a\in B$ and $b\in\mathrm{Soc}(B)$, by Lemma 3.46 we have

$$\lambda_a\lambda_{\lambda_a^{-1}(b)} = \lambda_b\lambda_{\lambda_b^{-1}(a)} = \lambda_a,$$

giving us that $\lambda_{\lambda_a^{-1}(b)} = \mathrm{id}$, and therefore $\lambda_a^{-1}(b)\in\mathrm{Soc}(G)$, giving us that the socle is an ideal of the left brace G. □

Recall the definition of the structure group given in Definition 2.18.

Theorem 4.35. (Corollary 3.10, [15]) Let (X,r) be a finite non-degenerate solution of the Yang-Baxter equation. Then

$$G(X,r)/\mathrm{Soc}(G(X,r))$$

is a finite skew left brace.

Proof. Omitted. (See [15]) □

Lemma 4.36. (Proposition 6.2, [8]) If $(B,+,\circ)$ is a finite two-sided brace then $\mathrm{Soc}(B)\neq\{1\}$. Furthermore, the set theoretic solution to the Yang-Baxter equation associated to $(B,+,\circ)$ is a multipermutation solution.

Proof. Omitted. (See [8]) □

Theorem 4.37 (Corollary 7, [25])**.** Let B be a left brace of cardinality $p_1^{\alpha_1} \dots p_n^{\alpha_n}$ for some n, some primes $p_1 < p_2 < \dots < p_n$, and some positive integers $\alpha_1, \dots, \alpha_n$. Let B_i denote the Sylow subgroup of the additive group of A with cardinality $p_i^{\alpha_i}$. Suppose that for some $m \leq n$ the brace B_m has nonzero socle and p_m does not divide $p_j^i - 1$ for all $j \leq n$ and each $i \leq \alpha_j$. Then the socle of B is nonzero.

Proof. We use a similar proof to that in [25]. By Theorem 4.26, since p_m does not divide $p_j^i - 1$ for any $i \leq \alpha_j$, we get $(B_m \circledast B_j, +, \circ) = (0, +, \circ)$ for all $j \leq n$. Then for $b \in \mathrm{Soc}(B_n, +, \circ)$ we have $(b \circledast B_i, +, \circ) = (0, +, \circ)$ for all i, and b must be in the socle of $(B, +, \circ)$. □

Corollary 4.38. Let $(B, +, \circ)$ be the dihedral brace with adjoint group congruent to D_p for some prime p, and define $(B_2, +, \circ)$ and $(B_p, +, \circ)$ as its subbraces. The socle $\mathrm{Soc}(B_p) \subseteq \mathrm{Soc}(B)$.

Proof. We first note that $B_p \circledast B_2 = 0$ by Theorem 4.26. Every element a in the socle

$$\mathrm{Soc}(B_p) = \{a \in B_p : a * b = 0 \text{ for all } b \in B_p\}$$

has $a * c = 0$ for $c \in B_2$, so $a \in \mathrm{Soc}(B)$, giving us that $\mathrm{Soc}(B_p) \subseteq \mathrm{Soc}(B)$. □

Remark 4.39. From this, we obtain the useful result that if $(B_p, +, \circ)$ has nonzero socle then $(B, +, \circ)$ has nonzero socle.

Corollary 4.40. The brace $(B, +, \circ)$ with $(B, \circ) \cong D_p$ is right nilpotent.

Proof. We wish to show that

$$\underbrace{(((B \circledast B) \circledast B) \cdots \circledast B)}_{n} = 0 \tag{4.4}$$

for some $n \in \mathbb{N}$. Indeed, for each bracket $B \circledast B$ we can write $(B, +) = (B_2, +) \circledast (B_p, +)$, so $B \circledast B = B \circledast (B_2 + B_p)$. Furthermore, $B_2 = \langle h \rangle_* = \{1_B, h\}$ since $h * h = 0$. So for $x \in B_2$, $y \in B_p$, take

$$\begin{aligned} h * (x + y) &= h * x + h * y \\ &= h * y \end{aligned}$$

as x is either 0 or h, in both cases resulting with $h * x = 0$. □

With this terminology, we can now construct the brace with D_p as the adjoint group using an alternative method. To do so, we wish to determine the lambda function which provides us with an operation $\circ$ satisfying $(B, \circ) \cong D_p$. For this, we must have $|B| = 2p$ and $(B, +) = (B_2, +) + (B_p, +)$ for subbraces of cardinality 2 and p respectively. Let a generate $(B_2, +)$ and b generate $(B_p, +)$. We know that $0 * b = 0$, and that $a * b$ is one of

$$a * b = \begin{cases} b, \\ 2b, \\ 3b, \\ \vdots \\ (p-1)b \end{cases}$$

due to the properties of ring multiplication discussed in Remark 3.26. Let $a * b = (i-1)b$ for some $i \in \mathbb{N}$. The lambda function gives

$$\begin{aligned} \lambda_a(b) &= b + a * b = b + (i-1)b = ib \\ \lambda_a(\lambda_a(b)) &= \lambda_{a \circ a}(b) = b \text{ since } a \circ a = 0, \text{ so} \\ b &= i^2 b. \end{aligned}$$

Therefore we have $p \,|\, (i^2 - 1)$ giving us that either $p \,|\, i+1$ or $p \,|\, i-1$, or in other equations, $a * b = -2b$ or $a * b = 0$ so we have two choices of lambda functions;

$$\lambda_a(b) = -b \quad \text{or} \quad \lambda_a(b) = b.$$

Let us first consider the latter case, where $\lambda_a(b) = b$ and $a * b = 0$ for all $a, b \in B$. Here, we see that $a \circ b = a + b$, so $(B, +, \circ)$ is a trivial brace. Furthermore, the commutativity of $(+)$ forces $(\circ)$ to be abelian, so $(B, \circ)$ cannot have dihedral structure.

Then we must have $a * b = -2b$, $\lambda_a(b) = -b$. Here $(\circ)$ is defined by $a \circ b = a - b$ for generators a of $(B_2, +, \circ)$ and b of $(B_p, +, \circ)$. Indeed, this agrees with our conjecture for the lambda function and $\circ$ operation for the D_3 example, where any nonidentity element h in $(B_2, +, \circ)$ has negative sign, giving $\lambda_h(g) = -g$ for $g \in (B_p, +, \circ)$ and the identity element 0 gives $\lambda_0(g) = g$, satisfying the conjectured $\lambda_h(g) = (-1)^h g$ and $h \circ g = h + (-1)^h g$. This is to say that this lambda function agrees with the dihedral brace structure with $(B, \circ) \cong D_p$ for any prime p.

4.2.2 Braces with adjoint group D_{p^i}

Let $p > 2$ be some prime, and let $(B, +, \circ)$ be a brace with Sylow subgroups B_2 and B_{p^i} in $(B, +)$ such that

$$(B, +) = (B_2, +) + (B_{p^i}, +).$$

Here, $(B_2, +, \circ)$ and $(B_{p^i}, +, \circ)$ are subbraces. Consider a brace $(B, +, \circ)$ of order p^i for some prime p and $i \in \mathbb{N}$.

Theorem 4.41. (p680, [23]) Let $(B, +, \circ)$ be a brace of cardinality p^n with $p > 2$ prime. If either one of $(B, +)$ or $(B, \circ)$ is cyclic then both are cyclic, and we call $(B, +, \circ)$ **bicyclic**.

Proof. Omitted. (See [23]) □

Theorem 4.42. (p680, [23]) For $p > 2$ prime, every cyclic brace $(B, +, \circ)$ with $|B| = p^m$ is bicyclic.

Proof. Omitted. (See [23]) □

Remark 4.43. Notice that for a dihedral brace of order $2p^n$, there will be only one Sylow p-subgroup by Sylow's third theorem.

Lemma 4.44. For a brace $(B, +, \circ)$ whose adjoint group is isomorphic to D_{p^n} for some prime p and $n \geq 2$, $(B, \circ)$ has a cyclic subgroup of order p^n.

Proof. This is clear, since $(B, \circ)$ is isomorphic to D_{p^n}, which by definition has a cyclic group of order p^n. □

The following example was the result of collaboration with Scott Warrander during project discussions.

Example 4.45. Let us conjecture the necessary form of the dihedral group D_{p^2}, for some prime p. Here there are two nontrivial normal subgroups of the adjoint group. If g generates the subgroup $\mathbb{Z}_{p^2}$ of rotations, then both $\langle g \rangle_\circ$ and $\langle g^{\circ(p)} \rangle_\circ$ are normal subgroups. Then we must consider two possible additive groups; $\mathbb{Z}_{2p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_{2p}$. We examine first (arguably the more interesting case) the additive group to be $\mathbb{Z}_p \times \mathbb{Z}_{2p}$. In this case $\lambda : (B, \circ) \to \mathrm{Aut}(B, +)$ is given by

$$\lambda : D_{p^2} \to \mathrm{Aut}(\mathbb{Z}_{2p} \times \mathbb{Z}_p).$$

So let us examine the contents of this automorphism group. Since $\mathrm{Aut}(G \times H) = \mathrm{Aut}(G) \times \mathrm{Aut}(H)$ for G and H of coprime order, we recognise that $\mathbb{Z}_p \times \mathbb{Z}_{2p} \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_2$ and since the automorphism group of $\mathbb{Z}_2$ is trivial we have $\mathrm{Aut}(\mathbb{Z}_{2p} \times \mathbb{Z}_p) = \mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)$. Furthermore, the automorphism group of $\mathbb{Z}_p$ gives

$$\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times,$$

the invertible elements $\{1, \ldots, p-1\}$ of $\mathbb{Z}_p$. Since they are all coprime to p we can send the generator 1 to any of them and generate a valid automorphism. This is congruent also to $\mathbb{Z}_{p-1}$, given that there is a primitive root modulo p that generates the nonzero elements. Choosing where to send the two generators $(1, 0)$ and $(0, 1)$, we can send the first to any element except $(0, 0)$ (giving $p^2 - 1$ options), and then the second to any element linearly independent to the first element (giving $p^2 - p$ options). To see this from an alternative viewpoint, if the linear transformation $\mathbb{Z}_p^2 \to \mathbb{Z}_p^2$ is given as a matrix with entries in $\mathbb{Z}_p$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} a \\ c \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \to \begin{pmatrix} b \\ d \end{pmatrix},$$

for $\begin{pmatrix} a \\ c \end{pmatrix}$ and $\begin{pmatrix} b \\ d \end{pmatrix}$ linearly independent. Then our automorphism group is also congruent to the general linear group $GL_2(\mathbb{Z}_p)$.

Let $\phi : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$ be a homomorphism. Then for $\begin{pmatrix} a \\ b \end{pmatrix}$, we must have

$$\phi \begin{pmatrix} a \\ b \end{pmatrix} = \phi \left(a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = a\phi \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\phi \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Now we examine the kernel of λ. This must be a normal subgroup of D_{p^2}. So, if the rotational subgroup of D_{p^2} is generated by g, then our kernel has three options: $\ker\lambda = \{0\}$, $\ker\lambda = \langle g \rangle_\circ$, or $\ker\lambda = \langle g^{\circ(p)} \rangle_\circ$. We find the image ${}^{(D_{p^2},\circ)}/_{(e,\circ)} \cong (D_{p^2}, \circ)$ and likewise with the additive group, so we obtain the same brace. To calculate ${}^{D_{p^2}}/_{\langle g^{\circ(p)} \rangle_\circ}$, we must first verify that $\langle g^{\circ(p)} \rangle_\circ$ is an ideal in the brace. Particularly we need a few lemmas.

Lemma 4.46. (Lemma 15, [25]) Let B be a left brace and let $a, b \in B$. Then for $n \in \mathbb{N}$, we have that

$$a^{\circ(n)} = \sum_{i=1}^{n} \binom{n}{i} a^{*(i)}. \tag{4.5}$$

Proof. Omitted. (See [25]) □

Lemma 4.47. For a brace $(B, +, \circ)$ with $(B, \circ) \cong D_{p^n}$, where p is a prime and n a positive integer, let $(B_2, \circ)$ and $(B_{p^n}, +, \circ)$ denote the Sylow subgroups of $(B, \circ)$. Then we have

- $B_{p^n} \circledast B_2 \subseteq B_2$; and
- $B_2 \circledast B_{p^n} \subseteq B_{p^n}$.

Proof. These follow from the fact that for $a \in B_2, b \in B_{p^n}$, $n(a * b) = a * nb$ by Corollary 3.26, and vice versa. This is to say that $a * b$ will have the same order as b, and therefore they will both belong to the same brace. □

Now we can state the following result about ideals in the brace D_{p^2}.

Lemma 4.48. For the dihedral brace with $(B, \circ) \cong D_{p^2}$ with g the generator of the normal subgroup in $(B, \circ)$, we have that

(i) $(\langle g^{\circ(p)} \rangle_\circ, +, \circ)$ is a ring,

(ii) $\lambda_a(p\langle g \rangle_\circ) \subseteq p\langle g \rangle_\circ$ for all a in the brace.

Proof. For (i), we observe that $g * g = 0$ by Lemma 4.19, so using similar justification as that in Lemma 4.46 we find that

$$\binom{p}{i} * g^{*(i)} = \binom{b}{i} * \underbrace{g * (g * (g * \cdots * (g * g)))}_{i} = 0$$

for all $i > 1$. In fact, there exists some function $f(g)$ with no constant terms, allowing

$$\begin{aligned} g^{\circ(p)} &= \underbrace{g \circ (g \circ \cdots \circ (g \circ g))}_{p} \\ &= \underbrace{g + (g + \cdots + (g + g))}_{p} + (g * (f(g))) \\ &= pg \end{aligned}$$

since $g * f(g) = 0$ by Lemma 4.19. This gives us the result that $g^{\circ(p)} = p \cdot g^{\circ}$ in $\langle g^{\circ(p)} \rangle_{\circ}$, so $\circ$ can be expressed in terms of the commutative operation $*$, and $(\langle g^{\circ(p)} \rangle_{\circ}, \circ)$ is abelian. So $(\langle g^{\circ(p)} \rangle_{\circ}, +, \circ)$ is a ring, as required.

Now we recognise that showing $\lambda_a(\langle g^{\circ(p)} \rangle_{\circ}) \subseteq \langle g^{\circ(p)} \rangle_{\circ}$ for all $a \in D_{p^n}$ is equivalent to showing

$$\lambda_a(p\langle g \rangle_{\circ}) \subseteq p\langle g \rangle_{\circ}.$$

Indeed, our lambda function is given by

$$\lambda_a(b) = a * b + b,$$

as in Notation 1.2 which in this case gives

$$\lambda_a(p\langle g \rangle_{\circ}) = a * p\langle g \rangle_{\circ} + p\langle g \rangle_{\circ}. \tag{4.6}$$

Ring multiplication laws dictate that $a * p\langle g \rangle_{\circ} \subseteq p\langle g \rangle_{\circ}$ by Lemma 4.47, so the sum

$$\lambda_a(p\langle g \rangle_{\circ}) = a * p\langle g \rangle_{\circ} + p\langle g \rangle_{\circ} \subseteq p\langle g \rangle_{\circ},$$

as required. □

Then for the image, we conjecture that the quotient braces will have adjoint groups given by those shown in the table.

Quotient group	imλ
$D_{p^2}/\langle g \rangle_{\circ}$	$\mathbb{Z}_2$
$D_{p^2}/\langle g^{\circ(p)} \rangle_{\circ}$	D_p
$D_{p^2}/\langle e \rangle_{\circ}$	D_{p^2}

Now we move to the more general case; examining D_{p^n} for $n > 2$. Let $(B, +, \circ)$ be a brace of order $2p^n$ for some prime p and some positive integer n, where the adjoint group is the dihedral group D_{p^i}. We can express $(B, +) = (B_2, +) + (B_{p^n}, +)$ where $(B_2, +)$ is a Sylow 2-subgroup and $(B_{p^n}, +)$ a Sylow p-subgroup. By Sylow's theorems, there is only one Sylow p-subgroup, and this is normal in B. Also, since $(B_{p^n}, +)$ is closed under $\circ$ we have that $(B_{p^n}, +, \circ)$ is a brace. Therefore $(B_{p^n}, \circ)$ is a Sylow p-subgroup of B, and

$$(B_{p^n}, \circ) = (\{0, g, ..., g^{\circ(p^n - 1)}\}, \circ).$$

Braces whose multiplicative group is cyclic were classified by Rump. In particular, they are bicyclic by Theorem 4.41. In particular the rotational subgroup $(B_{p^n},+)$ is cyclic. Let B be a brace of cardinality $2p^n$ and consider the additive group $(B_{2p^n},+)$. Then B_{p^n} and B_2 under addition are Sylow p-subgroups of B_{2p^n}. Then for all $a \in B$ we have that $a = b + c$ uniquely for $b \in B_{p^n}$ and $c \in B_2$ by Theorem 4.1, thus $(B_{2p^n},+) = (B_{p^n},+) + (B_2,+)$.

With the definition of the product brace given in Equation (4.3), we obtain

$$B_{p^n} \circledast B_2 := \langle a * b : a \in B_{p^n}, b \in B_2 \rangle_+.$$

This is in itself a subbrace.

We now specialise to the D_{p^n} case. We write

$$D_{p^n} = \langle g, h : g^{\circ(p^n)} = h^{\circ(2)} = 0, g^{\circ(-1)} \circ h = h \circ g \rangle_\circ.$$

For a brace with $(B,+) = (B_2,+) + (B_{p^n},+)$, where $h \in B_2$ and g is a generator of the cyclic subgroup $(B_{p^n},\circ)$, we know that $h * h = h + h$. Furthermore we have the following lemma.

Lemma 4.49. In the dihedral brace with $(B,\circ) \cong D_{p^n}$, the generator g of the cyclic subgroup of $(B,\circ)$ has

$$g * g = mg$$

for some m divisible by p.

Proof. This follows from the fact that $(B_{p^n},+,*)$ is a nilpotent ring. □

We now make the following claim.

Proposition 4.50. Let $(B,+,\circ)$ be a brace with $(B,\circ) \cong D_{p^n}$ for some prime $p > 2$ and some positive integer n. Writing $(B,+) = (B_2,+) + (B_{p^n},+)$, where g is a generator of the cyclic subgroup $(B_{p^n},\circ)$, then $g * g = mg$ for some integer m by Lemma 4.49, and for any $t = ag + b \in B$ and $h \in (B_2,\circ)$ we have

- $t * h = 0$; and
- $t * g = (-am - 2)g$.

Proof. The proof follows a similar method to that in Section 4.2.1. By Theorem 4.26 we have $B_{p^n} \circledast B_2 = 0$. Also, for $h \in B_2$ and $g \in B_{p^n}$ we have $B_2 \circledast B_{p^n} \subseteq B_{p^n}$, so

$$h * g = \begin{cases} g \\ 2g \\ 3g \\ \vdots \\ (p^n - 1)g. \end{cases}$$

Then for $h \in B_2$ and $g \in B_{p^n}$ we must have

$$h * g = \gamma g,$$

for some $\gamma \in B_{p^n}$. Then $\lambda_h(g) = (\gamma+1)g$, and

$$g = \lambda_0(g) = \lambda_h(\lambda_h(g)) = (\gamma+1)^2 g,$$

giving us that $(\gamma+1)^2 \cong 1 \mod p^n$. This is to say that either $p^n \,|\, \gamma$ or $p^n \,|\, \gamma+2$. Assuming the former is true, we have $\lambda_h(g) = g$ and $h * g = 0$. Therefore the adjoint group of the brace is nilpotent and cannot have adjoint group D_{p^n}. So the latter must be true; $p^n \,|\, \gamma+2$. Here we must have $\gamma \cong -2 \mod p^n$. So if we let $(B_2, +) = \{0, h\}$ we have $h + h = 0$ and $h * h = 0$, and $h * g = -2g$ since $p^n \,|\, \gamma+2$. Also, as stated, $g * g = mg$ for some integer m divisible by p. Indeed this determines all relations in the brace. As $(B_{p^n}, +, *)$ is a ring,

$$ig * jg = ijmg$$

and as $B_{p^n} \circledast B_2 = 0$ we have

$$g * h = 0.$$

As in the proposition, let $t \in (B, +, \circ)$ be such that $t = ag + b$ for g the generator of $(B_{p^n}, \circ)$, a some integer less than p^n and b some element of $(B_2, +, \circ)$ (where + denotes composition). Then using the fact that

$$(x + y + x * y) * z = x * z + y * z + x * (y * z),$$

and that $ag * b = 0$, we procure

$$\begin{aligned}(ag + b) * b &= (ag + b + ag * b) * b \\ &= ag * b + b * b + ag * (b * b) \\ &= 0\end{aligned}$$

as $b * b = 0$ by definition of $(B_2, \circ)$. Therefore we can conclude that for any element t (uniquely determined by a and b for $ag + b$) we must have $t * b = 0$, implying that

$$(B, +, \circ) \circledast (B_2, +, \circ) = (0, +, \circ).$$

Then for $t * g$ we use $g * g = mg$ to find:

$$\begin{aligned}(ag + b) * g &= (ag + b + ag * b) * g \\ &= ag * g - 2g - 2ag * g \\ &= -ag * g - 2g \\ &= (-am - 2)g,\end{aligned}$$

as proposed. □

4.2.3 Braces with adjoint group D_n (n odd)

For a brace B, $\lambda_a : (B, \circ) \to \mathrm{Aut}(B, +)$, for $(B, \circ) \cong D_n$ and $(B, +) \cong \mathbb{Z}_n$, we let our adjoint multiplicative operation $\circ$ be defined as follows.

$$\begin{aligned} \circ : \mathbb{Z}_{2n} \times \mathbb{Z}_{2n} &\to \mathbb{Z}_{2n} \\ a \circ b &\mapsto a + (-1)^a b. \end{aligned}$$

Indeed we see that this binary operation is not well defined for braces with an odd number of elements, as if n is odd then $a \cong 1 \mod n$ would be odd for $a = 1$ and even for $a = n + 1$, giving two possible values for $a \circ b$.

So what else can we say about a brace with dihedral adjoint group D_n for n odd? First, we state the following lemma.

Lemma 4.51. (Lemma 33, [26]) Let $s \in \mathbb{N}$, A be a right nilpotent left brace (so that $A^{(s)} = 0$ for some s). Let $a, b \in A$. Define inductively elements $d_i = d_i(a, b)$, $d'_i = d'_i(a, b)$ as follows: $d_0 = a$, $d'_0 = b$, and for $i \geq 1$ define $d_{i+1} = d_i + d'_i$ and $d'_{i+1} = d'_i * d_i$. Then for every $c \in A$ we have

$$(a + b) * c = a * c + b * c + \sum_{i=0}^{2s} (-1)^{i+1} \cdot ((d'_i * d_i) * c - d'_i * (d_i * c)).$$

Proof. Omitted. (See [26]) □

Also, our brace is strongly nilpotent since $a * b$ defines the whole brace. All cyclic groups are nilpotent. We recall Theorem 4.18, which says that if the multiplicative group of a finite brace is nilpotent this brace is a direct product of braces.

Corollary 4.52. (Proposition 3, [23]) For $(B_n, +, \circ)$ the cyclic subbrace of the dihedral brace $(B, +, \circ)$ with $(B, \circ) \cong D_n$, we have that $(B_n, +, *)$ is a commutative radical ring, and decomposes into its primary components like so,

$$(B_n, +, \circ) = \prod_{p \text{ prime}} (B_{p^i}, +, \circ),$$

with multiplication over $\otimes$ where $(B_{p^i}, +, \circ) := \{a \in B : \; p^i a = 0\}$ and $n = \sum_p p^i$.

Proof. Omitted. (See Proposition 3, [23]) □

Write $n = p_1^{\alpha_1} \cdot p_2^{\alpha_1} \cdot \dots \cdot p_i^{\alpha_i}$. Since n odd, p_j are all odd. The number of options we have for this finite abelian group is an open problem in mathematics, but more information can be found on what we call the **partition function** in [2], [7] and [29]. If $m = 2n$ and $p : \mathbb{N} \to \mathbb{N}$ takes a number m to the number of ways m can be written as a sum of positive integers,

$$|x| < 1 : \quad \sum_{m=0}^{\infty} p(m) x^m = \prod_{m=1}^{\infty} \frac{1}{1 - x^m},$$

which gives us various results but not a conclusive number of ways in which to partition $m = 2n$ in our case of the dihedral group, so we will leave this problem to the reader.

In this chapter, we have classified skew braces of cardinality pq and skew and abelian braces of cardinality p^n, specialising to the case when $p = 2$ and that when $n = 2$, using results from ([4], [27], [23], [6], [3]). We have used the lambda function to construct a brace with adjoint group D_3 and to show it is unique up to isomorphism. From this, we have used a conjectured form for the lambda function for all D_p braces and showed that indeed the lambda function

$$\lambda_a(b) = (-1)^a b$$

satisfies the axioms to form a left brace. We showed also that the prime dihedral brace is strongly nilpotent. We defined the socle and gave some interesting results pertaining to it and previous concepts in the paper. We then used this definition to prove nontrivial facts about the subgroups of the cyclic subgroups inside dihedral braces, particularly those with $(B, \circ) \cong D_{p^2}$. We stated a conjecture about the quotient braces given by quotienting different ideals from D_{p^2}, and from here proven two further propositions dictating how elements with a brace with $(B, \circ) \cong D_{p^n}$ interact. Finally, an attempt was made to extend what was known about prime dihedral braces to dihedral braces with $(B, \circ) \cong D_n$ for n odd.

Conclusion

To conclude, through the study of braces we have discovered many nice results. We have found that all nilpotent rings are Jacobson radical rings and the set theoretic solutions to the Yang-Baxter equation coincide with braces defined under

$$r_A(x,y) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x \circ y)^{-1}x(x \circ y)).$$

Furthermore, we have found that Jacobson radical rings coincide with two-sided braces. Having defined the holomorph of a group we have obtained the result that the holomorph with $N := (B,+)$ and $H := (B,\circ)$ gives a brace. We have classified skew and abelian braces of different cardinalities. We have used the lambda function to construct a small and tangible example of a dihedral brace, and thus gone on to state results on prime dihedral braces, prime power dihedral braces and odd dihedral braces.

Acknowledgements

We would like to first thank our supervisor Agata, for helping us navigate the treacherous seas of brace theory. Particularly, for encouraging us at times when we felt cast adrift. She has introduced us to a highly interesting and modern area of mathematics in which she has produced countless papers and for that we are grateful. We also wish to thank Scott and Dora for meeting with us early on and acting as the perfect soundboards as we got to grips with the technical areas of the project. Finally we wish to thank Dave who embarked on this journey into braces alongside us and was present and insightful in our early meetings before his dissertation deviated from our area of focus.

Bibliography

[1] E. Acri and M. Bonatto. *Skew braces of size pq*. Jan. 2020. URL: https://doi.org/10.10802F00927872.2019.1709480.

[2] T. M. Apostol. *Introduction to analytic number theory*. 2011.

[3] D. Bachiller Perez. *Classification of braces of order p^3*. 2014. URL: https://arxiv.org/abs/1407.5224.

[4] D. Bachiller Perez. *Counterexample to a conjecture about braces*. 2015. URL: https://arxiv.org/abs/1507.02137.

[5] D. Bachiller Perez. *Extensions, matched products, and simple braces*. 2015. URL: https://arxiv.org/abs/1511.08477.

[6] D. Bachiller Perez. *Study of the algebraic structure of left braces and the Yang-Baxter equation*. 2016. URL: https://core.ac.uk/display/78544947.

[7] K. Banerjee and P. Das Adhikary. *An elementary alternative proof for Chan's analogue of Ramanujan's most beautiful identity and some inequality of the cubic partition*. 2016.

[8] F. Cedo, E. Jespers, and J. Okninski. *Braces and the Yang-Baxter equation*. 2012. URL: https://arxiv.org/abs/1205.3587.

[9] F. Cedo, A. Smoktunowicz, and L. Vendramin. *Skew left braces of nilpotent type*. 2018. URL: https://arxiv.org/abs/1806.01127.

[10] F. Cedo et al. *On various types of nilpotency of the structure monoid and group of a set-theoretic solution of the Yang-Baxter equation*. 2022. URL: https://doi.org/10.1016/j.jpaa.2022.107194.

[11] A. Doikou and B. Rybolowicz. *Novel non-involutive solutions of the Yang-Baxter equation from (skew) braces*. 2022. URL: https://arxiv.org/abs/2204.11580.

[12] P. Etingof, T. Schedler, and A. Soloviev. *Set-theoretical solutions to the quantum Yang-Baxter equation*. 1998. URL: https://arxiv.org/abs/math/9801047.

[13] R. Fenn, M. Jordan-Santana, and L. H. Kauffman. *Biquandles and virtual links*. 2004.

[14] R. Fox and L. Neuwirth. *The Braid Groups*. 1962. URL: http://www.jstor.org/stable/24489274.

[15] L. Guarnieri and L. Vendramin. *Skew braces and the Yang–Baxter equation*. Nov. 2016. URL: https://doi.org/10.10902Fmcom2F3161.

[16] E. Jespers, A. Van Antwerpen, and L. Vendramin. *Nilpotency of skew braces and multipermutation solutions of the Yang–Baxter equation*. Oct. 2022. URL: https://doi.org/10.11422Fs021919972250064x.

[17] E. Jespers, L. Kubat, and A. Van Antwerpen. *The structure monoid and algebra of a non-degenerate set-theoretic solution of the Yang-Baxter equation*. 2018. URL: https://arxiv.org/abs/1812.02026.

[18] P. Kinnear, I. Lau, and D. Puljic. *Year 4 Project: Left Braces and the Solutions of the Yang-Baxter Equation*. 2019.

[19] A. Koch and P. J. Truman. *Opposite skew left braces and applications*. 2019. URL: https://arxiv.org/abs/1908.02682.

[20] K. Nejabati Zenouz. *On Hopf-Galois Structures and Skew Braces of Order p^3*. Jan. 2018. URL: http://hdl.handle.net/10871/32248.

[21] V. N. Remeslennikov. *Holomorph of a group*. June 2020.

[22] W. Rump. *Braces, radical rings, and the quantum Yang–Baxter equation*. 2007. URL: https://www.sciencedirect.com/science/misc/pii/S0021869306002626.

[23] W. Rump. *Classification of cyclic braces*. June 2007.

[24] S. Sierra. *Group Theory*. 2022.

[25] A. Smoktunowicz. *A note on set-theoretic solutions of the Yang-Baxter equation*. 2015. URL: https://arxiv.org/abs/1512.06642.

[26] A. Smoktunowicz. *On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation*. 2015. URL: https://arxiv.org/abs/1509.00420.

[27] A. Smoktunowicz and L. Vendramin. *On skew braces (with an appendix by N. Byott and L. Vendramin)*. Feb. 2018. URL: https://doi.org/10.41712Fjca2F2-1-3.

[28] L. Stefanello and S. Trappeniers. *On bi-skew braces and brace blocks*. 2023. URL: https://www.sciencedirect.com/science/misc/pii/S0022404922002936.

[29] E. M. Stein and R. Shakarchi. *Complex Analysis*. 2009.

[30] V. G. Turaev. *Quantum Invariants of Knots and 3-Manifolds*. Berlin, Boston, 2016. URL: https://doi.org/10.1515/9783110435221.