# Cayley-Dickson Loops

Jenya Kirshtein
*University of Denver*

# Cayley–Dickson Loops

A Dissertation

Presented to

the Faculty of Natural Sciences and Mathematics

University of Denver

in Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

by

Jenya Kirshtein

August 2012

Advisor: Petr Vojtěchovský

Author: Jenya Kirshtein
Title: Cayley-Dickson Loops
Advisor: Petr Vojtěchovský
Degree date: August 2012

# Abstract

In this dissertation we study the Cayley–Dickson loops, multiplicative structures arising from the standard Cayley–Dickson doubling process. More precisely, the Cayley–Dickson loop $Q_n$ is the multiplicative closure of basic elements of the algebra constructed by $n$ applications of the doubling process (the first few examples of such algebras are real numbers, complex numbers, quaternions, octonions, sedenions). Starting at the octonions, Cayley–Dickson algebras and loops become nonassociative, which presents a significant challenge in their study.

We begin by describing basic properties of the Cayley–Dickson loops $Q_n$. We establish or recall elementary facts about $Q_n$, e.g., inverses, conjugates, orders of elements, and diassociativity. We then discuss some important subloops of $Q_n$, for instance, associator subloop, derived subloop, nuclei, center, and show that $Q_n$ are Hamiltonian.

We study the structure of the automorphism groups of $Q_n$. We show that all subloops of $Q_n$ of order 16 fall into two isomorphism classes, in particular, any such subloop is either isomorphic to the octonion loop $\mathbb{O}_{16}$, or the quasioctonion loop $\tilde{\mathbb{O}}_{16}$. This helps to establish that starting at the sedenion loop, the group $\mathrm{Aut}\,(Q_n)$ is isomorphic to $\mathrm{Aut}\,(\mathbb{O}_{16}) \times (\mathbb{Z}_2)^{n-3}$.

Next we study two notions that are of interest in loop theory, the inner mapping group $Inn(Q_n)$ and the multiplication group $Mlt(Q_n)$. We prove that $Inn(Q_n)$ is an elementary abelian 2-group of order $2^{2^n-2}$, moreover, every $f \in Inn(Q)$ is a product of disjoint transpositions of the form $(x, -x)$. This implies that nonassociative Cayley–Dickson loops are not automorphic. The elements of $Mlt(Q_n)$ are even permutations and have order $1, 2$ or $4$. We show that $Mlt(Q_n)$ is a semidirect product of $Inn(Q_n) \times \mathbb{Z}_2$ and an elementary abelian 2-group $K$, and construct an isomorphic copy of $Mlt(Q_n)$ as an external semidirect product of two abstract elementary abelian 2-groups. The groups $Inn_l(Q_n)$ and $Inn_r(Q_n)$ are proved to be equal, elementary abelian 2-groups of order $2^{2^{n-1}-1}$. We also establish that $Mlt_l(Q_n)$ is a semidirect product of $Inn_l(Q_n) \times \mathbb{Z}_2$ and $K$, and that $Mlt_l(Q_n)$ and $Mlt_r(Q_n)$ are isomorphic.

Finally, we describe the progress made on the study of the subloop structure of the Cayley–Dickson loops. We calculate the number of subloops of a certain size, and provide the subloop lattice for $\mathbb{O}_{16}$. Then we describe numerical experiments performed to determine the isomorphism types of maximal (index 2) subloops of the Cayley–Dickson loops, and explain the obstacles on the way to finding an invariant that distinguishes such subloops. We provide incidence tetrahedra for the sedenion loop and other subloops of order 32, generalizing the idea of the octonion multiplication Fano plane. A number of conjectures concerning the subloops of $Q_n$ is posed in the last part of the dissertation.

## Acknowledgements

I am indebted to my advisor Petr Vojtěchovský for introducing me to loop theory and combinatorics, for his expertise, countless suggestions, and time spent on discussions. Without his guidance this dissertation would not have been possible, and no words can express my gratitude.

I would like to thank Michael Kinyon, Richard Ball, Nikolaos Galatos, Richard Green, and J. Michael Daniels for reading this dissertation and serving on my PhD committee.

I had the pleasure to meet many people of the loop theory community, and would like to thank them for their openness and interest. My warmest thanks go to Alvaro Arias and James Hagler for their care during all stages of my study. I thank Julien Langou for inviting me for summer internship at the Innovative Computing Laboratory, University of Tennessee Knoxville. I also thank the faculty, my fellow students, Liane Beights, and Don Oppliger for making the Department of Mathematics a great place for work and collaboration. I am indebted to the Department of Mathematics for providing financial support for conference travel.

I am grateful to my family and friends all around the world for their encouragement and for bringing happiness into my life. I thank Eugene Vecharynski for his support, expertise, and sense of humor.

**Dedicated to my parents, Alek and Alla**

# Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction

The study of loops originated from algebra, combinatorics, geometry, and topology, and developed into an independent discipline during the last eighty years. The story of the Cayley–Dickson loops, however, began earlier, when William R. Hamilton invented the quaternions. Hamilton discovered in 1835 that complex numbers can be treated as pairs of real numbers, and spent years trying to find a bigger, 3-dimensional normed division algebra. The problem was that there is no 3-dimensional normed division algebra, and he needed a 4-dimensional one. A solution came to Hamilton in 1843, while he was walking along the Royal Canal in Dublin, and he carved

$$i^2 = j^2 = k^2 = ijk = -1$$

on the side of the Brougham Bridge. Quaternions are usually denoted by $\mathbb{H}$ in honor of Hamilton. Several months later, John T. Graves extended Hamilton's idea and suggested the 8-dimensional normed division octonion algebra, calling it "the octaves". Hamilton pointed out that the octonions were not associative, suggesting the term "associative" around the same time (in fact, the octonions were the first example of an abstract nonassociative system [35]). Graves postponed publishing his results until Arthur Cayley independently discovered the octonions and published his findings in 1845 [8]. As a result, the octonions became widely known as "Cayley numbers" [2]. Adolf Hurwitz established in 1898 [17] that real numbers, complex numbers, quaternions and octonions were the only normed division algebras. Leonard E. Dickson generalized the construction beyond the dimension 8 in 1919 [11], suggesting what became known as the Cayley–Dickson doubling process. Dickson and his former student A. Adrian Albert formed a research group at the University of Chicago, and introduced the term "loop" around 1942, named after the Chicago Loop business district. R. D. Schafer finally mentioned the Cayley–Dickson loops in 1954 [38] as the elements of the normalized basis of the generalized Cayley–Dickson algebras with multiplication.

In this work we study the Cayley–Dickson loops from the algebraic perspective. In particular, we describe basic properties of the Cayley–Dickson loops, their automorphism groups, multiplication groups, inner mapping groups, and make progress in the study of the subloop structure. We often use GAP system for computational discrete algebra [15], specifically the LOOPS package [32], to perform numerical experiments and verify conjectures. Many of the results presented in this dissertation can also be found in [24], [25], [26].

The concepts we touch upon in this work have connections to various fields of mathematics, physics, and computer science, for instance, coding theory ([41]), computer graphics ([40]), combinatorial designs and cryptography (difference sets in loops [19], [20], [21]), spectral graph theory (expander graphs [28]), functional analysis (analysis over Cayley–Dickson numbers [29], [30]), polyhedral geometry (latin square polytopes [13], [1], [14]). In his paper [2] John Baez describes connections of the octonions to Clifford algebras and spinors, projective geometry, Jordan algebras, exceptional Lie groups, quantum logic, special relativity and supersymmetry, etc., providing an extensive list of references.

## 1.1 Summary of Results

The dissertation is organized as follows. In *Chapter 2* we study basic properties of the Cayley–Dickson loops $Q_n$. We establish or recall elementary facts about $Q_n$, e.g., inverses, conjugates, orders of elements, and diassociativity. We then study some important subloops of $Q_n$, for instance, associator subloop, derived subloop, nuclei, center, and show that $Q_n$ are Hamiltonian. The chapter also includes a section on calculus for commutators and associators.

*Chapter 3* is devoted to the automorphism groups of $Q_n$. We show that all subloops of $Q_n$ of order 16 fall into two isomorphism classes, in particular, any such subloop is either isomorphic to the octonion loop $\mathbb{O}_{16}$, or the quasioctonion loop $\tilde{\mathbb{O}}_{16}$. This fact helps to establish that starting at the sedenion loop, the group $\mathrm{Aut}\,(Q_n)$ is isomorphic to $\mathrm{Aut}\,(\mathbb{O}_{16}) \times (\mathbb{Z}_2)^{n-3}$.

In *Chapter 4* we study two notions that are of interest in loop theory, the inner mapping group $Inn(Q_n)$ and the multiplication group $Mlt(Q_n)$. We prove that $Inn(Q_n)$ is an elementary abelian 2-group of order $2^{2^n-2}$, moreover, every $f \in Inn(Q_n)$ is a product of disjoint transpositions of the form $(x, -x)$. This implies that nonassociative Cayley–Dickson loops are not automorphic. The elements of $Mlt(Q_n)$ are even permutations and have order $1, 2$ or $4$. We show that $Mlt(Q_n)$ is a semidirect product of $Inn(Q_n) \times \mathbb{Z}_2$ and an elementary abelian 2-group $K$, and construct an isomorphic copy of $Mlt(Q_n)$ as an external semidirect product of two abstract elementary abelian 2-groups. The groups $Inn_l(Q_n)$ and $Inn_r(Q_n)$ are proved to be equal, elementary abelian 2-groups of order $2^{2^{n-1}-1}$. We conclude the chapter by establishing that $Mlt_l(Q_n)$ is a semidirect product of $Inn_l(Q_n) \times \mathbb{Z}_2$ and $K$, and $Mlt_l(Q_n)$ and $Mlt_r(Q_n)$ are isomorphic.

*Chapter 5* describes the progress made in the study of the subloop structure of the Cayley–Dickson loops. We calculate the number of subloops of a certain size, and provide the subloop lattice for $\mathbb{O}_{16}$. Then we describe numerical experiments performed to determine the isomorphism types of maximal (index 2) subloops of the Cayley–Dickson loops, and explain the obstacles on the way to finding an invariant that distinguishes such subloops. We provide incidence tetrahedrons for the sedenion loop and other subloops of order 32, generalizing the idea of the octonion multiplication Fano plane. A number of conjectures concerning the subloops of $Q_n$ is posed throughout the chapter.

## 1.2 Preliminaries

In this section we introduce basic concepts of abstract algebra and loop theory that are used in this work. For more information on these topics a reader can be referred to [34], [4], [3].

A *groupoid* (or *magma*) $(Q,\cdot)$ is a nonempty set $Q$ with a binary operation $\cdot$ on $Q$. A groupoid $(Q,\cdot)$ is a *quasigroup* if for any $x,z \in Q$ there is a unique $y$ such that $x \cdot y = z$, and for any $y,z \in Q$ there is a unique $x$ such that $x \cdot y = z$. The multiplication table of a finite quasigroup is a *Latin square*, i.e., an $n \times n$ table filled with $n$ distinct symbols so that each symbol occurs once in every row and once in every column. A quasigroup $(Q,\cdot)$ is a *loop* if there is a neutral element $1 \in Q$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$. A subset $S$ of a loop $Q$ is a *subloop* if $(S,\cdot)$ is a loop. For convenience and to avoid excessive bracketing, we often write $xy$ instead of $x \cdot y$, $x \cdot yz$ instead of $x \cdot (y \cdot z)$, and $Q$ instead of $(Q,\cdot)$.

We agree to write mappings on the left of an argument, e.g., $f(x)$, and compose them from right to left. Let $Q, Q_2$ be quasigroups. A mapping $\phi : Q \to Q_2$ is an *injection* if $\phi(x) = \phi(y)$ implies $x = y$ for all $x, y \in Q$, a *surjection* if for every $y \in Q_2$ there is $x \in Q$ such that $y = \phi(x)$, a *bijection* if it is both an injection and a surjection, and a *homomorphism* if $\phi(x)\phi(y) = \phi(xy)$ for all $x, y \in Q$. A homomorphism $\phi : Q \to Q_2$ is an *isomorphism* if it is a bijection. If $Q$ is isomorphic to $Q_2$, we write $Q \cong Q_2$. An isomorphism $\phi : Q \to Q$ is called an *automorphism*.

The set of all automorphisms of a quasigroup $Q$ forms a group under composition, called the *automorphism group*, denoted by $Aut(Q)$.

Study of arbitrary loops presents a significant challenge, and it is natural to consider loops where some weakened form of the associative law holds.

A quasigroup $Q$ is said to have the *left inverse property* if there exists a bijection $\lambda : x \mapsto x^{\lambda}$ on $Q$ such that $x^{\lambda}(xy) = y$ for every $y \in Q$. Similarly, a quasigroup $Q$ is said to have the *right inverse property* if there exists a bijection $\rho : x \mapsto x^{\rho}$ on $Q$ such that $(yx)x^{\rho} = y$ for every $y \in Q$. A quasigroup which has both left and right inverse properties is called an *inverse property quasigroup*.

If $Q$ is a loop with identity 1, every element $x$ of $Q$ has a unique left inverse $x^{\lambda}$ and a unique right inverse $x^{\rho}$ such that $x^{\lambda}x = xx^{\rho} = 1$. However, the existence of $x^{\lambda}$ and $x^{\rho}$ does not necessarily imply $x^{\lambda}(xy) = y$ and $(yx)x^{\rho} = y$. Therefore not every loop is an inverse property loop.

A simple argument can be used to show that in a left (or right) inverse property loop one-sided inverses coincide, i.e., $x^{\lambda} = x^{\rho} = x^{-1}$, where $x^{-1}x = xx^{-1} = 1$. Note that in this case $Q$ is not necessarily an inverse property loop.

A loop with two-sided inverses has an *anti-automorphic inverse property* if $(xy)^{-1} = y^{-1}x^{-1}$. Inverse property loops satisfy the anti-automorphic inverse property.

A loop $Q$ is *alternative* if it satisfies the *left and right alternative properties*

$$\begin{aligned} x(xy) &= x^2y, \\ (yx)x &= yx^2. \end{aligned}$$

A loop $Q$ is *power-associative* if every element of $Q$ generates a group in $Q$, and *diassociative* if every pair of elements of $Q$ generates a group in $Q$. One can see that diassociativity implies the inverse property.

A loop $Q$ is a *Moufang loop* if it satisfies any of the following *Moufang identities*:

$$\begin{aligned} ((xz)y)z &= x(z(yz)), && (1.2.1)\\ (zx)(yz) &= z((xy)z), && (1.2.2)\\ z(x(zy)) &= (z(xz))y. && (1.2.3) \end{aligned}$$

Note that any one of these identities implies the other two. Ruth Moufang studied these loops first under the name "quasigroup".

For a loop $Q$ and $x, a \in Q$, mappings $L_x(a) = xa$ and $R_x(a) = ax$ are called *left* and *right translations*. These mappings are permutations on $Q$. Define the following subgroups of $Sym(Q)$,

*multiplication group of* $Q$, $Mlt(Q) = \langle L_x, R_x \mid x \in Q \rangle$,

*inner mapping group of* $Q$, $Inn(Q) = Mlt(Q)_1 = \{f \in Mlt(Q) \mid f(1) = 1\}$,

*left multiplication group of* $Q$, $Mlt_l(Q) = \langle L_x \mid x \in Q \rangle$,

*left inner mapping group of* $Q$, $Inn_l(Q) = Mlt_l(Q)_1 = \{f \in Mlt_l(Q) \mid f(1) = 1\}$,

*right multiplication group of* $Q$, $Mlt_r(Q) = \langle R_x \mid x \in Q \rangle$,

*right inner mapping group of* $Q$, $Inn_r(Q) = Mlt_r(Q)_1 = \{f \in Mlt_r(Q) \mid f(1) = 1\}$.

Let $R_Q = \{R_x \mid x \in Q\}$. Then $R_Q$ is a *left transversal* to $Inn(Q)$ in $Mlt(Q)$, and also a *right transversal* to $Inn(Q)$ in $Mlt(Q)$. That is, for every $f \in Mlt(Q)$ there is a unique $x \in Q$ and a unique $y \in Q$ such that $f \in R_x Inn(Q)$, $f \in Inn(Q)R_y$. An analogous statement is true for $L_Q = \{L_x \mid x \in Q\}$. Define *middle, left* and *right inner mappings* on $Q$ by

$$\begin{aligned} T_x &= L_x^{-1} R_x,\\ L_{x,y} &= L_{yx}^{-1} L_y L_x,\\ R_{x,y} &= R_{xy}^{-1} R_y R_x. \end{aligned}$$

Note that the inner mapping $T_x$ plays the role of conjugation. The mappings $L_{x,y}$, $R_{x,y}$ measure deviations from associativity, just as $T_x$ measures deviations from commutativity.

**Theorem 1.2.1.** *[34] Let $Q$ be a loop. Then*

$$\begin{aligned} Inn(Q) &= \langle L_{x,y}, R_{x,y}, T_x \mid x, y \in Q \rangle, \\ Inn_l(Q) &= \langle L_{x,y} \mid x, y \in Q \rangle, \\ Inn_r(Q) &= \langle R_{x,y} \mid x, y \in Q \rangle. \end{aligned}$$

**Lemma 1.2.2.** *Let $Q$ be a finite loop. Then*

$$\begin{aligned} |Mlt(Q)| &= |Q||Inn(Q)|, \\ |Mlt_l(Q)| &= |Q||Inn_l(Q)|, \\ |Mlt_r(Q)| &= |Q||Inn_r(Q)|. \end{aligned}$$

**Remark 1.2.3.** *Let $G$ be a group. If $G$ is abelian, then $Mlt(G) \cong G$, and $Inn(G) \cong \{1\}$. If $G$ is not abelian, then*

$$\begin{aligned} Mlt(G) &\cong (G \times G)/\{(g,g) \mid g \in Z(G)\}, \\ Inn(G) &\cong G/Z(G). \end{aligned}$$

In an inverse property loop we have $R_x^{-1} = R_{x^{-1}}$ and $L_x^{-1} = L_{x^{-1}}$.

The *commutant* of a loop $Q$, denoted by $C(Q)$, is the set of elements that commute with every element of $Q$. More precisely, $C(Q) = \{a \in Q \mid ax = xa,\ \forall x \in Q\}$.

Let $Q$ be a loop. Define

$$\textit{the left nucleus of } Q,\ N_l(Q) = \{a \in Q \mid a \cdot xy = ax \cdot y, \quad \forall x, y \in Q\},$$

$$\textit{the middle nucleus of } Q,\ N_m(Q) = \{a \in Q \mid xa \cdot y = x \cdot ay, \quad \forall x, y \in Q\},$$

$$\textit{the right nucleus of } Q,\ N_r(Q) = \{a \in Q \mid xy \cdot a = x \cdot ya, \quad \forall x, y \in Q\}.$$

The *nucleus* of $Q$, denoted by $N(Q)$, is the set of elements that associate with all elements of $Q$. More precisely,

$$\begin{aligned} N(Q) &= N_l(Q) \cap N_m(Q) \cap N_r(Q) \\ &= \{a \in Q \mid a \cdot xy = ax \cdot y, xa \cdot y = x \cdot ay, xy \cdot a = x \cdot ya, \quad \forall x, y \in Q\}. \end{aligned}$$

The nuclei $N(Q), N_l(Q), N_m(Q), N_r(Q)$ are subloops of $Q$.

A subloop $S$ of a loop $Q$ is *normal* (denoted by $S \trianglelefteq Q$) if $xS = Sx$, $(xS)y = x(Sy)$, $x(yS) = (xy)S$ for all $x, y \in Q$.

**Remark 1.2.4.** *[12] The following are equivalent for a subloop $S$ of a loop $Q$*

*(i)* $S \trianglelefteq Q$,

*(ii)* $\phi(S) = S$ *for all* $\phi \in Inn(Q)$,

*(iii)* $S$ *is the kernel of some loop homomorphism* $\psi : Q \to Q_2$.

A *Hamiltonian loop* is a loop in which every subloop is normal.

The *center* of a loop $Q$, denoted by $Z(Q)$, is the set of elements that commute and associate with every element of $Q$. More precisely, $Z(Q) = C(Q) \cap N(Q)$. Note that $Z(Q)$ is a normal subloop of $Q$. For any $x, y, z \in Q$ define the *commutator*

$[x, y]$ and the *associator* $[x, y, z]$ by

$$\begin{aligned} xy &= (yx)[x, y], \\ xy \cdot z &= (x \cdot yz)[x, y, z]. \end{aligned}$$

**Remark 1.2.5.** *Commutators and associators in a loop $Q$ are well-defined modulo the center. That is, if $s_1, s_2, s_3 \in Z(Q)$, then $[x, y] = [s_1x, s_2y]$, $[x, y, z] = [s_1x, s_2y, s_3z]$.*

Let $Z_1(Q) = Z(Q)$, define $Z_{i+1}(Q)$ by $Z(Q/Z_i(Q)) = Q/Z_{i+1}(Q)$. Then $Q$ is *(centrally) nilpotent* if $Z_m(Q) = 1$ for some $m$, and the *nilpotency class* $cl(Q)$ of $Q$ is the smallest integer $m$ for which $Z_m(Q) = 1$.

The *associator subloop* of a loop $Q$, denoted by $A(Q)$, is the smallest normal subloop of $Q$ such that $Q/A(Q)$ is a group. Note that $A(Q)$ is the smallest normal subloop of $Q$ containing all associators $[x, y, z]$, where $x, y, z \in Q$.

The *derived subloop* of a loop $Q$, denoted by $Q'$, is the smallest normal subloop of $Q$ such that $Q/Q'$ is an abelian group. Note that $Q'$ is the smallest normal subloop of $Q$ containing all commutators $[x, y]$ and associators $[x, y, z]$, where $x, y, z \in Q$.

A *cyclic group* of order $n$, denoted $\mathbb{Z}_n$, is a group of order $n$ generated by an element $a$ of $\mathbb{Z}_n$, i.e., $\mathbb{Z}_n = \langle a \rangle = \{a^0, \dots, a^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$.

An *elementary abelian $p$-group* is a finite abelian group, where every non-identity element has prime order $p$.

A *direct product* of groups $(N, *)$ and $(K, \cdot)$ is a group $G = \{(h, k) \mid h \in N, k \in K\}$ with operation $\circ$ defined by $(h_1, k_1) \circ (h_2, k_2) = (h_1 * h_2, k_1 \cdot k_2)$. The direct product is denoted by $G = N \times K$. A *semidirect product* of groups $(N, *)$ and $(K, \cdot)$ is a group $G = \{(h, k) \mid h \in N, k \in K\}$ with operation $\circ$ defined by $(h_1, k_1) \circ (h_2, k_2) = (h_1 * \phi_{k_1}(h_2), k_1 \cdot k_2)$, where $\phi : K \to Aut(N)$ is a homomorphism. The semidirect product is denoted by $G = N \rtimes K$.

Finally, recall the Correspondence Theorem for loops; for the proof see [12]. The set of all subloops of a loop $Q$ forms a bounded lattice $Sub(Q)$ under the operations $A \wedge B = A \cap B$ and $A \vee B = \langle A \cup B \rangle$, with largest element $Q$ and smallest element $\{1\}$. The set of all normal subloops of $Q$ also forms a bounded lattice $Sub_{\trianglelefteq}(Q)$ with the same extreme elements and operations as in $Sub(Q)$, and $Sub_{\trianglelefteq}(Q)$ is a sublattice of $Sub(Q)$.

**Correspondence Theorem 1.2.6.** *Let $Q$ be a loop, $A \trianglelefteq Q$ and $\mathcal{L} = \{B \in Sub(Q) \mid A \leq B\}$. Then the projection $\pi_A : Q \to Q/A, a \mapsto aA$ induces an isomorphism of lattices $\phi : \mathcal{L} \to Sub(Q/A), B \mapsto B/A$ and an isomorphism of lattices $\psi : \mathcal{L} \cap Sub_{\trianglelefteq}(Q) \to Sub_{\trianglelefteq}(Q/A)$. Moreover, if $B, C \in \mathcal{L}$ then $B \trianglelefteq C$ if and only if $B/A \trianglelefteq C/A$, and in such a case $C/B \cong \phi(C)/\phi(B)$.*

## 1.3 Cayley–Dickson Doubling Process

We begin this section by introducing a notion of a composition algebra, and continue with the description of the Cayley–Dickson doubling process for construction of such algebras. We follow presentation of T. A. Springer and F. D. Veldkamp, and refer the reader to [39] for further details.

A *quadratic form* on a vector space $V$ over a field $F$ is a mapping $N : V \to F$ such that

(i) $N(\lambda x) = \lambda^2 N(x), \quad \lambda \in F, x \in V$;

(ii) The mapping $\langle\ ,\ \rangle : V \times V \to F$ defined by

$$\langle x, y \rangle = N(x+y) - N(x) - N(y)$$

is bilinear, i.e., linear in each of $x$ and $y$ separately.

A mapping $\langle\ ,\ \rangle$ is called the bilinear form associated with $N$. The form $\langle\ ,\ \rangle$ is said to be *nondegenerate* if

$$\langle x, y\rangle = 0 \text{ for all } y \in V \Rightarrow x = 0.$$

An *algebra* over a field $F$ is a vector space over $F$ with a bilinear (not necessarily associative) vector multiplication. A *composition algebra* $C$ over a field $F$ is a not necessarily associative algebra over $F$ with identity element 1 such that there exists a nondegenerate quadratic form $N$ on $C$ which permits composition, i.e., such that

$$N(xy) = N(x)N(y), \quad x, y \in C.$$

The quadratic form $N$ is often referred to as the *norm* on $C$, and the associated bilinear form $\langle\ ,\ \rangle$ is called the *inner product*. Every composition algebra satisfies the Moufang identities (1.2.1)–(1.2.3).

**Theorem 1.3.1.** *Every composition algebra is obtained by repeated doubling (see below), starting from $F$ in characteristic $\neq 2$ and from a 2-dimensional composition algebra in characteristic 2. The possible dimensions of a composition algebra are 1 (in characteristic $\neq 2$), 2, 4, and 8. Composition algebras of dimension 1 and 2 are commutative and associative, those of dimension 4 are associative but not commutative, and those of dimension 8 are neither commutative nor associative.*

A composition algebra of dimension $2n$ can be constructed from a composition algebra of dimension $n$ using the *Cayley–Dickson doubling process*. This construction can be carried out ad infinitum, producing a sequence of power-associative algebras of dimension $2, 4, 8, 16, 32$, and so on, that are not composition algebras after dimension 8. If a composition algebra $C$ contains a nonzero vector $x$ with $N(x) = 0$, it is called a *split composition algebra*. Otherwise, $C$ is a *division composition algebra*.

A well-known instance of the Cayley–Dickson process constructs complex numbers $\mathbb{C}$ from real numbers $\mathbb{R}$, quaternions $\mathbb{H}$ from complex numbers, octonions $\mathbb{O}$ from quaternions. A. Hurwitz showed in [17] that these are the only normed division algebras.

The Cayley–Dickson construction over a field $F$ is done as follows:

$$\begin{aligned} \mathbb{A}_0 &= F, \text{ with conjugation } a^* = a \text{ for all } a \in F, \\ \mathbb{A}_{n+1} &= \{(a,b) \mid a,b \in A_n\} \text{ for } n \in \mathbb{N}, \end{aligned}$$

with multiplication, addition, and conjugation

$$\begin{aligned} (a,b)(c,d) &= (ac + \lambda d^* b, da + bc^*) \quad (\text{where } 0 \neq \lambda \in F), \\ (a,b) + (c,d) &= (a + c, b + d), \\ (a,b)^* &= (a^*, -b). \end{aligned}$$

Conjugation defines a norm $\|a\| = (aa^*)^{1/2}$ and the multiplicative inverse for nonzero elements $a^{-1} = a^* / \|a\|^2$. Note that $(a,b)(a,b)^* = (\|a\|^2 + \|b\|^2, 0)$ and $(a^*)^* = a$. The dimension of $\mathbb{A}_n$ over $F$ is $2^n$.

When $\lambda = -1$, the construction is called the standard Cayley–Dickson process, which produces complex, quaternion, and octonion division composition algebras over $F$ [9]. The standard construction is the main focus of this work, and we further refer to it as simply the Cayley–Dickson process.

## 1.4 Cayley–Dickson Loops

We study multiplicative structures that arise from the Cayley–Dickson doubling process. Let $F$ be a field of characteristic other than two. Define *Cayley–Dickson* *loops* $(Q_n, \cdot)$ over $F$ inductively as follows:

$$Q_0 = \{1, -1\}, \quad Q_n = \{(x,0),(x,1) \mid x \in Q_{n-1}\}, \tag{1.4.1}$$

with multiplication

$$(x,0)(y,0) = (xy,0), \tag{1.4.2}$$

$$(x,0)(y,1) = (yx,1), \tag{1.4.3}$$

$$(x,1)(y,0) = (xy^*,1), \tag{1.4.4}$$

$$(x,1)(y,1) = (-y^*x,0), \tag{1.4.5}$$

and conjugation

$$\begin{aligned}(x,0)^* &= (x^*,0),\\ (x,1)^* &= (-x,1).\end{aligned}$$

**Proposition 1.4.1.** *Cayley–Dickson loops are independent of the underlying field $F$ of characteristic not two.*

*Proof.* By induction on $n$. Let $F$, $E$ be fields of characteristic not two, and let $(Q_n^F, \circ)$, $(Q_n^E, \diamond)$ be Cayley–Dickson loops over these fields. When $n = 0$ we have $Q_0^F = \{1_F, -1_F\}$, where

$$\begin{aligned}1_F \circ 1_F &= -1_F \circ (-1_F) = 1_F, \quad 1_F \circ (-1_F) = -1_F \circ 1_F = -1_F,\\ 1_F^* &= 1_F, \quad (-1_F)^* = -1_F,\end{aligned}$$

and $Q_0^E = \{1_E, -1_E\}$, where

$$\begin{aligned} 1_E \diamond 1_E &= -1_E \diamond (-1_E) = 1_E, \quad 1_E \diamond (-1_E) = -1_E \diamond 1_E = -1_E, \\ 1_E^* &= 1_E, \quad (-1_E)^* = -1_E. \end{aligned}$$

Suppose that $(Q_{n-1}, \cdot)$ is independent of the underlying field. Then in $Q_n^F$ we have

$$\begin{aligned} (x, 0_F) \circ (y, 0_F) &= (x \cdot y, 0_F), \\ (x, 0_F) \circ (y, 1_F) &= (y \cdot x, 1_F), \\ (x, 1_F) \circ (y, 0_F) &= (x \cdot y^*, 1_F), \\ (x, 1_F) \circ (y, 1_F) &= (-y^* \cdot x, 0_F), \\ (x, 0_F)^* &= (x^*, 0_F), \\ (x, 1_F)^* &= (-x, 1_F), \text{ where } x, y \in Q_{n-1}, \end{aligned}$$

and in $Q_n^E$ we have

$$\begin{aligned} (x, 0_E) \diamond (y, 0_E) &= (x \cdot y, 0_E), \\ (x, 0_E) \diamond (y, 1_E) &= (y \cdot x, 1_E), \\ (x, 1_E) \diamond (y, 0_E) &= (x \cdot y^*, 1_E), \\ (x, 1_E) \diamond (y, 1_E) &= (-y^* \cdot x, 0_E), \\ (x, 0_E)^* &= (x^*, 0_E), \\ (x, 1_E)^* &= (-x, 1_E), \text{ where } x, y \in Q_{n-1}. \quad \square \end{aligned}$$

The reader can assume $F = \mathbb{R}$ without loss of generality from now on.

The order of $Q_n$ is $2^{n+1}$. The loop $Q_n$ embeds into $Q_{n+1}$ by $x \mapsto (x, 0)$, so that

$Q_n \cong \{(x,0) \mid (x,0) \in Q_{n+1}\}$. All elements of $Q_n$ have norm one due to the fact that

$$\|(x, x_{n+1})\|^2 = (x, x_{n+1})(x, x_{n+1})^* = (\|x\|^2, 0) = \|x\|^2 = \|(x_1, \ldots, x_n)\|^2 = \ldots = \|x_1\| = 1,$$

however, not all the elements of $\mathbb{A}_n$ of norm one are in $Q_n$.

As will become apparent soon, we can think of the Cayley–Dickson loop as the multiplicative closure of basic units in the corresponding Cayley–Dickson algebra, with one unit added in each step of the doubling construction. The first few examples of the Cayley–Dickson loops are the group of real units $\mathbb{R}_2$ (abelian); the group of complex integral units $\mathbb{C}_4$ (abelian); the group of quaternion integral units $\mathbb{H}_8$ (not abelian); the octonion loop $\mathbb{O}_{16}$ (Moufang); the sedenion loop $\mathbb{S}_{32}$ (not Moufang); the trigintaduonion loop $\mathbb{T}_{64}$ (the name suggested by J.D.H. Smith comes from the Latin word "trigintaduo", meaning 32).

Denote the opposite of an element $(x_1, x_2, x_3, \ldots, x_{n+1})$ by

$$-(x_1, x_2, x_3, \ldots, x_{n+1}) = (-x_1, x_2, x_3, \ldots, x_{n+1}).$$

The elements $1_{Q_n}, -1_{Q_n} \in Q_n$ are

$$\begin{aligned} 1_{Q_n} &= (1, \underbrace{0, \ldots, 0}_{n}), \\ -1_{Q_n} &= (-1, \underbrace{0, \ldots, 0}_{n}). \end{aligned}$$

We call $1_{Q_n}$ by 1, and $-1_{Q_n}$ by $-1$. One can see that 1 and $-1$ commute and associate with every element of $Q_n$.

We denote the loop generated by elements $x_1, \ldots, x_n$ of a loop $L$ by $\langle x_1, \ldots, x_n \rangle$. Denote by $i_n$ the element $(1_{Q_{n-1}}, 1) = (1, \underbrace{0, \ldots, 0}_{n-1}, 1)$ of $Q_n$. Such element $i_n$ satisfies $Q_n = Q_{n-1} \cup (Q_{n-1} i_n) = \langle Q_{n-1}, i_n \rangle$. Thus $Q_n = \langle i_1, i_2, \ldots, i_n \rangle$. We call $i_1, i_2, \ldots, i_n$

the *canonical generators* of $Q_n$. Any $x \in Q_n$ can be written as

$$x = \pm \prod_{j=1}^{n} i_j^{\epsilon_j}, \quad \epsilon_j \in \{0, 1\}.$$

For example,

$$\begin{aligned}
Q_0 = \mathbb{R}_2 &= \{1, -1\}, \\
Q_1 = \mathbb{C}_4 &= \pm\{(1,0),(1,1)\} = \langle i_1 \rangle = \{1, -1, i_1, -i_1\}, \\
Q_2 = \mathbb{H}_8 &= \pm\{(1,0,0),(1,1,0),(1,0,1),(1,1,1)\} = \langle i_1, i_2 \rangle = \pm\{1, i_1, i_2, i_1 i_2\}, \\
Q_3 = \mathbb{O}_{16} &= \langle i_1, i_2, i_3 \rangle = \pm\{1, i_1, i_2, i_1 i_2, i_3, i_1 i_3, i_2 i_3, i_1 i_2 i_3\}, \\
Q_4 = \mathbb{S}_{32} &= \langle i_1, i_2, i_3, i_4 \rangle .
\end{aligned}$$

We use

$$e = i_n$$

for the unit added in the last step of the process. Figure 1.1 illustrates the construction of $Q_n$ from $Q_{n-1}$ by doubling.

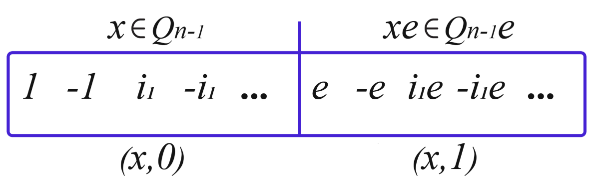


Figure 1.1: Construction of $Q_n$ from $Q_{n-1}$ by doubling

# Chapter 2

# Basic Properties

In this chapter we study fundamental properties of the Cayley–Dickson loops, for instance, subloops, Hamiltonian property, and calculus for commutators and associators.

## 2.1 Orders, Inverses, Conjugates of Elements

**Proposition 2.1.1.** *Let $Q_n$ be a Cayley–Dickson loop, let $x, y \in Q_n$. The following hold:*

1. $1_{Q_n} = (1, \underbrace{0, \ldots, 0}_{n})$ *is the identity of $Q_n$;*
2. *the conjugates of the elements of $Q_n$ are $x^* = -x$ for $x \in Q_n \setminus \{1, -1\}$, $1^* = 1$, $(-1)^* = -1$;*
3. *the orders of the elements of $Q_n$ are $|x| = 4$ for $x \in Q_n \setminus \{1, -1\}$, $|1| = 1$, $|-1| = 2$;*
4. *the inverses of the elements of $Q_n$ are $x^{-1} = x^*$;*
5. *$xy = -yx$ when $x, y \neq \pm 1$, $x \neq \pm y$, and $xy = yx$ otherwise;*
6. *$(xy)^{-1} = y^{-1}x^{-1}$ (anti-automorphic inverse property).*

*Proof.* 1. By induction on $n$. In $\mathbb{R}_2$ we have $1 \cdot 1 = 1$, $1 \cdot (-1) = (-1) \cdot 1 = -1$, so 1 is the identity of $\mathbb{R}_2$. Suppose $1_{Q_{n-1}}$ is the identity of $Q_{n-1}$. Then in $Q_n$ we have

$$\begin{aligned}
(1_{Q_{n-1}}, 0)(x, 0) &= (1_{Q_{n-1}} x, 0) = (x, 0) = (x 1_{Q_{n-1}}, 0) = (x, 0)(1_{Q_{n-1}}, 0), \\
(1_{Q_{n-1}}, 0)(x, 1) &= (x 1_{Q_{n-1}}, 1) = (x, 1) = (1_{Q_{n-1}} x, 1) = (x, 1)(1_{Q_{n-1}}, 0),
\end{aligned}$$

hence $1_{Q_n} = (1_{Q_{n-1}}, 0)$ is the identity of $Q_n$.

2. By induction on $n$. In $\mathbb{R}_2$, $1 \cdot 1 = -1 \cdot (-1) = 1$. Suppose $x^* = -x$ holds for all $x \in Q_n \backslash \{\pm 1\}$, then in $Q_{n+1}$ by definition $(x, 0)^* = (x^*, 0) = (-x, 0) = -(x, 0)$ and $(x, 1)^* = (-x, 1) = -(x, 1)$.

3. By induction on $n$. In $\mathbb{C}_4$, $(1, 0)(1, 0) = (1, 0)$ and $(1, 1)(1, 1) = -(1, 0)$. Suppose $x^2 = -1$ holds for all $x \in Q_n \backslash \{\pm 1\}$, then in $Q_{n+1}$ $(x, 0)(x, 0) = (xx, 0) = (-1_{Q_n}, 0) = -(1_{Q_n}, 0) = -1_{Q_{n+1}}$ and $(x, 1)(x, 1) = (-x^* x, 0) = (xx, 0) = (-1_{Q_n}, 0) = -(1_{Q_n}, 0) = -1_{Q_{n+1}}$.

4. Follows from 2. and 3. We have $x^* x = (-x)x = -(xx) = 1 = -(xx) = x(-x) = x x^*$ when $x \neq \pm 1$ and $(\pm 1)^2 = 1$.

5. The property holds for $\mathbb{H}_8$. Suppose it also holds for $Q_n$. In $Q_{n+1}$, if $x, y \neq \pm 1$, $x \neq \pm y$, then

$$\begin{aligned}
(x, 0)(y, 0) &= (xy, 0) = (-yx, 0) = -(y, 0)(x, 0), \\
(x, 0)(y, 1) &= (yx, 1) = (-yx^*, 1) = -(y, 1)(x, 0), \\
(x, 1)(y, 1) &= (-y^* x, 0) = (yx, 0) = (-xy, 0) = -(-x^* y, 0) = -(y, 1)(x, 1).
\end{aligned}$$

The cases when either $x, y \neq \pm 1$ and $x = \pm y$, or $x = \pm 1, y \neq \pm 1$, or $x = \pm y = \pm 1$ can be treated similarly.

6. We show that $(xy)^* = y^*x^*$ for all $x, y \in Q_n$, by induction on $n$. The property holds for $\mathbb{R}_2$. Suppose $(xy)^* = y^*x^*$ for all $x, y \in Q_n$, then in $Q_{n+1}$

$$
\begin{aligned}
((x,0)(y,0))^* &= (xy,0)^* = ((xy)^*,0) = (y^*x^*,0) = (y^*,0)(x^*,0) \\
&= (y,0)^*(x,0)^*, \\
((x,0)(y,1))^* &= (yx,1)^* = (-yx,1) = ((-y)(x^*)^*,1) \\
&= (-y,1)(x^*,0) = (y,1)^*(x,0)^*, \\
((x,1)(y,0))^* &= (xy^*,1)^* = (-xy^*,1) = (y^*,0)(-x,1) = (y,0)^*(x,1)^*, \\
((x,1)(y,1))^* &= (-y^*x,0)^* = ((-y^*x)^*,0) = (-x^*(y^*)^*,0) \\
&= (-x^*y,0) = (-y,1)(-x,1) = (y,1)^*(x,1)^*. \qquad \square
\end{aligned}
$$

Schafer showed in [38, Lemma 4] that the Cayley–Dickson loops satisfy the alternative properties.

**Lemma 2.1.2.** *Every Cayley–Dickson loop is alternative.*

*Proof.* By induction on $n$. The complex group $\mathbb{C}_4$ is associative, and hence alternative. Suppose

$$
\begin{aligned}
x(xy) &= x^2y, \\
(yx)x &= yx^2
\end{aligned}
$$

holds for all $x, y \in Q_n$, then in $Q_{n+1}$ we have

$$
\begin{aligned}
(x,0)\cdot(x,0)(y,0) &= (x,0)\cdot(xy,0) = (x(xy),0) = (x^2y,0) = (x^2,0)(y,0) \\
&= (x,0)(x,0)\cdot(y,0), \\
(x,0)\cdot(x,0)(y,1) &= (x,0)\cdot(yx,1) = ((yx)x,1) = (yx^2,1) = (x^2,0)\cdot(y,1) = \\
&= (x,0)(x,0)\cdot(y,1),
\end{aligned}
$$

$$
\begin{aligned}
(x,1)\cdot(x,1)(y,0) &= (x,1)\cdot(xy^*,1) = (-(xy^*)^*x,0) = (-(yx^*)x,0) = (-y(x^*x),0)\\
&= (-(x^*x)y,0) = (-x^*x,0)(y,0) = (x,1)(x,1)\cdot(y,0),\\
(x,1)\cdot(x,1)(y,1) &= (x,1)\cdot(-y^*x,0) = (x(-y^*x)^*,1) = (-x(x^*y),1) = (-(xx^*)y,1)\\
&= (-y(xx^*),1) = (-x^*x,0)(y,1) = (x,1)(x,1)\cdot(y,1).
\end{aligned}
$$

The right alternative property can be proved similarly. □

**Proposition 2.1.3.** *Cayley–Dickson loops are indeed loops.*

*Proof.* Let $Q_n$ be a Cayley–Dickson loop. By Proposition 2.1.1-(1),

$$1_{Q_n} = (1, \underbrace{0,\ldots,0}_{n})$$

is the identity of $Q_n$. By Proposition 2.1.1-(2) we have $x^* = -x$ for $x \in Q_n \setminus \{1,-1\}$, $1^* = 1$, $(-1)^* = -1$. Note that $-1$ commutes and associates with every element of $Q_n$. Using Lemma 2.1.2, for all $x, z \in Q_n$ there is a unique $y = x^*z \in Q_n$ such that $xy = x(x^*z) = (xx^*)z = z$, and for all $y, z \in Q_n$ there is a unique $x = zy^* \in Q_n$ such that $xy = (zy^*)y = z(y^*y) = z$. □

## 2.2 Diassociativity

Culbert established in [10] that Cayley–Dickson loops are diassociative.

**Theorem 2.2.1.** *Any pair of elements of a Cayley–Dickson loop generates a subgroup of the quaternion group. In particular, a pair $x, y$ generates a real group when $x = \pm 1$ and $y = \pm 1$; a complex group when either $x = \pm 1$, or $y = \pm 1$ (but not both), or $x = \pm y \neq \pm 1$; a quaternion group otherwise.*

*Proof.* Let $x, y$ be elements of a Cayley–Dickson loop. If $x, y \neq \pm 1$ and $x \notin \langle y \rangle$, then by Proposition 2.1.1 we have $xy = -yx$ and $x^2 = y^2 = -1$, and by Lemma 2.1.2 we have $x(xy) = x^2y$ and $(yx)x = yx^2$, thus

$$\begin{aligned} x(xy) &= x^2y = -y, \\ y(xy) &= -y(yx) = -y^2x = x, \\ (xy)x &= -(yx)x = -yx^2 = y, \\ (xy)y &= xy^2 = -x. \end{aligned}$$

These calculations allow to construct the multiplication table of a loop $\langle x, y\rangle$.

| $1$ | $-1$ | $x$ | $-x$ | $y$ | $-y$ | $xy$ | $-xy$ |
|---|---|---|---|---|---|---|---|
| $-1$ | $1$ | $-x$ | $x$ | $-y$ | $y$ | $-xy$ | $xy$ |
| $x$ | $-x$ | $-1$ | $1$ | $xy$ | $-xy$ | $-y$ | $y$ |
| $-x$ | $x$ | $1$ | $-1$ | $-xy$ | $xy$ | $y$ | $-y$ |
| $y$ | $-y$ | $-xy$ | $xy$ | $-1$ | $1$ | $x$ | $-x$ |
| $-y$ | $y$ | $xy$ | $-xy$ | $1$ | $-1$ | $-x$ | $x$ |
| $xy$ | $-xy$ | $y$ | $-y$ | $-x$ | $x$ | $-1$ | $1$ |
| $-xy$ | $xy$ | $-y$ | $y$ | $x$ | $-x$ | $1$ | $-1$ |

Table 2.1: Multiplication table of $\langle x, y\rangle$

One can check that $\langle x, y\rangle$ is a quaternion group.

If either $x = \pm 1$, or $y = \pm 1$ (but not both), we have

| $1$ | $-1$ | $x$ | $-x$ |
|---|---|---|---|
| $-1$ | $1$ | $-x$ | $x$ |
| $x$ | $-x$ | $-1$ | $1$ |
| $-x$ | $x$ | $1$ | $-1$ |

Table 2.2: Multiplication table of $\langle x\rangle$

One can see that $\langle x\rangle$ is a complex group.

If $x = \pm 1$ and $y = \pm 1$, clearly

$$\langle x, y \rangle = \{1, -1\} \cong \mathbb{R}_2. \qquad \square$$

Lemma 3.2.1 in Section 3.2 generalizes Theorem 2.2.1 and shows that any three elements of a Cayley–Dickson loop generate a subloop of either the octonion loop, or the quasioctonion loop.

**Corollary 2.2.2.** *Every Cayley–Dickson loop is diassociative.*

*Proof.* The quaternion group $\mathbb{H}_8$ is associative and the rest follows from Theorem 2.2.1. $\square$

In particular, Cayley–Dickson loops are inverse property loops. An inverse property loop $Q$ is a *RIF* loop ("respects inverses, flexible", see [22]) if for any $x, y, z \in Q$

$$(xy)(z \cdot xy) = ((x \cdot yz)x)y. \tag{2.2.1}$$

**Lemma 2.2.3.** *Every Cayley–Dickson loop is a RIF loop.*

*Proof.* Let $Q_n$ be a Cayley–Dickson loop. Let us show that all $x, y, z \in Q_n$ satisfy (2.2.1)

$$(xy)(z \cdot xy) = ((x \cdot yz)x)y.$$

If $|\langle x, y, z \rangle| \leq 8$ then $\langle x, y, z \rangle$ is a group by Theorem 2.2.1, and the statement holds. Let $|\langle x, y, z \rangle| = 16$. By Theorem 2.2.1, $z \notin \langle x, y \rangle \cong \mathbb{H}_8$. We have $z \notin \langle xy \rangle$, $x \notin \langle yz \rangle$, $y \notin \langle z \rangle$, thus $[z, xy] = [x, yz] = [y, z] = -1$. Also, $x, y, xy \neq \pm 1$, therefore $x^2 = y^2 = (xy)^2 = -1$. Using diassociativity, we have

$$(xy)(z \cdot xy) = [z, xy](xy)(xy \cdot z) = [z, xy](xy)^2 z = z,$$

$$
\begin{aligned}
((x\cdot yz)x)y &= [x,yz]((yz\cdot x)x)y = [x,yz](yz\cdot x^2)y = [x,yz]x^2(yz\cdot y)\\
&= [x,yz][y,z]x^2(zy\cdot y) = [x,yz][y,z]x^2(z\cdot y^2)\\
&= [x,yz][y,z]x^2y^2z = z. \qquad \square
\end{aligned}
$$

## 2.3 Associator Subloop, Derived Subloop, Nuclei, Center

**Theorem 2.3.1.** *If $Q_n$ is a Cayley–Dickson loop, then $Q_n/\{1,-1\} \cong (\mathbb{Z}_2)^n$.*

*Proof.* The loop $\{1,-1\}$ is a unique minimal subloop of $Q_n$. Let us show that $Q_n/\{1,-1\}$ has exponent 2 and hence is an elementary abelian 2-group. Proceed by induction on $n$. Consider the construction (1.4.1). In $\mathbb{C}_4/\{1,-1\}$, we have $(1,0)(1,0) = (1,0)$ and $(1,1)(1,1) = (1,0)$. Suppose $x^2 = 1$ holds for all $1 \neq x \in Q_n/\{1,-1\}$, then in $Q_{n+1}/\{1,-1\}$ we have $(x,0)(x,0) = (xx,0) = (1,0) = 1$ and $(x,1)(x,1) = (xx,0) = (1,0) = 1$. The order of $Q_n/\{1,-1\}$ is $\frac{|Q_n|}{2} = 2^n$. $\square$

It follows immediately from Theorem 2.3.1 that $cl(Q_n) = 2$ when $n \geq 2$, and $cl(Q_n) = 1$ otherwise.

**Lemma 2.3.2.** *Let $S$ be a subloop of $Q_n$. The following hold:*

1. *the center of $S$, $Z(S) = \{1,-1\}$ when $|S| > 4$ and $Z(S) = S$ otherwise;*
2. *the nuclei of $S$ coincide, i.e., $N(S) = N_l(S) = N_m(S) = N_r(S)$, moreover, $N(S) = \{1,-1\}$ when $|S| > 8$ and $N(S) = S$ otherwise;*
3. *the group $S/Z(S)$ is an elementary abelian 2-group;*
4. *the associator subloop of $S$, $A(S) = Z(S)$ when $|S| > 8$ and $A(S) = 1$ otherwise;*
5. *the derived subloop of $S$, $S' = Z(S)$ when $|S| > 4$ and $S' = 1$ otherwise.*

*Proof.* 1. Let $S$ be a subloop of $Q_n$. By Theorem 2.2.1, $S \leq \mathbb{C}_4$ when $|S| \leq 4$; $\mathbb{C}_4$ is an abelian group, hence $Z(S) = S$. Let $|S| > 4$. By Theorem 2.2.1, $\langle 1, x\rangle \leq \mathbb{C}_4$ and $\langle -1, x\rangle \leq \mathbb{C}_4$, $\mathbb{C}_4$ is abelian and therefore $\{1, -1\} \in C(S)$. Let $x \in S\backslash\{\pm 1\}$, choose an element $y \notin \{\pm 1, \pm x\}$. Then $\langle x, y\rangle \cong \mathbb{H}_8$ by Theorem 2.2.1, and $[x, y] = -1$. It follows that $C(S) = \{1, -1\}$. Also, $\langle 1, x, y\rangle \leq \mathbb{H}_8$ and $\langle -1, x, y\rangle \leq \mathbb{H}_8$, therefore $[1, x, y] = 1$ and $[-1, x, y] = 1$ for any $x, y \in S$, and

$$\{1, -1\} \in N(S). \tag{2.3.1}$$

It follows that $Z(S) = \{1, -1\}$.

2. Let $S$ be a subloop of $Q_n$. In any inverse property loop, the four nuclei coincide (see [34, p.21]). If $|S| \leq 8$, then $S$ is a group by Theorem 2.2.1, and $N(S) = S$. Let $|S| > 8$. From (2.3.1) we have $\{1, -1\} \leq N(S)$. For any $(x, x_{n+1}) \in S\backslash\{1, -1\}$ (where $x \neq \pm 1$, $x_{n+1} \in \{0, 1\}$), the size of $S$ allows to choose $y \notin \langle x\rangle$ in $S$, such that either $(y, 0)$ or $(y, 1)$ is in $S$, and

$$\begin{aligned}
(x,0)(y,0)\cdot(1,1) &= (xy,0)(1,1) = (xy,1) = (-yx,1) = (-x,0)(y,1) \\
&= -(x,0)\cdot(y,0)(1,1), \\
(x,0)(y,1)\cdot(1,1) &= (yx,1)(1,1) = (-yx,0) = (xy,0) = (-x,0)(-y,0) \\
&= -(x,0)\cdot(y,1)(1,1), \\
(x,1)(y,0)\cdot(1,1) &= (xy^*,1)(1,1) = (-xy^*,0) = (y^*x,0) = (-x,1)(y,1) \\
&= -(x,1)\cdot(y,0)(1,1), \\
(x,1)(y,1)\cdot(1,1) &= (-y^*x,0)(1,1) = (-y^*x,1) = (xy^*,1) = (-x,1)(-y,0) \\
&= -(x,1)\cdot(y,1)(1,1),
\end{aligned}$$

thus $(x, x_{n+1}) \notin N(S)$. It also follows from the above equations that $(1,1) \notin N(S)$.

3. Follows from Theorem 2.3.1.

4. Let $|S| > 8$. The group $S/Z(S)$ is abelian, hence $A(S) \leq Z(S)$. Also, $A(S) \neq 1$ since $S$ is not a group, so $A(S) = Z(S)$. Let $|S| \leq 8$, then $S \leq \mathbb{H}_8$ and $\mathbb{H}_8$ is a group, so $A(S) = 1$.

5. Let $|S| > 4$. The group $S/Z(S)$ is abelian, hence $S' \leq Z(S)$. Also, $S' \neq 1$ since $S$ is not an abelian group, so $S' = Z(S)$. Let $|S| \leq 4$, then $S \leq \mathbb{C}_4$ and $\mathbb{C}_4$ is an abelian group, so $S' = 1$. □

## 2.4 Commutator-Associator Calculus

For a Cayley–Dickson loop $Q_n$ we study commutators and associators in $Q_n$. Some of the results of this section are not used for further proofs, but are presented for completeness.

**Moufang's Theorem 2.4.1.** *[31] Let $Q$ be a Moufang loop and $x, y, z \in Q$. If $[x, y, z] = 1$ then $\langle x, y, z\rangle$ is a group and, in particular, the associator of $x, y, z$ is trivial for any ordering of the three elements.*

**Lemma 2.4.2.** *Let $x, y, z$ be elements of $Q_n$. The following hold:*

1. *the commutator $[x, y] = -1$ when $\langle x, y\rangle \cong \mathbb{H}_8$ and $[x, y] = 1$ when $\langle x, y\rangle < \mathbb{H}_8$;*

2. *the associator $[x, y, z] = 1$ or $[x, y, z] = -1$, in particular, $[x, y, z] = 1$ when $\langle x, y, z\rangle \leq \mathbb{H}_8$ and $[x, y, z] = -1$ when $\langle x, y, z\rangle \cong \mathbb{O}_{16}$.*

*Proof.* 1. Follows from Proposition 2.1.1-(5).

2. The loop $\mathbb{H}_8$ is associative, therefore $[x, y, z] = 1$ when $\langle x, y, z\rangle \leq \mathbb{H}_8$. If $\mathbb{H}_8 < \langle x, y, z\rangle$, we have $A(Q_n) \in \{1, -1\}$ by Lemma 2.3.2-(4), and $A(Q_n)$ is the smallest normal subloop of $Q_n$ containing all associators $[x, y, z]$, where

$x, y, z \in Q_n$. The loop $\mathbb{O}_{16}$ is Moufang and not a group, therefore by Moufang's Theorem $[x, y, z] = -1$ when $\langle x, y, z\rangle \cong \mathbb{O}_{16}$. $\square$

**Remark 2.4.3.** *It can happen that* $\langle x, y, z\rangle \ncong \mathbb{R}_2, \mathbb{C}_4, \mathbb{H}_8, \mathbb{O}_{16}$ *(see Lemma 3.2.1).*

If $\langle x, y, z\rangle \le \mathbb{H}_8$, then $\langle x, y, z\rangle$ is a group and $[y, x, z] = [z, x, y] = 1$. If $|\langle x, y, z\rangle| = 16$, then

$$\langle x, y, z\rangle = \pm\{1, x, y, xy, z, xz, yz, (xy)z\},$$

where all elements are distinct. This implies that $x \notin \pm\{1, y, z\}$, $zx \notin \pm\{1, y\}$, $yx \notin \pm\{1, z\}$, and by Lemma 2.4.2,

$$[x, z] = [y, zx] = [x, y] = [yx, z] = [x, yz] = [z, xy] = -1, \tag{2.4.1}$$

**Lemma 2.4.4.** *Let $Q$ be a loop. Suppose that $cl(Q) \le 2$ and $Z(Q)$ has exponent 2. Then $[xy, z][x, y][x, zy][y, z][x, y, z][z, y, x] = 1$. Thus in a Cayley–Dickson loop we have*

$$[x, y, z] = [z, y, x].$$

*Proof.* We have

$$\begin{aligned} xy \cdot z &= [xy, z]z \cdot xy = [xy, z][x, y]z \cdot yx = [xy, z][x, y][z, y, x]zy \cdot x \\ &= [xy, z][x, y][z, y, x][x, zy]x \cdot zy = [xy, z][x, y][z, y, x][x, zy][y, z]x \cdot yz \\ &= [xy, z][x, y][z, y, x][x, zy][y, z][x, y, z]xy \cdot z, \end{aligned}$$

and the first identity follows. In a Cayley–Dickson loop, if $\langle x, y, z\rangle$ is a group then we are done, else $[xy, z] = [x, y] = [x, zy] = [y, z] = -1$ by (2.4.1) and we are done. $\square$

**Lemma 2.4.5.** *Let $Q$ be a loop. Suppose that $cl(Q) \le 2$ and $Z(Q)$ has exponent 2. Then $[x, yz][y, zx][z, xy][x, y, z][y, z, x][z, x, y] = 1$. Thus in a Cayley–*

*Dickson loop, if $\langle x,y,z\rangle$ is not a group then*

$$[x,y,z][y,z,x][z,x,y] = -1.$$

*Proof.* We have

$$\begin{aligned} xy\cdot z &= [x,y,z]x\cdot yz = [x,y,z][x,yz]yz\cdot x \\ &= [x,y,z][x,yz][y,z,x]y\cdot zx = [x,y,z][x,yz][y,z,x][y,zx]zx\cdot y \\ &= [x,y,z][x,yz][y,z,x][y,zx][z,x,y]z\cdot xy \\ &= [x,y,z][x,yz][y,z,x][y,zx][z,x,y][z,xy]xy\cdot z, \end{aligned}$$

and the first identity follows. If we are in a Cayley–Dickson loop and $\langle x,y,z\rangle$ is not a group, the three commutators in the formula are all equal to $-1$ by (2.4.1). □

**Lemma 2.4.6.** *Let $Q$ be a loop. Suppose that $cl(Q)\le 2$ and $Z(Q)$ has exponent 2. Then for every $x$, $y$, $z$, $w\in Q$ we have $[xy,z,w][x,yz,w][x,y,zw] = [x,y,z][y,z,w]$.*

*Proof.* We have $xy\cdot zw = [x,y,zw]x(y\cdot zw) = [x,y,zw][y,z,w]x(yz\cdot w)$. On the other hand, we also have $xy\cdot zw = [xy,z,w](xy\cdot z)w = [xy,z,w][x,y,z](x\cdot yz)w = [xy,z,w][x,y,z][x,yz,w]x(yz\cdot w)$. □

**Lemma 2.4.7.** *In a Cayley–Dickson loop we have $[x,xy,z] = [x,y,z]$.*

*Proof.* We have $[x,xy,z]x^2\cdot yz = [x,xy,z]x^2y\cdot z = [x,xy,z](x\cdot xy)z = x(xy\cdot z) = [x,y,z]x\cdot x(yz) = [x,y,z]x^2\cdot yz$. □

**Lemma 2.4.8.** *In a Cayley–Dickson loop we have $[xy,y,xz] = [y,x,z]$.*

*Proof.* Note that $(xy)^2 = xyxy = [x,y]x^2y^2$. Then

$$\begin{aligned} y^2x^2 \cdot z &= y^2 \cdot x(xz) = xy^2 \cdot xz = (xy \cdot y) \cdot xz = [xy, y, xz]xy \cdot y(xz) \\ &= [xy, y, xz][y, x, z]xy \cdot (yx)z = [xy, y, xz][y, x, z][x, y]xy \cdot (xy)z \\ &= [xy, y, xz][y, x, z][x, y](xy)^2 z = [xy, y, xz][y, x, z]x^2y^2 \cdot z. \qquad \square \end{aligned}$$

**Lemma 2.4.9.** *In a Cayley–Dickson loop, the value of* $[xy, x, z]$ *is invariant under any permutation of* $x$, $y$, $z$. *In particular,* $[xy, x, z] = [xy, y, z]$.

*Proof.* We have $[yx, y, z] = [xy, y, z] = [xy, xy \cdot x, z]$ since $x^2$ is central. By Lemma 2.4.7 (with $x$ replaced with $xy$, and $y$ replaced with $x$), $[xy, xy \cdot x, z] = [xy, x, z]$. Thus $[xy, x, z] = [yx, y, z]$, and $[xy, x, z]$ is invariant under the transposition $(x, y)$. Now, $[yx, y, z] = [xy, y, z] = [xy, y, x \cdot xz]$, and by Lemma 2.4.8 (with $z$ replaced with $xz$), $[xy, y, x \cdot xz] = [y, x, xz]$, which equals to $[xz, x, y]$ by Lemma 2.4.4. Hence $[xy, x, z] = [xz, x, y]$, and $[xy, x, z]$ is invariant under the transposition $(y, z)$. $\square$

The next lemma is used to prove Lemmas 3.2.2 and 3.2.4.

**Lemma 2.4.10.** *If* $x, y, z \in Q_{n-1}$, *then in* $Q_n$ *we have*

*(a)* $[(x, 0), (y, 0), (z, 1)] = [x, y][z, y, x]$,

*(b)* $[(x, 0), (y, 1), (z, 0)] = [x, z][y, x, z][y, z, x]$,

*(c)* $[(x, 0), (y, 1), (z, 1)] = [x, y][x, z][z, x, y][x, z, y]$,

*(d)* $[(x, 1), (y, 0), (z, 0)] = [y, z][x, y, z]$,

*(e)* $[(x, 1), (y, 0), (z, 1)] = [y, x][y, z][z, y, x]$,

*(f)* $[(x, 1), (y, 1), (z, 0)] = [z, x][z, y][y, x, z][y, z, x]$,

*(g)* $[(x, 1), (y, 1), (z, 1)] = [x, y][x, z][y, z][z, x, y][x, z, y]$.

*Proof.* (a) $(x,0)(y,0)\cdot(z,1) = (xy,0)(z,1) = (z\cdot xy,1) = [x,y](z\cdot yx,1)$

$= [x,y][z,y,x](zy\cdot x,1) = [x,y][z,y,x]((x,0)(zy,1))$

$= [x,y][z,y,x]((x,0)\cdot(y,0)(z,1))$.

(b) $(x,0)(y,1)\cdot(z,0) = (yx,1)(z,0) = (yx\cdot z^*,1) = [y,x,z](y\cdot xz^*,1)$

$= [x,z][y,x,z](y\cdot z^*x,1) = [x,z][y,x,z][y,z,x](yz^*\cdot x,1)$

$= [x,z][y,x,z][y,z,x]((x,0)(yz^*,1)) = [x,z][y,x,z][y,z,x]((x,0)\cdot(y,1)(z,0))$.

(c) $(x,0)(y,1)\cdot(z,1) = (yx,1)(z,1) = (-z^*\cdot yx,0) = [x,y](-z^*\cdot xy,0)$

$= [x,y][z,x,y](-z^*x\cdot y,0) = [x,y][x,z][z,x,y](x(-z^*)\cdot y,0)$

$= [x,y][x,z][z,x,y][x,z,y](x\cdot(-z^*)y,0)$

$= [x,y][x,z][z,x,y][x,z,y]((x,0)\cdot(-z^*y,0))$

$= [x,y][x,z][z,x,y][x,z,y]((x,0)\cdot(y,1)(z,1))$.

(d) $(x,1)(y,0)\cdot(z,0) = (xy^*,1)(z,0) = (xy^*\cdot z^*,1) = [x,y,z](x\cdot y^*z^*,1)$

$= [x,y,z]((x,1)((y^*z^*)^*,0)) = [x,y,z]((x,1)(zy,0))$

$= [y,z][x,y,z]((x,1)(yz,0)) = [y,z][x,y,z]((x,1)\cdot(y,0)(z,0))$.

(e) $(x,1)(y,0)\cdot(z,1) = (xy^*,1)(z,1) = (-z^*\cdot xy^*,0) = [y,x](-z^*\cdot y^*x,0)$

$= [y,x][z,y,x](-z^*y^*\cdot x,0) = [y,x][z,y,x]((x,1)(-(-z^*y^*)^*,1))$

$= [y,x][z,y,x]((x,1)(yz,1)) = [y,x][y,z][z,y,x]((x,1)(zy,1))$

$= [y,x][y,z][z,y,x]((x,1)\cdot(y,0)(z,1))$.

(f) $(x,1)(y,1)\cdot(z,0) = (-y^*x,0)(z,0) = (-y^*x\cdot z,0) = [y,x,z](-y^*\cdot xz,0)$

$= [z,x][y,x,z](-y^*\cdot zx,0) = [z,x][y,x,z][y,z,x](-y^*z\cdot x,0)$

$= [z,x][y,x,z][y,z,x]((x,1)(-(-y^*z)^*,1)) = [z,x][y,x,z][y,z,x]((x,1)(z^*y,1))$

$= [z,x][z,y][y,x,z][y,z,x]((x,1)(yz^*,1)) = [z,x][z,y][y,x,z][y,z,x]((x,1)\cdot$
$(y,1)(z,0))$.

(g) $(x,1)(y,1)\cdot(z,1) = (-y^*x,0)(z,1) = (z\cdot(-y^*)x,1) = [x,y](z\cdot x(-y^*),1)$

$= [x,y][z,x,y](zx\cdot(-y^*),1) = [x,y][x,z][z,x,y](xz\cdot(-y^*),1)$

$$= [x,y][x,z][z,x,y][x,z,y](x \cdot z(-y^*),1)$$
$$= [x,y][x,z][z,x,y][x,z,y]((x,1)((z(-y^*))^*,0))$$
$$= [x,y][x,z][z,x,y][x,z,y]((x,1)(-yz^*,0))$$
$$= [x,y][x,z][y,z][z,x,y][x,z,y]((x,1)(-z^*y,0))$$
$$= [x,y][x,z][y,z][z,x,y][x,z,y]((x,1)\cdot(y,1)(z,1)). \qquad \square$$

## 2.5 Subloops

**Lemma 2.5.1.** *Let $B$ be a subloop of $Q_n$. The following hold:*

1. *the center $Z(Q_n) \le B$ for any $B \le Q_n, B \ne 1, n \ge 2$;*
2. *if $B \ne 1$ and $x \in Q_n \backslash B$, then $|\langle B,x\rangle| = 2|B|$;*
3. *if $B = 1$ and $x \in Q_n \backslash B$, then $\langle B,x\rangle = \{1,-1,x,-x\}$;*
4. *any $n$ elements of a Cayley–Dickson loop generate a subloop of order $2^k$, $k \le n+1$;*
5. *the order of $B$ is $2^m$ for some $m \le n$.*

*Proof.* 1. When $n \ge 2$, we have $Z(Q_n) = \{1,-1\}$ by Lemma 2.3.2, and $\{1,-1\} \le B$ for $B \ne 1$.

2. Let $1 \ne B \le Q_n$ and $x \in Q_n \backslash B$. By Lemma 2.3.2, $Z(Q_n) \le B$ and $Z(Q_n) \le \langle B,x\rangle$, then $B/Z(Q_n)$ and $\langle B,x\rangle/Z(Q_n)$ are subgroups of

$$Q_n/Z(Q_n) \cong (\mathbb{Z}_2)^n.$$

   It follows that $|\langle B,x\rangle/Z(Q_n)| = 2|B/Z(Q_n)|$ because we work in the vector space $(\mathbb{Z}_2)^n$ and we added another vector.

3. Let $B = 1$. If $x \ne -1$ then $x^2 = -1$ by Proposition 2.1.1 and $\langle B,x\rangle = \langle x\rangle = \{1,-1,x,-x\}$. Also, $\langle B,-1\rangle = \{1,-1\}$.

4. By induction on $n$. The order of $\langle x\rangle$ is $1,2$ or $4$. Suppose $n$ elements of a Cayley–Dickson loop generate a subloop $B$ of order $2^k$ for some $k\le n+1$. Add an element $x$ to $B$. If $x\in B$, then $|\langle B,x\rangle| = |B| = 2^k$, $k\le n+1\le n+2$. If $x\notin B$, then $|\langle B,x\rangle| = 2\,|B| = 2^{k+1}$, $k+1\le n+2$, by 2.

5. Follows from 4. $\square$

## 2.6 Cayley–Dickson Loops are Hamiltonian

We show that the Cayley–Dickson loops are Hamiltonian. Norton [33] formulated a number of theorems characterizing diassociative Hamiltonian loops and showed that the octonion loop is Hamiltonian; however, at that time he did not study the generalized Cayley–Dickson loops. It is shown computationally in [7] that $\mathbb{T}_{64}$ is Hamiltonian.

**Theorem 2.6.1.** *Every Cayley–Dickson loop $Q_n$ is Hamiltonian.*

*Proof.* By Theorem 2.3.1, the group $Q_n/Z(Q_n)$ is abelian, thus all its subgroups are normal. Then $Q_n$ is Hamiltonian by the Correspondence Theorem 1.2.6. $\square$

For an elementary proof of Theorem 2.6.1, let $S$ be a subloop of $Q_n$, $s\in S$, $x,y\in Q_n$. If $S$ is nontrivial, then either $S=\{1,-1\}$, or there is $x\ne\pm1$, such that $x\in S$, and $x^2=-1\in S$. Thus $-1\in S$. Using Lemma 2.4.2 and Lemma 2.3.2,

$$\begin{aligned}
xs &= [x,s]sx\in\{sx,-sx\}\subseteq Sx,\\
(xs)y &= [x,s,y]x(sy)\in\{x(sy),-x(sy)\}\subseteq x(Sy),\\
x(ys) &= [x,y,s](xy)s\in\{(xy)s,-(xy)s\}\subseteq(xy)S.
\end{aligned}$$

**Theorem 2.6.2** (Norton [33]). *A Hamiltonian diassociative loop $L$ is either an abelian group, or the direct product of an abelian group with elements of odd order and a loop $H$ with the following properties.*

1. *The commutant of $H$ consists of the elements of order 1 or 2.*

2. *If $x, y, z, \ldots$ are elements not in the commutant, then $x^2 = y^2 = z^2 = \ldots \neq 1$, $x^4 = y^4 = z^4 = \ldots = 1$.*

3. *If $x, y$ do not commute, then $\langle x, y \rangle$ is a quaternion group (since $H$ is assumed not abelian, there exists at least one such pair of elements). If $x, y$ commute, then $x = c_1 y$ where $c_1$ is an element of the commutant.*

4. *If $x, y$ do not commute and if $c_2$ is an element of $H$ which commutes with every element of $\langle x, y \rangle$, then $c_2$ is an element of the commutant.*

**Theorem 2.6.3** (Norton [33])**.** *If $A$ is an abelian group with elements of odd order, $T$ is an abelian group with exponent 2, and $K$ is a diassociative loop such that*

1. *elements of $K$ have order 1, 2 or 4,*

2. *there exist elements $x, y$ in $K$ such that $\langle x, y \rangle \cong \mathbb{H}_8$,*

3. *every element of $K$ of order 2 is in the center,*

4. *if $x, y, z \in K$ are of order 4, then $x^2 = y^2 = z^2$,*
   *$xy = d \cdot yx$ where $d = 1$ or $d = x^2$,*
   *and $xy \cdot z = h(x \cdot yz)$ where $h = 1$ or $h = x^2$,*

*then their direct product $A \times T \times K$ is a diassociative Hamiltonian loop.*

Theorem 2.6.3 with $A = T = 1$ can alternatively be used to establish Theorem 2.6.1 for all Cayley–Dickson loops.

# Chapter 3

# Automorphism Groups

In this section we study the automorphism groups of the Cayley–Dickson loops.

## 3.1 Motivation

Define the *orbit* of a set $X$ under the action of a group $G$ by $O_G(X) = \{gx \mid g \in G,\ x \in X\}$. Define the (pointwise) *stabilizer* of a set $X$ in $G$ by $G_X = \{g \in G \mid gx = x,\ x \in X\}$.

**Orbit-Stabilizer Theorem 3.1.1.** *[37, p.67] If $G$ is a finite group acting on a finite set $X$, then $|O_G(X)| = [G : G_X] = \frac{|G|}{|G_X|}$.*

We use Theorem 3.1.1 to find an upper bound on the size of $Aut(\mathbb{C}_4)$ and $Aut(\mathbb{H}_8)$. Let us first consider $G = Aut(\mathbb{C}_4)$. Any automorphism of $\mathbb{C}_4$ fixes 1 and $-1$ (1 is the only element of order 1, and $-1$ is the only element of order 2), therefore it is only possible for an automorphism to map $i_1 \mapsto i_1$ (e.g., the identity mapping), and $i_1 \mapsto -i_1$ (e.g., conjugation). The size of the orbit $O_G(i_1)$ is therefore 2. Note that $G_{\{i_1\}} = G_{\mathbb{C}_4}$, since $\mathbb{C}_4$ is generated by $i_1$. It follows that

$$|G| = |O_G(i_1)| \cdot \left|G_{\{i_1\}}\right| = |O_G(i_1)| = 2.$$

Next, let $G = Aut(\mathbb{H}_8)$. Again, 1 and $-1$ are fixed by any automorphism and are not in $O_G(i_1)$, therefore the size of $|O_G(i_1)|$ can be at most $|\mathbb{H}_8| - 2 = 6$. When $i_1$ is stabilized, $\left|G_{\{i_1\}}\right| = \left|O_{G_{\{i_1\}}}(i_2)\right| \cdot \left|G_{\{i_1,i_2\}}\right|$, moreover, $G_{\{i_1,i_2\}} = G_{\mathbb{H}_8}$, since $\mathbb{H}_8$ is generated by $\{i_1, i_2\}$. The orbit $O_{G_{\{i_1\}}}(i_2)$ can have the size at most $|\mathbb{H}_8| - 4 = 4$, because the set $\{1, -1, i_1, -i_1\}$ is fixed. We have

$$
\begin{aligned}
|G| &= |O_G(i_1)| \cdot \left|G_{\{i_1\}}\right| = |O_G(i_1)| \cdot \left|O_{G_{\{i_1\}}}(i_2)\right| \cdot \left|G_{\{i_1,i_2\}}\right| \\
&= |O_G(i_1)| \cdot \left|O_{G_{\{i_1\}}}(i_2)\right| \leq 6 \cdot 4 = 24.
\end{aligned}
\tag{3.1.1}
$$

It has been shown, in fact, (see, e.g., [43]), that $Aut(\mathbb{H}_8)$ is isomorphic to the symmetric group $S_4$ of order 24.

Recall that the *special linear group* $SL_2(7)$ is the group of invertible $2 \times 2$ matrices over the finite field with 7 elements having a unit determinant. Let $I$ be the identity matrix of $SL_2(7)$. Then the *projective special linear group* $PSL_2(7)$ is a quotient group $SL_2(7)/\{I, -I\}$; it is a nonabelian simple group of order 168. The group $PSL_2(7)$ is the group of symmetries of the Fano plane, and has important applications in algebra and geometry. It has been established in [27] that $Aut(\mathbb{O}_{16})$ has order 1344 and is an extension of the elementary abelian group $(\mathbb{Z}_2)^3$ of order 8 by $PSL_2(7)$. One can use an approach similar to (3.1.1) to see what $Aut(\mathbb{O}_{16})$ looks like.

To get an idea about the general case, we calculated the automorphism groups of $\mathbb{S}_{32}$ and $\mathbb{T}_{64}$ using LOOPS package for GAP. This information is summarized in Table 3.1. One may notice that the automorphism groups of $\mathbb{C}_4$, $\mathbb{H}_8$ and $\mathbb{O}_{16}$ are as big as they possibly can be, subject to the obvious structural restrictions in $\mathbb{C}_4, \mathbb{H}_8, \mathbb{O}_{16}$. On the contrary, the automorphism groups of $\mathbb{S}_{32}$ and $\mathbb{T}_{64}$ are only double the size of the preceding ones. Theorem 3.1.2 below explains such behavior.

| $Q_n$ | Size of $Aut(Q_n)$ | Structure of $Aut(Q_n)$ |
|---|---|---|
| $\mathbb{C}_4$ | 2 | $\mathbb{Z}_2$ |
| $\mathbb{H}_8$ | 24 | $\mathbb{S}_4$ |
| $\mathbb{O}_{16}$ | $1344 = 8 \cdot 168$ | Extension of $(\mathbb{Z}_2)^3$ by $PSL_2(7)$ |
| $\mathbb{S}_{32}$ | $2688 = 1344 \cdot 2$ | $Aut(\mathbb{O}_{16}) \times \mathbb{Z}_2$ |
| $\mathbb{T}_{64}$ | $5376 = 2688 \cdot 2$ | $Aut(\mathbb{S}_{32}) \times \mathbb{Z}_2$ |

Table 3.1: Automorphism groups of $Q_n$, $n \leq 5$

Recall that we use

$$e = i_n$$

to denote the unit added in the $n-th$ step of the doubling construction.

**Theorem 3.1.2.** *Let $n \geq 4$. If $\phi : Q_n \to Q_n$ is an automorphism and $\psi = \phi \restriction_{Q_{n-1}}$, then*

1. $\phi(1) = 1$, $\phi(-1) = -1$,
2. $\phi(e) = e$ *or* $\phi(e) = -e$,
3. $\psi \in Aut(Q_{n-1})$,
4. $\phi((x,1)) = \psi(x)\phi(e), \forall x \in Q_{n-1}$.

*See Figure 3.1.*

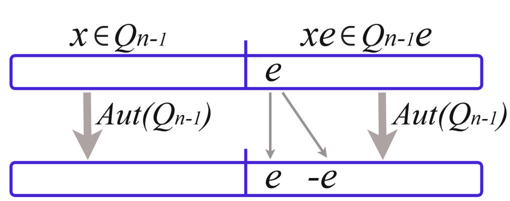


Figure 3.1: Automorphism group of $Q_n$, $n \geq 4$

## 3.2 Octonion and Quasioctonion Loops

We establish several auxiliary results and use them to prove Theorem 3.1.2 at the end of the chapter. The following lemma shows that all subloops of $Q_n$ of order 16 fall into two isomorphism classes. In particular, any such subloop is either isomorphic to $\mathbb{O}_{16}$, the octonion loop, or $\tilde{\mathbb{O}}_{16}$, the quasioctonion loop, described in [6, 10]. The octonion loop is Moufang; however, the quasioctonion loop is not. We take $\langle i_1, i_2, i_3\rangle = \pm\{1, i_1, i_2, i_1i_2, i_3, i_1i_3, i_2i_3, i_1i_2i_3\}$ as a canonical octonion loop, and $\langle i_1, i_2, i_3i_4\rangle = \pm\{1, i_1, i_2, i_1i_2, i_3i_4, i_1i_3i_4, i_2i_3i_4, i_1i_2i_3i_4\}$ as a canonical quasioctonion loop in $\mathbb{S}_{32}$. We use LOOPS package for GAP [32] in Lemma 3.2.1 and further in the text to establish the isomorphisms between the subloops we construct, and either $\mathbb{O}_{16}$ or $\tilde{\mathbb{O}}_{16}$. Suppose $S$ is a subloop of order $2^n$ in a Cayley–Dickson loop. We want to extend it to a subloop $T$ of order $2^{n+1}$ by adjoining an element $z$. Then $T = S \cup Sz$. The multiplication in $T$ is given by

$$
\begin{aligned}
x \cdot y &= xy,\\
x \cdot yz &= [x, y, z](xy)z,\\
xz \cdot y &= [y, xz]y \cdot xz = [y, xz][y, x, z]yx \cdot z,\\
xz \cdot yz &= [y, z]xz \cdot zy = [y, z][x, z, zy]x(z \cdot zy) = -[y, z][x, z, zy]xy,
\end{aligned}
$$

where $x,\ y \in S$. Because the commutators $[x, y] = -1$ when $y \notin \langle x\rangle$, all we need in order to specify the multiplication in $T$ are the associators $[x, y, z]$, $[x, z, zy]$ for $x,\ y \in S$. By Lemmas 2.4.4 and 2.4.9, $[x, z, zy] = [zy, z, x] = [xy, x, z]$, so we only need to know the associators $[x, y, z]$ for $x,\ y \in S$. Recall that $|\langle x, y, z\rangle| \le 16$ for $x, y, z \in Q_n$.

**Lemma 3.2.1.** *If $x, y, z$ are elements of $Q_n$ such that $|\langle x, y, z\rangle| = 16$, then either*

$$\langle x, y, z\rangle \cong \mathbb{O}_{16} \ \text{or}\ \langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}.$$

*Proof.* Suppose that $S$ is a subloop of $Q_n$ of order 8, $S = \pm\{1, x, y, xy\}$. We need to know the following associators to determine a loop $T = \langle S, z\rangle$:

$$[x, y, z],$$

$$[x, xy, z] = [x, y, z], \text{ (Lemma 2.4.7)}$$

$$[y, x, z],$$

$$[y, xy, z] = [y, yx, z] = [y, x, z], \text{ (Lemma 2.4.7)}$$

$$[xy, x, z],$$

$$[xy, y, z] = [xy, x, z]. \text{ (Lemma 2.4.7)}$$

Thus all we need to describe $T$ are the 3 associators $[x, y, z]$, $[y, x, z]$, $[xy, y, z]$, this can be seen in Table 3.2. For example,

$$\begin{aligned}
(xy)(xz) &= -[xy, x, z](x(xy))z = [xy, x, z]yz, \\
(xy)(yz) &= [xy, y, z]((xy)y)z = -[xy, y, z]xz = -[xy, x, z]xz, \\
x((xy)z) &= [x, xy, z](x(xy))z = -[x, y, z]yz, \\
y((xy)z) &= -[y, xy, z]((xy)y)z = [y, x, z]xz, \\
(xz)((xy)z) &= [x(xy), x, z]x(xy) = -[y, x, z]y, \\
(yz)((xy)z) &= [y(xy), y, z]y(xy) = [x, y, z]x, \\
(xz)(yz) &= [xy, x, z]xy.
\end{aligned}$$

If $[x, y, z] = [y, x, z] = [xy, x, z] = -1$, then $\langle x, y, z\rangle \cong \mathbb{O}_{16}$ by $\{x, y, z\} \mapsto \{i_1, i_2, i_3\}$.
If $[x, y, z] = [y, x, z] = -1$, $[xy, x, z] = 1$, then $\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{xy, xz, x\} \mapsto \{i_1, i_2, i_3 i_4\}$.
If $[x, y, z] = [xy, x, z] = -1$, $[y, x, z] = 1$, then $\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{y, xz, x\} \mapsto \{i_1, i_2, i_3 i_4\}$.

If $[x,y,z] = -1$, $[y,x,z] = [xy,x,z] = 1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{x,z,y\} \mapsto \{i_1,i_2,i_3i_4\}$.
If $[x,y,z] = 1$, $[y,x,z] = [xy,x,z] = -1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{x,yz,y\} \mapsto \{i_1,i_2,i_3i_4\}$.
If $[x,y,z] = [xy,x,z] = 1$, $[y,x,z] = -1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{y,z,x\} \mapsto \{i_1,i_2,i_3i_4\}$.
If $[x,y,z] = [y,x,z] = 1$, $[xy,x,z] = -1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{xy,z,x\} \mapsto \{i_1,i_2,i_3i_4\}$.
If $[x,y,z] = [y,x,z] = [xy,x,z] = 1$, then $\langle x,y,z\rangle \cong \tilde{\mathbb{O}}_{16}$ by $\{x,y,z\} \mapsto \{i_1,i_2,i_3i_4\}$.

| $1$ | $x$ | $y$ | $xy$ | $z$ | $xz$ | $yz$ | $(xy)z$ |
|---|---|---|---|---|---|---|---|
| $x$ | $-1$ | $xy$ | $-y$ | $xz$ | $-z$ | $[x,y,z](xy)z$ | $-[x,y,z]yz$ |
| $y$ | $-xy$ | $-1$ | $x$ | $yz$ | $-[y,x,z](xy)z$ | $-z$ | $[y,x,z]xz$ |
| $xy$ | $y$ | $-x$ | $-1$ | $(xy)z$ | $[xy,x,z]yz$ | $-[xy,x,z]xz$ | $-z$ |
| $z$ | $-xz$ | $-yz$ | $-(xy)z$ | $-1$ | $x$ | $y$ | $xy$ |
| $xz$ | $z$ | $[y,x,z](xy)z$ | $-[xy,x,z]yz$ | $-x$ | $-1$ | $[xy,x,z]xy$ | $-[y,x,z]y$ |
| $yz$ | $-[x,y,z](xy)z$ | $z$ | $[xy,x,z]xz$ | $-y$ | $-[xy,x,z]xy$ | $-1$ | $[x,y,z]x$ |
| $(xy)z$ | $[x,y,z]yz$ | $-[y,x,z]xz$ | $z$ | $-xy$ | $[y,x,z]y$ | $-[x,y,z]x$ | $-1$ |

Table 3.2: Multiplication table of $\langle x,y,z\rangle$ of order 16

$\square$

The well-known multiplication Fano plane mnemonic for the octonion loop is shown in Figure 3.2. The plane contains 7 vertices (representing non-identity octonion units) and 7 lines (representing multiplication of these units). Exactly three lines go through every vertex, and there are exactly three vertices on every line. The arrows point in the direction of multiplication. To memorize the triples of adjacent vertices, one needs to remember that $1 \cdot 2 = 4$, the anticommutativity

$$j \cdot k = m \Rightarrow k \cdot j = -m,$$

and the index cycling identity

$$j \cdot k = m \Rightarrow (j+1)\cdot(k+1) = (m+1) \quad \mod \quad 7, \quad j,k,m \in \{1,\ldots 7\}$$

The mnemonic together with the facts that 1 is the multiplicative identity, and that

$\{1, \ldots 7\}$ are square roots of $-1$, completely determines the multiplication table of the octonion loop.

The Fano plane mnemonic for the quasioctonion loop is shown in Figure 3.3. All arrows except $(1, 2, 4)$ are reversed compared to the octonion plane.

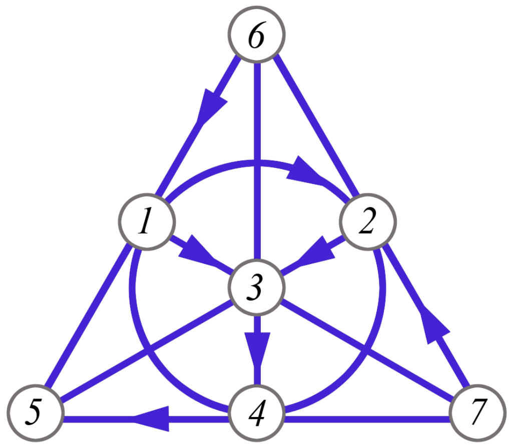


Figure 3.2: Octonion loop multiplication Fano plane

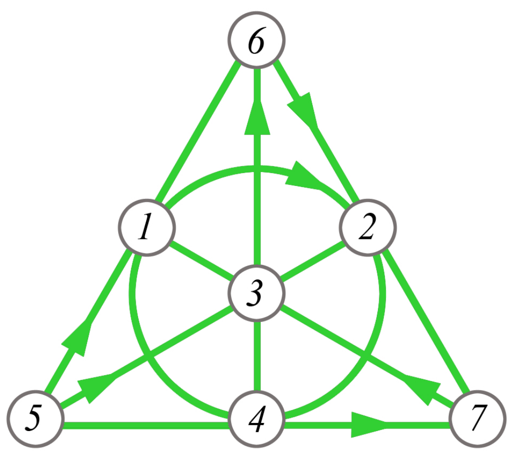


Figure 3.3: Quasioctonion loop multiplication Fano plane

Lemma 3.2.2 shows that $e \in Q_n$ is special; if we consider a subloop $\langle x, y, e\rangle$ of $Q_n$ such that $|\langle x, y, e\rangle| = 16$, then $\langle x, y, e\rangle$ is always a copy of the octonion loop $\mathbb{O}_{16}$. Lemma 3.3.5 shows that this, however, is not the case for any element of $Q_n \backslash \{\pm e\}$. Therefore, an automorphism on $Q_n$ cannot map $e$ to an element $x \in Q_n \backslash \{\pm e\}$. Also, we use Lemma 3.3.4 to show that an automorphism on $Q_n$ cannot map an element $x$ to $ye$ for any $x, y \in Q_{n-1}$.

**Lemma 3.2.2.** $\langle x, y, e\rangle \cong \mathbb{O}_{16}$ *for any* $x, y \in Q_n$ *such that* $e \notin \langle x, y\rangle \cong \mathbb{H}_8$.

*Proof.* Let $x, y$ be elements of $Q_n$ such that $e \notin \langle x, y\rangle \cong \mathbb{H}_8$. As follows from the proof of Lemma 3.2.1, in order to prove that $\langle x, y, e\rangle \cong \mathbb{O}_{16}$, it is sufficient to show that

$$[x, y, e] = [x, e, y] = [x, y, xe] = -1.$$

Let $\overline{x}, \overline{y}$ be elements of $Q_{n-1}$. We use Lemma 2.4.10, and consider the following cases:

If $x = (\overline{x}, 0), y = (\overline{y}, 0)$, then $xe = (\overline{x}, 0)(1, 1) = (\overline{x}, 1)$, and

$$\begin{aligned}
[x, y, e] &= [(\overline{x}, 0), (\overline{y}, 0), (1, 1)] = [\overline{x}, \overline{y}][1, \overline{y}, \overline{x}] = -1, \\
[x, e, y] &= [(\overline{x}, 0), (1, 1), (\overline{y}, 0)] = [\overline{x}, \overline{y}][1, \overline{x}, \overline{y}][1, \overline{y}, \overline{x}] = -1, \\
[x, y, xe] &= [(\overline{x}, 0), (\overline{y}, 0), (\overline{x}, 1)] = [\overline{x}, \overline{y}][\overline{x}, \overline{y}, \overline{x}] = -1.
\end{aligned}$$

If $x = (\overline{x}, 0), y = (\overline{y}, 1)$, then $xe = (\overline{x}, 0)(1, 1) = (\overline{x}, 1)$, and

$$\begin{aligned}
[x, y, e] &= [(\overline{x}, 0), (\overline{y}, 1), (1, 1)] = [\overline{x}, \overline{y}][\overline{x}, 1][1, \overline{x}, \overline{y}][\overline{x}, 1, \overline{y}] = -1, \\
[x, e, y] &= [(\overline{x}, 0), (1, 1), (\overline{y}, 1)] = [\overline{x}, 1][\overline{x}, \overline{y}][\overline{y}, \overline{x}, 1][\overline{x}, \overline{y}, 1] = -1, \\
[x, y, xe] &= [(\overline{x}, 0), (\overline{y}, 1), (\overline{x}, 1)] = [\overline{x}, \overline{y}][\overline{x}, \overline{x}][\overline{x}, \overline{x}, \overline{y}][\overline{x}, \overline{x}, \overline{y}] = -1.
\end{aligned}$$

If $x = (\overline{x}, 1), y = (\overline{y}, 0)$, then $xe = (\overline{x}, 1)(1, 1) = (-\overline{x}, 0)$, and

$$\begin{aligned}
[x, y, e] &= [(\overline{x}, 1), (\overline{y}, 0), (1, 1)] = [\overline{y}, \overline{x}][\overline{y}, 1][1, \overline{y}, \overline{x}] = -1, \\
[x, e, y] &= [(\overline{x}, 1), (1, 1), (\overline{y}, 0)] = [\overline{y}, \overline{x}][\overline{y}, 1][1, \overline{x}, \overline{y}][1, \overline{y}, \overline{x}] = -1, \\
[x, y, xe] &= [(\overline{x}, 1), (\overline{y}, 0), (-\overline{x}, 0)] = [\overline{y}, -\overline{x}][\overline{x}, \overline{y}, -\overline{x}] = -1.
\end{aligned}$$

If $x = (\overline{x}, 1), y = (\overline{y}, 1)$, then $xe = (\overline{x}, 1)(1, 1) = (-\overline{x}, 0)$, and

$$\begin{aligned}
[x, y, e] &= [(\overline{x}, 1), (\overline{y}, 1), (1, 1)] = [\overline{x}, \overline{y}][\overline{x}, 1][\overline{y}, 1][1, \overline{x}, \overline{y}][\overline{x}, 1, \overline{y}] = -1, \\
[x, e, y] &= [(\overline{x}, 1), (1, 1), (\overline{y}, 1)] = [\overline{x}, 1][\overline{x}, \overline{y}][1, \overline{y}][\overline{y}, \overline{x}, 1][\overline{x}, \overline{y}, 1] = -1, \\
[x, y, xe] &= [(\overline{x}, 1), (\overline{y}, 1), (-\overline{x}, 0)] = [-\overline{x}, \overline{x}][-\overline{x}, \overline{y}][\overline{y}, \overline{x}, -\overline{x}][\overline{y}, -\overline{x}, \overline{x}] = -1.
\end{aligned}$$

We conclude that $[x, y, e] = [x, e, y] = [x, y, xe] = -1$ for any $x, y \in Q_n$ such that $e \notin \langle x, y \rangle \cong \mathbb{H}_8$. By Lemma 3.2.1, $\langle x, y, e \rangle \cong \mathbb{O}_{16}$ by $\{x, y, e\} \mapsto \{i_1, i_2, i_3\}$. $\square$

The immediate consequence of Lemma 3.2.2 is that any three distinct canonical generators produce the octonion loop. We do not use this fact, but it might give some information about isomorphism classes of subloops of $Q_n$ in future.

**Corollary 3.2.3.** *Let $Q_n$ be a Cayley–Dickson loop, $n \geq 3$, and let $i_j, i_k, i_m$ be its distinct canonical generators. Then $\langle i_j, i_k, i_m \rangle \cong \mathbb{O}_{16}$.*

*Proof.* Without loss of generality, let $m > k, j$. Then $Q_n \restriction_{\langle i_1, i_2, \ldots, i_m \rangle} \cong Q_m$. Also, $i_j, i_k \in Q_m$, and $i_m \notin \langle i_j, i_k \rangle \cong \mathbb{H}_8$. By Lemma 3.2.2, $\langle i_j, i_k, e \rangle \cong \mathbb{O}_{16}$, where $e = i_m = (1_{Q_{m-1}}, 1) \in Q_m$. $\square$

The following lemma helps to distinguish between some copies of $\mathbb{O}_{16}$ and $\tilde{\mathbb{O}}_{16}$, and is used to prove Lemmas 3.3.4 and 3.3.5.

**Lemma 3.2.4.** *Let $x,y,z \in Q_{n-1}$, $n \geq 4$ be such that $\langle x,y,z\rangle \cong \mathbb{O}_{16}$. Then in $Q_n$*

$$\begin{aligned}\langle (x,0),(y,0),(z,0)\rangle &\cong \langle (x,1),(y,1),(z,1)\rangle \cong \mathbb{O}_{16},\\ \langle (x,0),(y,0),(z,1)\rangle &\cong \langle (x,0),(y,1),(z,1)\rangle \cong \tilde{\mathbb{O}}_{16}.\end{aligned}$$

*Proof.* Let $x,y,z \in Q_{n-1}$ be such that $\langle x,y,z\rangle \cong \mathbb{O}_{16}$. By Lemma 2.4.2, $[x,y,z] = [x,z,y] = [y,x,z] = -1$, and $[x,y] = [y,z] = [x,z] = -1$. Using Lemma 2.4.10,

$$[(x,0),(z,1),(y,0)] = [x,y][z,x,y][z,y,x] = -1 \tag{3.2.1}$$

shows that $\langle (x,0),(y,0),(z,1)\rangle > \mathbb{H}_8$ and hence $|\langle (x,0),(y,0),(z,1)\rangle| = 16$, while

$$[(x,0),(y,0),(z,1)] = [x,y][z,y,x] = 1 \tag{3.2.2}$$

shows that $\langle (x,0),(y,0),(z,1)\rangle$ is not Moufang and therefore $\langle (x,0),(y,0),(z,1)\rangle \cong \tilde{\mathbb{O}}_{16}$. Similarly, using Lemma 2.4.10,

$$\begin{aligned}[(y,1),(x,0),(z,1)] &= [x,y][x,z][z,x,y] = -1, && (3.2.3)\\ [(x,0),(y,1),(z,1)] &= [x,y][x,z][z,x,y][x,z,y] = 1 && (3.2.4)\end{aligned}$$

shows that $\langle (x,0),(y,1),(z,1)\rangle \cong \tilde{\mathbb{O}}_{16}$.

A loop $\langle (x,0),(y,0),(z,0)\rangle \cong \mathbb{O}_{16}$ is a copy of $\langle x,y,z\rangle$ in $Q_n$.

A loop $\langle (x,1),(y,1),(z,1)\rangle \cong \mathbb{O}_{16}$ by $\{(x,1),(y,1),(z,1)\} \mapsto \{i_1,i_2,i_3\}$. □

## 3.3 Subloops of Index 2

Let $B$ be a subloop of $Q_n$ of index 2 and $D$ be a subloop of $Q_{n-1}$ of index 2. One calls $B$ a *subloop of the first type* when $B = Q_{n-1}$, a *subloop of the second type* when $B = D \cup De$, a *subloop of the third type* when $B = D \cup (Q_{n-1}\backslash D)\,e$ (see Figure 3.4).

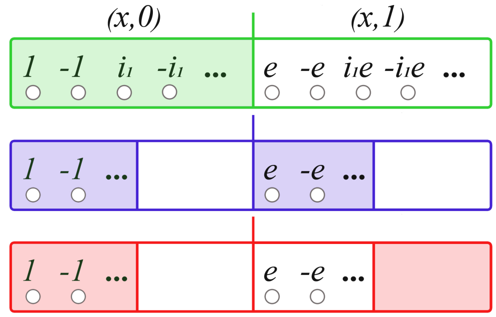


Figure 3.4: Three types of subloops of $Q_n$

Figure 3.5 illustrates all subloops of index 2 of the sedenion loop $\mathbb{S}_{32}$. Rows in the figure correspond to the subloops, columns show the elements these subloops contain. One may notice that each of the subloops is of one of three types. The following lemma shows that this is the case for all Cayley–Dickson loops.

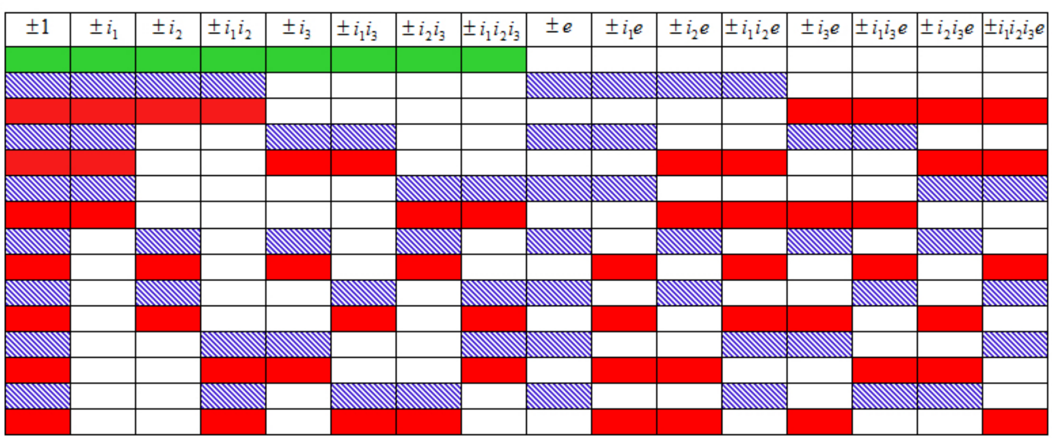


Figure 3.5: Subloops of $\mathbb{S}_{32}$ of index 2

**Lemma 3.3.1.** *Let $H$ be an elementary abelian 2-group, let $Q = H \times \mathbb{Z}_2$, and let $S$ be a subgroup of $Q$ of index 2. Then either $S = H \times 0$ or $|S \cap (H \times 0)| = |S \cap (H \times 1)| = \frac{|S|}{2}$.*

*Proof.* If $S = H \times 0$, we are done. Else let $x = (h, 1) \in S$, $A = S \cap (H \times 0)$, $B = S \cap (H \times 1)$.

Note that $xA \subseteq B$, $xB \subseteq A$. Since the left translation $L_x$ is injective, it follows that $|A| \leq |B|$ and $|B| \leq |A|$, i.e., $|A| = |B| = \frac{|S|}{2}$. $\square$

**Lemma 3.3.2.** *Let $S$ be a subloop of $Q_n$ of index 2, then either $S$ is a subloop of $Q_{n-1}$ or $|S \cap Q_{n-1}| = |S \cap Q_{n-1}e| = \frac{|S|}{2}$.*

*Proof.* Barring trivialities, $Z(Q_n) \leq S$. The statement holds in $Q_n/Z(Q_n)$ by Lemma 3.3.1, hence also in $Q_n$ by the Correspondence Theorem 1.2.6. $\square$

**Lemma 3.3.3.** *If $B$ is a subloop of $Q_n$ of index 2, then $B$ is a subloop of either the first, or the second, or the third type.*

*Proof.* If $B = Q_{n-1}$, it is of the first type. Suppose $B \neq Q_{n-1}$. Let $C = B \cap Q_{n-1}$. By Lemma 3.3.2, $|C| = \frac{|B|}{2}$. If $e \in B$ then $B = C \cup Ce$, a subloop of the second type. Else $C \cap Ce = \varnothing$, so $B = C \cup (Q_{n-1} \backslash C)e$, a subloop of the third type. $\square$

Next, we show that, starting at $\mathbb{S}_{32}$, any subloop of $Q_n$ of the third type is not a Cayley–Dickson loop.

**Lemma 3.3.4.** *Let $B \neq Q_{n-1}$ be a subloop of $Q_n$ of index 2 and $D$ be a subloop of $Q_{n-1}$ of index 2, $n \geq 4$.*

1. *For any $x \in Q_{n-1}$, $x \neq \pm 1$ there exist $y, z \in Q_{n-1}$ such that $\langle x, y, z\rangle \cong \mathbb{O}_{16}$, $\{x, y, z\} \cap D \neq \varnothing$ and $\{x, y, z\} \cap (Q_{n-1} \backslash D) \neq \varnothing$.*
2. *If $e \notin B$ then for any $x \in B$, $x \neq \pm 1$ there exist $y, z \in B$ such that $\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}$.*
3. *If $e \notin B$ then $B \ncong Q_{n-1}$. In particular, any subloop of the third type is not a Cayley–Dickson loop.*

*Proof.* 1. The order of $D$ is $\frac{|Q_{n-1}|}{2} \geq 8$. Let $i_{n-1} \in Q_{n-1}$. If $x \in D$, choose $y \notin D \cup \langle i_{n-1}, x\rangle$, then $\langle i_{n-1}, x, y\rangle \cong \mathbb{O}_{16}$ by Lemma 3.2.2. Similarly, if $x \notin D$, choose $y \in D$, $y \notin \langle i_{n-1}, x\rangle$, then $\langle i_{n-1}, x, y\rangle \cong \mathbb{O}_{16}$ by Lemma 3.2.2. If $x = i_{n-1}$, choose $y \notin D \cup \langle i_{n-1}\rangle$ and $z \in D \backslash \langle i_{n-1}, y\rangle$, then $\langle i_{n-1}, x, y\rangle \cong \mathbb{O}_{16}$ by Lemma 3.2.2.

2. By Lemma 3.3.3, $B = D \cup (Q_{n-1} \backslash D)\, e$ for some subloop $D$ of $Q_{n-1}$ of index 2. Let $x \in B$, $x \neq \pm 1$, then either $x = (\bar{x}, 0)$ or $x = (\bar{x}, 1)$ for some $\pm 1 \neq \bar{x} \in Q_{n-1}$. By 1 there exist $y, z \in Q_{n-1}$ such that $\langle \bar{x}, y, z \rangle \cong \mathbb{O}_{16}$, $\{\bar{x}, y, z\} \cap D \neq \varnothing$ and $\{\bar{x}, y, z\} \cap (Q_{n-1} \backslash D) \neq \varnothing$. Without loss of generality, suppose $y \in D$ and $z \in Q_{n-1} \backslash D$, then either $(\bar{x}, 0), (y, 0), (z, 1) \in B$ or $(\bar{x}, 1), (y, 0), (z, 1) \in B$. Using (3.2.1), (3.2.2), (3.2.3), (3.2.4) we have either

$$\begin{aligned} \langle (\bar{x}, 0), (y, 0), (z, 1) \rangle &\cong \tilde{\mathbb{O}}_{16} \text{ or} \\ \langle (\bar{x}, 1), (y, 0), (z, 1) \rangle &\cong \tilde{\mathbb{O}}_{16}. \end{aligned}$$

3. By Lemma 3.2.2, there is an element $i_{n-1} \in Q_{n-1}$ such that for any $x, y \in Q_{n-1}$, $|\langle i_{n-1}, x, y \rangle| = 16$ implies that $\langle i_{n-1}, x, y \rangle \cong \mathbb{O}_{16}$. However, by 2, $B$ does not contain such an element. $\square$

**Lemma 3.3.5.** *Let $x \in Q_n \backslash \{\pm 1, \pm e\}$, $n \geq 4$. There exist $y, z \in Q_n$ such that $\langle x, y, z \rangle \cong \tilde{\mathbb{O}}_{16}$.*

*Proof.* Without loss of generality, suppose $x \in Q_{n-1}$. By Lemma 3.3.4 part 1, there exist $y, z \in Q_{n-1}$ such that $\langle x, y, z \rangle \cong \mathbb{O}_{16}$. Using (3.2.1), (3.2.2), we have $\langle (x, 0), (y, 0), (z, 1) \rangle \cong \tilde{\mathbb{O}}_{16}$. $\square$

## 3.4 Automorphism Groups

Define the following mappings on $Q_n$:

$$\begin{aligned} (id, -id) &: (x, x_{n+1}) \mapsto ((-1)^{x_{n+1}} x, x_{n+1}), \\ (id, id) &: (x, x_{n+1}) \mapsto (x, x_{n+1}), \end{aligned}$$

where $x \in Q_{n-1}$ and $x_{n+1} \in \{0,1\}$. The mapping $(id, id)$ is an identity; the mapping $(id, -id)$ is an automorphism, as can be seen in Lemma 3.4.1.

**Lemma 3.4.1.** *Let $Q_n$ be a Cayley–Dickson loop, let $x \in Q_{n-1}$, $x_{n+1} \in \{0,1\}$. Then the mapping $\phi = (id, -id) : (x, x_{n+1}) \mapsto ((-1)^{x_{n+1}} x, x_{n+1})$ is an automorphism on $Q_n$.*

*Proof.* We need to consider the following cases:

$$\begin{aligned}
\phi((x,0)(y,0)) &= \phi((xy,0)) = (xy,0) = (x,0)(y,0) = \phi((x,0))\phi((y,0)),\\
\phi((x,0)(y,1)) &= \phi((yx,1)) = (-yx,1) = (x,0)(-y,1) = \phi((x,0))\phi((y,1)),\\
\phi((x,1)(y,0)) &= \phi((xy^*,1)) = (-xy^*,1) = (-x,1)(y,0) = \phi((x,1))\phi((y,0)),\\
\phi((x,1)(y,1)) &= \phi((-y^*x,0)) = (-y^*x,0) = (-x,1)(-y,1) = \phi((x,1))\phi((y,1)).\square
\end{aligned}$$

*Proof.* (of Theorem 3.1.2) Let $\phi : Q_n \to Q_n$, $n \geq 4$, be an automorphism.

1. By Proposition 2.1.1, $\phi(1) = 1$, $\phi(-1) = -1$.

2. Let $x \in Q_n \setminus \{\pm 1, \pm e\}$. By Lemma 3.3.5, there exist $y, z \in Q_n$ such that $\langle x, y, z\rangle \cong \tilde{\mathbb{O}}_{16}$, however, by Lemma 3.2.2, $\langle e, y, z\rangle \cong \mathbb{O}_{16}$ for any $y, z \in Q_n$. Therefore it is only possible that $\phi(e) = e$, which holds when $\phi$ is an identity mapping, or $\phi(e) = -e$, which holds when $\phi = (id, -id)$.

3. Consider the subloops of $Q_n$ of index 2. For $x \in Q_n$, let $\chi(x)$ denote the number of such subloops isomorphic to $Q_{n-1}$ containing $x$. By Lemma 3.3.4, any subloop of the third type is not isomorphic to $Q_{n-1}$. The subloop of the first type (there is only one such subloop) is a copy of $Q_{n-1}$ in $Q_n$ of the form $\{x \mid x \in Q_{n-1}\}$. If $B$ is a subloop of the second type, then for any $x \in Q_{n-1}$ we have $x \in B$ if and only if $xe \in B$. Thus for $x \in Q_{n-1}$ we have $\chi(xe) = \chi(x) - 1$. Let us show that if $x \in Q_{n-1}$ and $\phi \in Aut(Q_n)$, then $\phi(x) \in Q_{n-1}$. Suppose

that $\phi(x) = ye$ for some $y \in Q_{n-1}$. Then

$$\chi(x) = \chi(\phi(x)) = \chi(ye) = \chi(y) - 1, \tag{3.4.1}$$

but we also have

$$\begin{aligned} \phi(xe) &= \phi(x)\phi(e) = \pm(ye)e = \pm y, \\ \chi(y) &= \chi(\phi(xe)) = \chi(xe) = \chi(x) - 1, \end{aligned} \tag{3.4.2}$$

thus (3.4.1) and (3.4.2) lead to contradiction.

4. Let $x \in Q_{n-1}$. Using the multiplication formula (1.4.3), $xe = (x,0)(1,1) = (x,1)$. If $\phi$ is an automorphism on $Q_n$, then

$$\phi((x,1)) = \phi((x,0)(1,1)) = \phi((x,0))\phi((1,1)) = \psi(x)\phi(e). \qquad \square$$

Recall the following proposition.

**Proposition 3.4.2** ([16])**.** *A group $G$ is a direct product of groups $N$ and $K$ iff*

1. *$N$ and $K$ are normal subgroups of $G$,*
2. *$G = NK$,*
3. *$N \cap K = id$, the trivial subgroup of $G$.*

Finally, we show that, starting at $\mathbb{S}_{32}$, $Aut(Q_n)$ is a direct product of $Aut(Q_{n-1})$ and a cyclic group of order 2.

**Theorem 3.4.3.** *Let $Q_n$ be a Cayley–Dickson loop and let $n \geq 4$. Then $Aut\,(Q_n) \cong Aut\,(Q_{n-1}) \times \mathbb{Z}_2 \cong Aut(\mathbb{O}_{16}) \times (\mathbb{Z}_2)^{n-3}$. The order of $Aut(Q_n)$ is therefore $1344 \cdot 2^{n-3}$.*

*Proof.* Let $G = Aut\,(Q_n)$, $K = Aut\,(Q_{n-1})$, $N = \{(id, id), (id, -id)\} \cong \mathbb{Z}_2$, $n \geq 4$.

1. The group $K$ is normal in $G$ because $[G : K] = 2$.

2. Next, let us show that $N$ is normal in $G$. Let $g \in G$, $h \in N$. Note that $g^{-1}hg \in N$ iff $g^{-1}hg \restriction_{Q_{n-1}} = id_{Q_{n-1}}$. Let $x \in Q_{n-1}$, $g = kh_0$, where $k \in K$, $h_0 \in N$. Then

$$g^{-1}hg\,(x) = h_0^{-1}k^{-1}hk\,\underbrace{h_0\,(x)}_{x} = h_0^{-1}k^{-1}\underbrace{hk\,(x)}_{k(x)\in Q_{n-1}} = h_0^{-1}\underbrace{k^{-1}k\,(x)}_{x} = h_0^{-1}\,(x) = x,$$

therefore $g^{-1}hg \in N$.

3. Since $N$ is not a subset of $K$, we have $|KN| > |K| = \frac{|G|}{2}$, so $KN = G$.

4. Obviously, $(id, -id) \notin K$ and $N \cap K = \{id\}$. $\square$

# Chapter 4

# Inner Mapping Groups And Multiplication Groups

In this chapter we study multiplication groups and inner mapping groups of the Cayley–Dickson loops $Q_n$. When $n \leq 2$, the loop $Q_n$ is a group, and the structure of $Mlt(Q_n)$ and $Inn(Q_n)$ is known (see Remark 1.2.3). We therefore focus on nonassociative Cayley–Dickson loops $Q_n$, $n \geq 3$.

## 4.1 Inner Mapping Groups

**Lemma 4.1.1.** *Let $Q_n$ be a Cayley–Dickson loop. Elements of $Mlt(Q_n)$ are even permutations.*

*Proof.* Consider $L_x$. If $|x| = 1$ then $L_x = id$. If $|x| = 2$ then $L_x L_x(y) = xxy = y$ for every $y$, so $L_x$ is a product of $|Q_n|/2 = 2^n$ transpositions (of the form $(y, xy)$), and since $2^n$ is even, $L_x$ is even. If $|x| = 4$ then $L_x$ is a product of $2^{n-1}$ 4-cycles (of the form $(y, xy, xxy, xxxy)$), and since $2^{n-1}$ is even, $L_x$ is even. Similarly for right translations. Hence $Mlt(Q_n)$ is generated by even permutations, and it therefore consists of even permutations. $\square$

**Lemma 4.1.2.** *Let $Q_n$ be a Cayley–Dickson loop, and let $x, y \neq \pm 1$, $x \neq \pm y$ be elements of $Q_n$. Then*

$$\begin{aligned}
T_x &= \prod_{1,x \neq z \in Q_n/\{\pm 1\}} (z, -z), \\
T_y T_x &= (x, -x)(y, -y). \qquad (4.1.1)\\
L_{x,e} &= \prod_{1,x,e,xe \neq z \in Q_n/\{\pm 1\}} (z, -z), \\
L_{y,e} L_{x,e} &= (x, -x)(y, -y)(xe, -xe)(ye, -ye), \quad \textit{for } x, y \neq \pm e. \qquad (4.1.2)
\end{aligned}$$

*Proof.* Consider $T_x, R_{x,y}, L_{x,y}$ acting on $z \in Q_n$. Using diassociativity,

$$\begin{aligned}
T_x(z) &= x^{-1}(zx) = [x,z]x^{-1}(xz) = [x,z](x^{-1}x)z = [x,z]z, \qquad (4.1.3)\\
L_{x,y}(z) &= (yx)^{-1}(y(xz)) = [y,x,z](yx)^{-1}((yx)z) \qquad (4.1.4)\\
&= [y,x,z]((yx)^{-1}(yx))z = [y,x,z]z, \\
R_{x,y}(z) &= ((zx)y)(xy)^{-1} = [z,x,y](z(xy))(xy)^{-1} \qquad (4.1.5)\\
&= [z,x,y]z((xy)(xy)^{-1}) = [z,x,y]z.
\end{aligned}$$

Let $x, y \neq \pm 1$, $x \neq \pm y$. If $z \in \pm\{1, x\}$, then $\langle x, z\rangle \cong \langle x \rangle \cong \mathbb{C}_4$, and $[x,z] = 1$. Otherwise, $\langle x, z \rangle \cong \mathbb{H}_8$, and $[x,z] = -1$. Using (4.1.3),

$$T_x(z) = [x,z]z = \begin{cases} z, & \text{if } z \in \pm\{1, x\}, \\ -z & \text{otherwise.} \end{cases}$$

Similarly, if $z \in \pm\{x, y\}$, then $[y,z][x,z] = -1$. Otherwise, if $z \neq \pm 1$, then $\langle x, z\rangle \cong \langle y, z \rangle \cong \mathbb{H}_8$, and $[y,z] = [x,z] = -1$, if $z = \pm 1$, then $\langle x, z \rangle \cong \langle y, z\rangle \cong \mathbb{C}_4$, and $[y,z] = [x,z] = 1$. We get

$$T_yT_x(z) = [y,z][x,z]z = \begin{cases} -z, & \text{if } z \in \pm\{x,y\}, \\ z & \text{otherwise.} \end{cases}$$

Let $x, y \neq \pm e$. If $z \in \pm\{1, x, e, xe\}$, then $\langle e, x, z\rangle \cong \langle e, x\rangle \cong \mathbb{H}_8$, and $[e, x, z] = 1$. Otherwise, $\langle e, x, z\rangle \cong \mathbb{O}_{16}$ by Lemma 3.2.2, and $[e, x, z] = -1$. Using (4.1.4),

$$L_{x,e}(z) = [e,x,z]z = \begin{cases} z, & \text{if } z \in \pm\{1,x,e,xe\}, \\ -z & \text{otherwise.} \end{cases}$$

Similarly,

$$L_{y,e}L_{x,e}(z) = [e,y,z][e,x,z]z = \begin{cases} -z, & \text{if } z \in \pm\{x,y,xe,ye\}, \\ z & \text{otherwise.} \end{cases}$$ □

**Corollary 4.1.3.** *Let $Q_n$ be a Cayley–Dickson loop. Then*

$$L_{x,y} = R_{x,y} \text{ for all } x, y \in Q_n.$$

*Proof.* Let $x, y, z \in Q_n$. By Lemma 2.4.4,

$$[y,x,z] = [z,x,y],$$

$L_{x,y} = R_{x,y}$ follows from (4.1.4), (4.1.5) in Lemma 4.1.2. □

**Theorem 4.1.4.** *Let $Q_n$ be a Cayley–Dickson loop, $n \geq 1$. Then $Inn(Q_n)$ is an elementary abelian 2-group of order $2^{2^n-2}$. Moreover, every $f \in Inn(Q_n)$ is a product of disjoint transpositions of the form $(x, -x)$.*

*Proof.* Recall that $Z(Q_n) = \{1, -1\}$. Inner mappings fix $Z(Q_n)$ pointwise, therefore

$$f(1) = 1, f(-1) = -1.$$

Let $x \in Q_n, x \neq \pm 1$. Then $|x| = 4$ and $S = \langle x \rangle = \{1, x, -1, -x\}$. We know that $Q_n$ is Hamiltonian, therefore $S \trianglelefteq Q_n$. Inner mappings fix normal subloops, thus $f(S) = S$, and it follows that either $f(x) = x$, $f(-x) = -x$, or $f(x) = -x$, $f(-x) = x$. Hence every $f$ has the desired form. In particular, $|f| = 2$. A group of exponent 2 is an elementary abelian 2-group.

Let $e = i_n$ be a canonical generator of $Q_n$, let $x \in Q_n$, $x \notin \pm\{1, e\}$. Then $T_x T_e = (x, -x)(e, -e)$ by Lemma 4.1.2. For every $f \in Inn(Q_n)$, there is $\tilde{f} = T_x T_e f \in Inn(Q_n)$ such that

$$\tilde{f}(z) = \begin{cases} -f(z), & \text{when } z \in \pm\{x, e\}, \\ f(z), & \text{otherwise.} \end{cases}$$

Also, the values of $f(e), f(-e)$ are uniquely determined by the values of $f(z), z \neq \pm e$, since $f$ should remain an even permutation by Lemma 4.1.1 (see Figure 4.1).

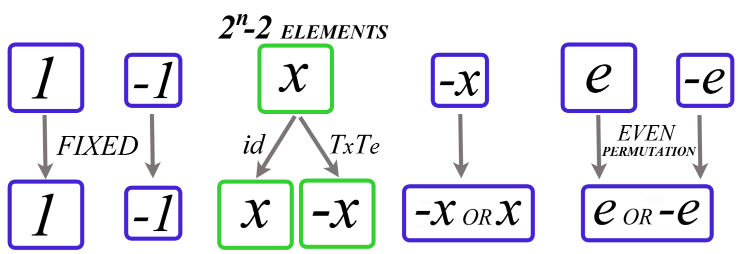


Figure 4.1: Inner mapping group of $Q_n$

It follows that $|Inn(Q_n)| = 2^{|Q_n|/2-2} = 2^{2^n-2}$. □

**Lemma 4.1.5.** *Let $f \in Mlt(Q_n)$, then $|f| \in \{1, 2, 4\}$. In particular, $f$ is a product of disjoint 2-cycles and 4-cycles.*

*Proof.* Denote by $-1$ the translation $L_{-1} = R_{-1} \in Mlt(Q_n)$. Let $f \in Mlt(Q_n)$. Let $x \in Q_n$ be such that $f(1) = x$. Then there is $h \in Inn(Q_n)$ such that $f = L_x h$. If $x = 1$ then $f \in Inn(Q_n)$, and we are done. If $x = -1$ then $f = -h$, $f^2 = (-h)(-h) = h^2 = 1$, and we are also done. Assume that $x \neq \pm 1$. We know that $f \in L_x Inn(Q_n)$. There is $y \in Q_n$ such that $f \in Inn(Q_n)L_y$, we want to determine $y$. Let $f = L_x h = kL_y$ for some $h, k \in Inn(Q_n)$. Since $x \neq \pm 1$, we have $y \neq \pm 1$. Then $f(-y) = kL_y(-y) = k(1) = 1$ and $f(-y) = L_x h(-y) = x(\pm y)$ (since $h(-y)$ is either $y$ or $-y$), so we conclude $y = x$ or $y = -x$. In the former case, we have $f = L_x h = kL_x$, and so $f^2 = kL_x L_x h = k(-1)h = -kh$, which has order at most two, so $f^4 = 1$. In the latter case, we have $f = L_x h = kL_{-x}$, and so $f^2 = kL_{-x}L_x h = kh$, which has order at most two, so $f^4 = 1$. □

A loop $Q$ is *automorphic* if $Inn(Q) \leq Aut(Q)$. Automorphic loops were introduced by Bruck and Paige [5] and received attention in the recent years, with foundational papers [18], [23].

**Corollary 4.1.6.** *Nonassociative Cayley–Dickson loops are not automorphic.*

*Proof.* Let $Q_n$ be a Cayley–Dickson loop. For $n \leq 2$, $Q_n$ is a group and hence is automorphic. Note that $|Inn(Q_n)| = 2^{2^n-2} > 1344 \cdot 2^{n-3} = |Aut(Q_n)|$ for $n > 3$ (see Theorem 3.4.3). Let $n = 3$, and let $i_1, i_2, i_3$ be canonical generators of $Q_n$. If $Inn(Q_n) \cap Aut(Q_n) = id$, we are done. Otherwise, let $f \in Inn(Q_n) \cap Aut(Q_n)$ be a nontrivial mapping defined by

$$f(i_k) = f_k, \quad k \in \{1, 2, 3\}.$$

For every $x \in Q_n$, $x \notin \pm\{i_1, i_2, i_3\}$, we know that $x = \prod_{j=1}^{3} i_j^{\epsilon_j}$ (where $\epsilon_j \in \{0, 1\}$), and since $f$ is an automorphism, $f(x)$ is uniquely defined by

$$f(x) = f(\prod_{j=1}^{3} i_j^{\epsilon_j}) = \prod_{j=1}^{3} f(i_j^{\epsilon_j}) = \prod_{j=1}^{3} f_j^{\epsilon_j}.$$

Let $y \notin \pm\{i_1, i_2, i_3, x\}$. Then by (4.1.1), $\tilde{f} = T_y T_x f$ satisfies

$$\begin{aligned} \tilde{f} \restriction_{\pm\{i_1,i_2,i_3\}} &= f, \\ \tilde{f}(x) &= -f(x), \end{aligned}$$

so $\tilde{f} \in Inn(Q_n)$ but $\tilde{f} \notin Aut(Q_n)$. □

## 4.2 Multiplication Groups

We establish the auxiliary Lemmas 4.2.1, 4.2.2, 4.2.3, 4.2.4 and use them in the construction of Lemma 4.2.6 and the proof of Theorem 4.2.7.

**Lemma 4.2.1.** *Let $G$ be a finite group, and let $g_1, g_2, \ldots, g_n$ be elements of $G$ of order 2 such that $G = \langle g_1, g_2, \ldots, g_n \rangle$. Then*

$$|g_j g_k| = 2 \text{ iff } g_j g_k = g_k g_j, \quad j, k \in \{1, \ldots, n\}, j \neq k,$$

*and if either holds for all $j, k$, then $G$ is an elementary abelian 2-group.*

*Proof.* Suppose $|g_j g_k| = 2$, then $(g_j g_k)(g_k g_j) = g_j g_k^2 g_j = g_j^2 = 1 = (g_j g_k)(g_j g_k)$, and hence $g_k g_j = g_j g_k$. If $g_k g_j = g_j g_k$, then $(g_j g_k)^2 = (g_j g_k)(g_j g_k) = (g_j g_k)(g_k g_j) = g_j g_k^2 g_j = g_j^2 = 1$, and $|g_j g_k| = 2$. If $g_k g_j = g_j g_k$ for all $j, k \in \{1, \ldots, n\}, j \neq k$, it is straightforward to check that $G$ is an elementary abelian 2-group. □

**Lemma 4.2.2.** *Let $Q_n$ be a Cayley–Dickson loop, $i_j, i_k$ among its canonical generators, and $x \in Q_n$. Let*

$$\begin{aligned} p_{j,k}(x) &= L_{i_j} \restriction_{\pm\{x, i_j x, i_k x, i_j(i_k x)\}} \\ &= (x, i_j x, -x, -i_j x)(i_k x, i_j(i_k x), -i_k x, -i_j(i_k x)), \\ q_{j,k}(x) &= T_{i_k x} T_x p_{j,k}(x), \end{aligned}$$

$$\begin{aligned} M_{j,k,x,1} &= \{T_{i_jx}T_x, T_{i_j(i_kx)}T_{i_kx}\}, \\ M_{j,k,x,-1} &= \{T_{i_j(i_kx)}T_x, T_{i_kx}T_{i_jx}\}. \end{aligned}$$

*Then* $|q_{j,k}(x)| = |tp_{k,j}(x)| = |q_{j,k}(x)(tp_{k,j}(x))| = 2,$ *where* $t \in M_{j,k,x,s},$ *and* $s \in Z(Q_n)$ *satisfies* $i_j(i_kx) = s(i_k(i_jx))$.

*Proof.* We write down the corresponding permutations and check that they only contain involutions. Using Lemma 4.1.2,

$$q_{j,k}(x) = T_{i_kx}T_xp_{j,k} = (x, i_jx)(-x, -i_jx)(i_kx, i_j(i_kx))(-i_kx, -i_j(i_kx)),$$

hence $|q_{j,k}(x)| = 2$.

Let $s$ be an element of $Q_n$ such that $i_j(i_kx) = s(i_k(i_jx))$. Note that $s \in Z(Q_n)$ as a product of commutators and associators, therefore $s \in \{1, -1\}$.

If $s = 1$ and $i_j(i_kx) = i_k(i_jx)$, then

$$\begin{aligned} p_{k,j}(x) &= (x, i_kx, -x, -i_kx)(i_jx, i_j(i_kx), -i_jx, -i_j(i_kx)), \\ T_{i_jx}T_xp_{k,j}(x) &= (x, i_kx)(-x, -i_kx)(i_jx, i_j(i_kx))(-i_jx, -i_j(i_kx)), \\ T_{i_j(i_kx)}T_{i_kx}p_{k,j}(x) &= (x, -i_kx)(-x, i_kx)(i_jx, -i_j(i_kx))(-i_jx, i_j(i_kx)). \end{aligned}$$

In this case,

$$\begin{aligned} q_{j,k}(x) \cdot (T_{i_jx}T_xp_{k,j}(x)) &= (x, i_j(i_kx))(-x, -i_j(i_kx))(i_jx, i_kx)(-i_jx, -i_kx), \\ q_{j,k}(x) \cdot (T_{i_j(i_kx)}T_{i_kx}p_{k,j}(x)) &= (x, -i_j(i_kx))(-x, i_j(i_kx))(i_jx, -i_kx)(-i_jx, i_kx). \end{aligned}$$

One can see that $|tp_{k,j}(x)| = |q_{j,k}(x)(tp_{k,j}(x))| = 2$, where $t \in \{T_{i_jx}T_x, T_{i_j(i_kx)}T_{i_kx}\}$.

Similarly, if $s = -1$ and $i_j(i_k x) = -i_k(i_j x)$, then

$$\begin{aligned} p_{k,j}(x) &= (x, i_k x, -x, -i_k x)(i_j x, -i_j(i_k x), -i_j x, i_j(i_k x)), \\ T_{i_j(i_k x)} T_x p_{k,j}(x) &= (x, i_k x)(-x, -i_k x)(i_j x, i_j(i_k x))(-i_j x, -i_j(i_k x)), \\ T_{i_k x} T_{i_j x} p_{k,j}(x) &= (x, -i_k x)(-x, i_k x)(i_j x, -i_j(i_k x))(-i_j x, i_j(i_k x)). \end{aligned}$$

In this case,

$$\begin{aligned} q_{j,k}(x) \cdot (T_{i_j(i_k x)} T_x p_{k,j}(x)) &= (x, i_j(i_k x))(-x, -i_j(i_k x))(i_j x, i_k x)(i_j x, i_k x), \\ q_{j,k}(x) \cdot (T_{i_k x} T_{i_j x} p_{k,j}(x)) &= (x, -i_j(i_k x))(-x, i_j(i_k x))(i_j x, -i_k x)(-i_j x, i_k x). \end{aligned}$$

Again, $\left|tp_{k,j}(x)\right| = \left|q_{j,k}(x)(tp_{k,j}(x))\right| = 2$, where $t \in \{T_{i_j(i_k x)} T_x, T_{i_k x} T_{i_j x}\}$. □

We use the following property to prove Lemmas 4.2.3 and 4.2.4.

**Lemma 4.2.3.** *Let $Q_n$ be a Cayley–Dickson loop, and let $i_1, i_2, \ldots, i_n$ be its canonical generators. Then $i_k(i_n x) = -i_n(i_k x)$ for any $x \in \langle i_1, i_2, \ldots, i_{n-1} \rangle$, $k < n$.*

*Proof.* Let $x \in \langle i_1, i_2, \ldots, i_{n-1} \rangle$. Then

$$\begin{aligned} i_k(i_n x) &= [i_k, i_n, x](i_k i_n)x = [i_k, i_n][i_k, i_n, x](i_n i_k)x \\ &= [i_k, i_n][i_k, i_n, x][i_n, i_k, x] i_n(i_k x). \end{aligned}$$

Recall that $\langle x, y, i_n \rangle \leq \mathbb{O}_{16}$ for any $x, y \in Q_n$, by Lemma 3.2.2, and $\langle x, y, i_n \rangle \cong \mathbb{O}_{16}$ implies that $[x, y, i_n] = -1$. Also, $[i_k, i_n] = -1$ as $\langle i_k, i_n \rangle \cong \mathbb{H}_8$. This leads to

$$[i_k, i_n][i_k, i_n, x][i_n, i_k, x] = \begin{cases} -1 \cdot 1 \cdot 1 = -1, & \text{if } x \in \langle i_k, i_n \rangle, \\ -1 \cdot (-1) \cdot (-1) = -1, & \text{otherwise.} \end{cases}$$

We conclude that $i_k(i_n x) = -i_n(i_k x)$. □

**Lemma 4.2.4.** *Let $Q_n$ be a Cayley–Dickson loop, and let $i_1, i_2, \ldots, i_n$ be its canonical generators. For any $x \in \langle i_1, i_2, \ldots, i_{n-1}\rangle$, $j < n, k < n, j \neq k$, if $i_j(i_k x) = s(i_k(i_j x))$, then $i_j(i_k(x i_n)) = s(i_k(i_j(x i_n)))$ (where $s \in Z(Q_n)$).*

*Proof.* Let $x \in \langle i_1, i_2, \ldots, i_{n-1}\rangle$, and let $s \in Z(Q_n)$ be such that $i_j(i_k x) = s(i_k(i_j x))$. Then

$$\begin{aligned}
i_j(i_k(x i_n)) &= [i_k, x, i_n] i_j((i_k x) i_n) = [i_k, x, i_n][i_j, i_k x, i_n](i_j(i_k x)) i_n \\
&= [i_k, x, i_n][i_j, i_k x, i_n] s((i_k(i_j x)) i_n) \\
&= [i_k, x, i_n][i_j, i_k x, i_n][i_k, i_j x, i_n] s i_k((i_j x) i_n) \\
&= [i_k, x, i_n][i_j, i_k x, i_n][i_k, i_j x, i_n][i_j, x, i_n] s i_k(i_j(x i_n)).
\end{aligned}$$

Recall that $\langle x, y, i_n\rangle \leq \mathbb{O}_{16}$ for any $x, y \in Q_n$, by Lemma 3.2.2, and $\langle x, y, i_n\rangle \cong \mathbb{O}_{16}$ implies that $[x, y, i_n] = -1$, which leads to

$$[i_k, x, i_n][i_j, i_k x, i_n][i_k, i_j x, i_n][i_j, x, i_n] = \begin{cases}
1 \cdot (-1) \cdot (-1) \cdot 1 = 1, & \text{if } x = \pm 1, \\
-1 \cdot (-1) \cdot 1 \cdot 1 = 1, & \text{if } x = \pm i_j, \\
1 \cdot 1 \cdot (-1) \cdot (-1) = 1, & \text{if } x = \pm i_k, \\
-1 \cdot 1 \cdot 1 \cdot (-1) = 1, & \text{if } x = \pm i_j i_k, \\
-1 \cdot (-1) \cdot (-1) \cdot (-1) = 1 & \text{otherwise.}
\end{cases}$$

We conclude that $i_j(i_k(x i_n)) = s(i_k(i_j(x i_n)))$. □

**Proposition 4.2.5.** *A group $G$ is a semidirect product of groups $N$ and $K$ iff*

1. *$N$ is a normal subgroup of $G$, $K$ is a subgroup of $G$,*
2. *$G = NK$,*
3. *$N \cap K = id$, the trivial subgroup of $G$.*

In Lemma 4.2.6 we present a construction of the subgroup $K$ of $Mlt(Q_n)$ which is used in Theorem 4.2.7 to establish that $Mlt(Q_n) \cong (Inn(Q_n) \times Z(Q_n)) \rtimes K$. For every $x \in Q_n/\{1,-1\}$, we want $K$ to contain the element $k_x$ such that $k_x(1) \in x$. This holds when $K$ is generated by $\{L_{i_k} \mid i_k$ a canonical generator of $Q_n\}$. We also want $K$ to be sufficiently small to allow $(Inn(Q_n) \times Z(Q_n)) \cap K = id$. To achieve this, we should adjust the left translations $L_{i_k}$ so that they generate a group as small as needed. This is done by multiplying $L_{i_k}$ by $\psi_k \in Inn(Q_n)$ such that $|\psi_k L_{i_k}| = |\psi_j L_{i_j}| = |(\psi_k L_{i_k}) \cdot (\psi_j L_{i_j})| = 2$ for all $j, k \leq n, j \neq k$. Consider the group $\mathbb{H}_8$, where left translations by canonical generators are

$$
\begin{aligned}
L_{i_1} &= (1, i_1, -1, -i_1)(i_2, i_1 i_2, -i_2, -i_1 i_2), \\
L_{i_2} &= (1, i_2, -1, -i_2)(i_1, i_2 i_1, -i_1, -i_2 i_1) = (1, i_2, -1, -i_2)(i_1, -i_1 i_2, -i_1, i_1 i_2).
\end{aligned}
$$

For an inner mapping $\psi_1 \in Inn(\mathbb{H}_8)$ such that $|\psi_1 L_{i_1}| = 2$ we can either take $T_{i_2}$, or $T_{i_1 i_2}$ (one can check that $|T_{i_1} L_{i_1}| = 4$),

$$
\begin{aligned}
T_{i_2} L_{i_1} &= (1, -i_1)(-1, i_1)(i_2, -i_1 i_2)(-i_2, i_1 i_2), \\
T_{i_1 i_2} L_{i_1} &= (1, -i_1)(-1, i_1)(i_2, i_1 i_2)(-i_2, -i_1 i_2).
\end{aligned}
$$

Similarly, for an inner mapping $\psi_2 \in Inn(\mathbb{H}_8)$ such that $|\psi_2 L_{i_2}| = 2$ we can either take $T_{i_1}$, or $T_{i_1 i_2}$,

$$
\begin{aligned}
T_{i_1} L_{i_2} &= (1, -i_2)(-1, i_2)(i_1, i_1 i_2)(-i_1, -i_1 i_2), \\
T_{i_1 i_2} L_{i_2} &= (1, -i_2)(-1, i_2)(i_1, -i_1 i_2)(-i_1, i_1 i_2).
\end{aligned}
$$

For a pair of mappings $\psi_1, \psi_2$ such that $|(\psi_1 L_{i_1}) \cdot (\psi_2 L_{i_2})| = 2$ we can either take $\psi_1 = T_{i_2}, \psi_2 = T_{i_1 i_2}$, or $\psi_1 = T_{i_1 i_2}, \psi_2 = T_{i_1}$,

$$(T_{i_2}L_{i_1})\cdot(T_{i_1i_2}L_{i_2}) = (1,i_1i_2)(-1,-i_1i_2)(i_1,i_2)(-i_1,-i_2),$$
$$(T_{i_1i_2}L_{i_1})\cdot(T_{i_1}L_{i_2}) = (1,-i_1i_2)(-1,i_1i_2)(i_1,i_2)(-i_1,-i_2).$$

Without loss of generality, we choose $\psi_1 = T_{i_2}, \psi_2 = T_{i_1i_2}$, and $K_2 = \langle g_{1,2}, g_{2,2}\rangle = \langle T_{i_2}L_{i_1}, T_{i_1i_2}L_{i_2}\rangle$. The group $K_2$ is not unique, and this particular choice allows to generalize the construction for higher dimensions. The group we present in Lemma 4.2.6 is based on this choice and suffices to establish the structure of $Mlt(Q_n)$. Note that the structure of $Mlt(\mathbb{H}_8)$ is known (see Remark 1.2.3), so the construction of $K$ for $\mathbb{H}_8$ is only used as an initial step of the inductive construction for $Q_n$.

Next, consider $\mathbb{O}_{16}$. We want to construct $K_3$ based on $K_2$ by extending the generators of $K_2$ to form the elements of $K_3$, and including one more generator based on $L_{i_3}$. By Lemma 2.4.2, we have

$$\begin{aligned} i_1(i_2i_3) &= -(i_1i_2)i_3,\\ i_2(i_1i_3) &= -(i_2i_1)i_3 = (i_1i_2)i_3,\\ i_3(i_1i_2) &= -(i_1i_2)i_3, \end{aligned}$$

hence

$$\begin{aligned} L_{i_1} &= (1,i_1,-1,-i_1)(i_2,i_1i_2,-i_2,-i_1i_2)(i_3,i_1i_3,-i_3,-i_1i_3)(i_2i_3,-(i_1i_2)i_3,-i_2i_3,(i_1i_2)i_3),\\ L_{i_2} &= (1,i_2,-1,-i_2)(i_1,-i_1i_2,-i_1,i_1i_2)(i_3,i_2i_3,-i_3,-i_2i_3)(i_1i_3,(i_1i_2)i_3,-i_1i_3,-(i_1i_2)i_3),\\ L_{i_3} &= (1,i_3,-1,-i_3)(i_1,-i_1i_3,-i_1,i_1i_3)(i_2,-i_2i_3,-i_2,i_2i_3)(i_1i_2,-(i_1i_2)i_3,-i_1i_2,(i_1i_2)i_3). \end{aligned}$$

For every cycle $(x, i_kx, -x, -i_kx)$ we want $\psi_k$ to include either $T_x$, or $T_{i_kx}$ (but not both), so that the cycle becomes a product of two 2-cycles, either $(x, i_kx)(-x, -i_kx)$, or $(x, -i_kx)(-x, i_kx)$. Note that a product of an odd number of mappings $T_{x_1}T_{x_2}T_{x_3}$

(where $x_1, x_2, x_3 \in \mathbb{O}_{16}$) fixes $\pm\{1, x_1, x_2, x_3\}$ and moves all other elements (see Lemma 4.1.2). Taking $\psi_1 = T_{i_2}T_{i_3}T_{i_2i_3}, \psi_2 = T_{i_1i_2}T_{i_3}T_{i_1i_2i_3}$, we get

$$\begin{aligned}
g_{1,3} &= T_{i_2}T_{i_3}T_{i_2i_3}L_{i_1} \\
&= (1,-i_1)(-1,i_1)(i_2,-i_1i_2)(-i_2,i_1i_2) \\
&\quad (i_3,-i_1i_3)(-i_3,i_1i_3)(i_2i_3,(i_1i_2)i_3)(-i_2i_3,-(i_1i_2)i_3), \\
g_{2,3} &= T_{i_1i_2}T_{i_3}T_{i_1i_2i_3}L_{i_2} \\
&= (1,-i_2)(-1,i_2)(i_1,-i_1i_2)(-i_1,i_1i_2) \\
&\quad (i_3,-i_2i_3)(-i_3,i_2i_3)(i_1i_3,(i_1i_2)i_3)(-i_1i_3,-(i_1i_2)i_3), \\
g_{1,3}g_{2,3} &= (1,i_1i_2)(-1,-i_1i_2)(i_1,i_2)(-i_1,-i_2) \\
&\quad (i_3,-(i_1i_2)i_3)(-i_3,(i_1i_2)i_3)(i_1i_3,i_2i_3)(-i_1i_3,-i_2i_3).
\end{aligned}$$

Again, this is one of several possible choices of $g_{1,3}, g_{2,3}$. Finally, we need to add a generator $g_{3,3}$ such that $|g_{3,3}| = |g_{1,3}g_{3,3}| = |g_{2,3}g_{3,3}| = 2$, one can choose, for example,

$$\begin{aligned}
g_{3,3} &= T_{i_1i_2}T_{i_1i_3}T_{i_2i_3}L_{i_3} \\
&= (1,-i_3)(-1,i_3)(i_1,-i_1i_3)(-i_1,i_1i_3) \\
&\quad (i_2,-i_2i_3)(-i_2,i_2i_3)(i_1i_2,(i_1i_2)i_3)(-i_1i_2,-(i_1i_2)i_3),
\end{aligned}$$

which results in

$$\begin{aligned}
g_{1,3}g_{3,3} &= (1,i_1i_3)(-1,-i_1i_3)(i_1,i_3)(-i_1,-i_3) \\
&\quad (i_2,-(i_1i_2)i_3)(-i_2,(i_1i_2)i_3)(i_1i_2,i_2i_3)(-i_1i_2,-i_2i_3), \\
g_{2,3}g_{3,3} &= (1,i_2i_3)(-1,-i_2i_3)(i_2,i_3)(-i_2,-i_3) \\
&\quad (i_1,-(i_1i_2)i_3)(-i_1,(i_1i_2)i_3)(i_1i_2,i_1i_3)(-i_1i_2,-i_1i_3).
\end{aligned}$$

Below is the description of the construction for $Q_n$.

**Lemma 4.2.6.** *Let $i_1, i_2, \ldots, i_n$ be canonical generators of a Cayley–Dickson loop $Q_n$, and let $K$ be the group constructed inductively as follows*

$$\begin{aligned}
s_{1,2} &= \{1, i_2\}, \quad s_{2,2} = \{1, i_1 i_2\}, \\
g_{1,2} &= (\prod_{x \in s_{1,2}} T_x) L_{i_1}, \\
g_{2,2} &= (\prod_{x \in s_{2,2}} T_x) L_{i_2}, \\
K_2 &= \langle g_{1,2}, g_{2,2} \rangle, \\
s_{k,n} &= \{x, i_n x \mid x \in s_{k,n-1}\}, \quad k \in \{1, \ldots, n-1\}, \\
s_{n,n} &= \left\{ \prod_{j=1}^{n} i_j^{p_j} \mid p_j \in \{0,1\}, \sum_{j=1}^{n} p_j \in 2\mathbb{Z} \right\}, \\
g_{k,n} &= (\prod_{x \in s_{k,n}} T_x) L_{i_k} = (\prod_{x \notin s_{k,n}} (x, -x)) L_{i_k}, \quad k \in \{1, \ldots, n\}, \\
K &= K_n = \langle g_{1,n}, g_{2,n}, \ldots, g_{n,n} \rangle.
\end{aligned}$$

*Then $K$ is an elementary abelian 2-group of order $2^n$.*

*Proof.* We show by induction on $n$ that generators of $K$ have order 2. If $n = 2$, then

$$\begin{aligned}
g_{1,2} &= T_{i_2} T_1 L_{i_1} = (1, -i_1)(-1, i_1)(i_2, -i_1 i_2)(-i_2, i_1 i_2), \\
g_{2,2} &= T_{i_1 i_2} T_1 L_{i_2} = (1, -i_2)(-1, i_2)(i_1, -i_1 i_2)(-i_1, i_1 i_2)
\end{aligned}$$

are of order 2. Suppose that generators $g_{1,n-1}, g_{2,n-1}, \ldots, g_{n-1,n-1}$ of $K_{n-1}$ have order 2. Note that a product of an odd number of mappings $T_{x_1} \ldots T_{x_{2^{n-1}-1}}$ (where $x_1, \ldots, x_{2^{n-1}-1} \in Q_n$) fixes $\pm\{1, x_1, \ldots, x_{2^{n-1}-1}\}$ and moves all other elements (see Lemma 4.1.2). Left translation $L_{i_k}$ consists of 4-cycles of the form

$$(x, i_k x, -x, -i_k x).$$

In order to transform such cycle into two 2-cycles, $L_{i_k}$ is multiplied by either $T_x$, or

$T_{i_k x}$. Then the cycle

$$(i_n x, i_k(i_n x), -i_n x, -i_k(i_n x))$$

that appears in the next step of the inductive construction, is multiplied by either $T_{i_n x}$ or $T_{i_n(i_k x)}$, leading to either

$$\begin{aligned}&(i_n x, -i_k(i_n x))(-i_n x, i_k(i_n x)), \text{ or}\\&(i_n x, i_k(i_n x))(-i_n x, -i_k(i_n x)),\end{aligned}$$

respectively.

If $x = 1$, the 4-cycle that corresponds to $(1, i_k, -1, -i_k)$ in the next step of the inductive construction is $(i_n, i_k i_n, -i_n, -i_k i_n)$, which is multiplied by $T_{i_n}$ and becomes $(i_n, -i_k i_n)(-i_n, i_k i_n)$. It follows that $g_{k,n}$ consists of 2-cycles and therefore $|g_{k,n}| = 2$.

Consider a generator $g_{n,n}$ added at the $n$-th step of the inductive construction. Left translation $L_{i_n}$ consists of cycles of the form

$$(x, i_n x, -x, -i_n x)$$

where either $x$, or $i_n x$ (but not both) is a product of even number of units $i_k$, for some $k \le n$. In the former case, if $x \neq \pm 1$, then multiplication of $L_{i_n}$ by $T_x$ transforms a cycle $(x, i_n x, -x, -i_n x)$ into

$$(x, -i_n x)(-x, i_n x),$$

otherwise, multiplication of $L_{i_n}$ by $T_{i_n x}$ transforms it into

$$(x, i_n x)(-x, -i_n x).$$

Also, $L_{i_n}$ is multiplied by $T_{x_k}, x_k \neq \pm i_n$, an odd number of times, mapping $i_n$ to $-i_n$, and a cycle $(1, i_n, -1, -i_n)$ becomes

$$(1, -i_n)(-1, i_n).$$

Generator $g_{n,n}$ consists of 2-cycles and therefore $|g_n| = 2$.

Next, use induction on $n$ to show that

$$\left|g_{j,n} g_{k,n}\right| = 2, \text{ for all } j, k \in \{1, \ldots, n\}, j \neq k.$$

If $n = 2$, then

$$g_{1,2} g_{2,2} = (1, i_1 i_2)(-1, -i_1 i_2)(i_1, i_2)(-i_1, -i_2)$$

and $|g_{1,2} g_{2,2}| = 2$. Suppose that $\left|g_{j,n-1} g_{k,n-1}\right| = 2$ for any pair of generators $g_{j,n-1}, g_{k,n-1}$ of $K_{n-1}$. Without loss of generality, let $j < k$. Up to renaming $x$ and $i_j x$, the cycles

$$p_{j,k}(x) = L_{i_j} \restriction_{\pm\{x, i_j x, i_k x, i_j(i_k x)\}} = (x, i_j x, -x, -i_j x)(i_k x, i_j(i_k x), -i_k x, -i_j(i_k x))$$

are acted upon by $T_{i_k x} T_x$ to construct $g_{j,n}$. Then, by Lemma 4.2.2, the cycles

$$p_{k,j}(x) = L_{i_k} \restriction_{\pm\{x, i_j x, i_k x, i_j(i_k x)\}} = (x, i_k x, -x, -i_k x)(i_j x, i_k(i_j x), -i_j x, -i_k(i_j x))$$

are acted upon by $t \in M_{j,k,x,s}$, where $t = T_y T_z$ for some $y, z \in Q_n$. The cycles

$$p_{j,k}(x i_n) = (x i_n, i_j(x i_n), -x i_n, -i_j(x i_n))(i_k(x i_n), i_j(i_k(x i_n)), -i_k(x i_n), -i_j(i_k(x i_n)))$$

added at the next step of the inductive construction are multiplied by $T_{i_n(i_k x)} T_{i_n x}$. The cycles

$$\begin{aligned} p_{k,j}(x i_n) &= L_{i_k} \restriction_{\pm\{x i_n, i_j(x i_n), i_k(x i_n), i_j(i_k(x i_n))\}} \\ &= (x i_n, i_k(x i_n), -x i_n, -i_k(x i_n))(i_j(x i_n), i_k(i_j(x i_n)), -i_j(x i_n), -i_k(i_j(x i_n))) \end{aligned}$$

are multiplied by $T_{yi_n}T_{zi_n} \in M_{j,k,xi_n,s}$. By Lemma 4.2.4, $i_j(i_k(xi_n)) = s(i_k(i_j(xi_n)))$, and therefore by Lemma 4.2.2,

$$\left|(T_{(i_kx)i_n}T_{xi_n}p_{j,k}(xi_n)) \cdot (tp_{k,j}(xi_n))\right| = 2 \text{ for } t \in M_{j,k,xi_n,s}.$$

It is left to show that $|g_{j,n}g_{n,n}| = 2$, where $j < n$. Up to renaming $x$ and $i_jx$, the cycles

$$p_{j,k}(x) = L_{i_j} \restriction_{\pm\{x,i_jx,i_nx,i_j(i_nx)\}} = (x, i_jx, -x, -i_jx)(i_nx, i_j(i_nx), -i_nx, -i_j(i_nx))$$

are acted upon by $T_{i_nx}T_x$. By Lemma 4.2.3, $i_j(i_nx) = -i_n(i_jx)$, therefore by Lemma 4.2.2,

$$\left|(T_{i_nx}T_xp_{j,k}(x)) \cdot (tp_{n,j}(x))\right| = 2 \text{ where } t \in \{T_xT_{i_j(i_nx)}, T_{i_jx}T_{i_nx}\}.$$

If $x$ is a product of even number of units $i_k$, for some $k \le n$, then $i_j(i_nx)$ is also a product of even number of units, so $x, i_j(i_nx)$ are in $s_{n,n}$, and $T_xT_{i_j(i_nx)}$ is a part of the construction of $g_{n,n}$. If $x$ is a product of odd number of units, then $i_jx, i_nx$ are products of even number of units, and are included in $s_{n,n}$, so $T_{i_jx}T_{i_nx}$ is a part of the construction of $g_{n,n}$. In both cases this leads to $|g_{j,n}g_{n,n}| = 2$.
Summarizing, $K$ satisfies the assumptions of Lemma 4.2.1 and is therefore an elementary abelian 2-group.
To determine the order of $K$, define a mapping $\phi : Q_n/\{1,-1\} \to K$ by

$$\phi(\{i_k, -i_k\}) = g_{k,n}, k \in \{1, \dots, n\}.$$

Note that for any

$$\begin{aligned} x &= \pm\{\prod_{j=1}^{n} i_j^{\epsilon_j}\} \in Q_n/\{1,-1\} \quad (\text{ where } \epsilon_j \in \{0,1\}), \text{ there is} \\ g &= \prod_{j=1}^{n} \phi(i_j^{\epsilon_j}) = \prod_{j=1}^{n} g_{j,n}^{\epsilon_j}, \end{aligned} \tag{4.2.1}$$

such that $g(1) \in x$. We conclude that

$$|K| \geq |Q_n/\{1,-1\}| = \frac{|Q_n|}{2} = 2^n.$$

Also, $K$ is an elementary abelian 2-group with $n$ generators, so

$$|K| \leq 2^n. \tag{4.2.2}$$

We conclude that the order of $K$ is $2^n$. □

For any loop $Q$, Albert showed $Z(Mlt(Q)) = \{L_x \,|\, x \in Z(Q)\} \cong Z(Q)$. To improve legibility, we will identify $Z(Mlt(Q))$ with $Z(Q)$ in what follows.

In Theorem 4.2.7 we use the group $N = \langle Inn(Q_n), Z(Q_n)\rangle = Inn(Q_n)Z(Q_n)$ to establish the structure of $Mlt(Q_n)$. Recall that elements of $Inn(Q_n)$ are all even products of 2-cycles $(x,-x)$ (where $1 \neq x \in Q_n/\{1,-1\}$). A group $Inn(Q_n)$ stabilizes 1, therefore $Inn(Q_n) \cap Z(Q_n) = 1$. The index $[N : Inn(Q_n)] = 2$, therefore $Inn(Q_n) \trianglelefteq N$, and $Z(Q_n) \trianglelefteq Mlt(Q_n)$ implies $Z(Q_n) \trianglelefteq N$. It follows that $N = Inn(Q_n) \times Z(Q_n)$, and $N = Inn(Q_n) \cup (-Inn(Q_n))$.
A basis for $Inn(Q_n)$ can be taken to be

$$\{T_x T_e = (x,-x)(e,-e) \,|1, e \neq x \in Q_n/\{1,-1\}\}.$$

Elements of $N$ are all even products of 2-cycles $(x,-x)$, for $x \in Q_n/\{1,-1\}$. A mapping $L_{-1}T_e = (1,-1)(e,-e)$ can be used to construct a basis for $N$ (see Figure 4.2),

$$N^* = \{L_{-1}T_e, T_xT_e \,|1, e \neq x \in Q_n/\{1,-1\}\}\,.$$

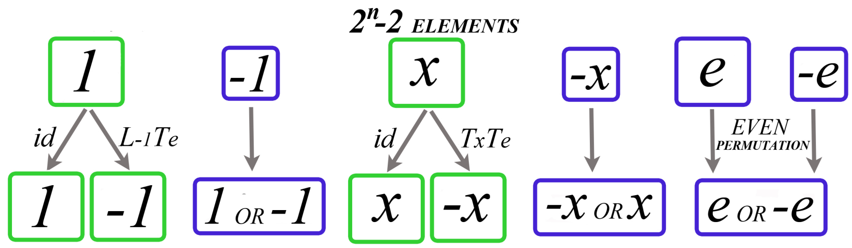


Figure 4.2: Group $N = Inn(Q_n) \times Z(Q_n)$

**Theorem 4.2.7.** *Let $Q_n$ be a Cayley–Dickson loop, $n \geq 2$. Then $Mlt(Q_n) \cong (Inn(Q_n) \times Z(Q_n)) \rtimes K$, where $K$ is the group constructed in Lemma 4.2.6. In particular, $Mlt(Q_n) \cong ((\mathbb{Z}_2)^{2^n-2} \times \mathbb{Z}_2) \rtimes (\mathbb{Z}_2)^n$.*

*Proof.* Let $G = Mlt(Q_n)$, $N = Inn(Q_n) \times Z(Q_n)$, and $K$ be the group constructed in Lemma 4.2.6. We want to show that $G = N \rtimes K$.

1. Let $\alpha \in N, g \in G$. There exist $x \in Q_n, \beta \in Inn(Q_n)$ such that $g = \beta L_x$. Consider $g\alpha g^{-1}$ acting on 1,

$$g\alpha g^{-1}(1) \;=\; \beta L_x\alpha(\beta L_x)^{-1}(1) = \beta L_x \alpha L_x^{-1}\underbrace{\beta^{-1}(1)}_{1} = \beta\underbrace{L_x\alpha L_x^{-1}(1)}_{\pm 1} = \pm\beta(1) = \pm 1.$$

   This shows that $g\alpha g^{-1} \in Inn(Q_n) \cup (-Inn(Q_n)) = N$, so $N$ is normal in $G$.

2. By (4.2.1), (4.2.2), $K$ contains a unique element $g$ such that $g(1) \in \{1,-1\}$. Since $K$ is a group, $g = id$, thus $N \cap K = id$.

3. We established that $N \trianglelefteq G, K \leq G$, and $N \cap K = id$. We have $N \rtimes K \leq G$.

Recall that

$$
\begin{aligned}
[Mlt(Q_n) : Inn(Q_n)] &= |Q_n|, \text{ thus} \\
[Mlt(Q_n) : (Inn(Q_n) \times Z(Q_n))] &= [Mlt(Q_n) : Inn(Q_n)]/2 = 2^n = |K|,
\end{aligned}
$$

and $(Inn(Q_n) \times Z(Q_n)) \rtimes K \cong Mlt(Q_n)$ follows. $\square$

## 4.3 Group Action for $Inn(Q_n) \times Z(Q_n) \trianglelefteq Mlt(Q_n)$

We have shown that $Mlt(Q_n)$ is a semidirect product of two permutation groups $N$, $K$, both elementary abelian 2-groups. In this section we construct an isomorphic copy of $Mlt(Q_n)$ as an external semidirect product of two abstract elementary abelian 2-groups.

Recall that if $N$, $K$ are groups and $\phi : K \to Aut(N)$ is a homomorphism, then the external semidirect product is defined on $N \times K$ by

$$
(h_1, k_1) \circ (h_2, k_2) = (h_1 * \phi_{k_1}(h_2), k_1 \cdot k_2), \quad h_1, h_2 \in N, k_1, k_2 \in K.
$$

In an internal semidirect product $G = N \rtimes_\phi K$, the action $\phi : K \to Aut(N)$ is natural, that is, by conjugation $\phi_{k_1}(h_2) = k_1 h_2 k_1^{-1}$.

**Lemma 4.3.1.** *[36, p.170] Let $G, N, K$ be finite groups such that $N \trianglelefteq G$ and $G = N \rtimes_\phi K$. Then $K$ acts on $N$ by conjugation.*

Let $Q_n$ be a Cayley–Dickson loop, let $N = Inn(Q_n) \cup (-Inn(Q_n))$, with a basis

$$
N^* = \{L_{-1}T_e, T_xT_e \,|1, e \neq x \in Q_n/\{1, -1\}\},
$$

and let $K$ be the group constructed in Lemma 4.2.6, with a basis

$$K^* = \{\psi_m L_{i_m} \mid i_m \text{ a canonical generator of } Q_n, \psi_m \in Inn(Q_n)\}.$$

Groups $N$ and $K$ can be viewed as vector spaces over $GF(2)$, with $dim(N) = |N^*| = \left|\frac{Q_n}{2}\right| - 1 = 2^n - 1$, $dim(K) = |K^*| = n$. Let $n_j \in N^*, k_m \in K^*$, $\phi_{k_m}(n_j) = k_m^{-1} n_j k_m$. Note that $N \lhd Mlt(Q_n)$, therefore $\phi_{k_m}(n_j) \in N$. Every $\phi_{k_m}$ is an automorphism of $N$, and can be identified with a $(2^n - 1) \times (2^n - 1)$ matrix

$$\begin{aligned}
A_m &= (a_{jl}^{(m)}), \text{ where} \\
\phi_{k_m}(n_j) &= \sum_{l=1}^{2^n-1} a_{jl}^{(m)} n_l, \\
a_{jl}^{(m)} &\in \{0, 1\}.
\end{aligned}$$

We want to determine matrices $A_m$, $1 \le m \le n$. We have either $n_j = T_x T_e = (x, -x)(e, -e)$, or $n_j = L_{-1} T_e = (1, -1)(e, -e)$. Let $k_m(x) = y \in \pm\{i_m x\}$. By construction, $k_m = \psi_m L_{i_m}$ has order 2 and only contains 2-cycles, thus $(k_m)_{\restriction_{\pm\{x,y\}}} = (x, y)(-x, -y)$ and $k_m^{-1} n_j k_m = k_m n_j k_m$. We need to consider the following cases

1. If $n_j$ moves both $x$ and $y$, then

$$\begin{aligned}
(k_m n_j k_m)_{\restriction_{\pm\{x,y\}}} &= (x, y)(-x, -y) \cdot ((x, -x)(y, -y) \cdot (x, y)(-x, -y)) \\
&= (x, y)(-x, -y) \cdot (x, -y)(-x, y) = (x, -x)(y, -y) = (n_j)_{\restriction_{\pm\{x,y\}}}.
\end{aligned}$$

2. If $n_j$ fixes both $x$ and $y$, then

$$\begin{aligned}
(k_m n_j k_m)_{\restriction_{\pm\{x,y\}}} &= (x, y)(-x, -y) \cdot ((x)(-x)(y)(-y) \cdot (x, y)(-x, -y)) \\
&= (x, y)(-x, -y) \cdot (x, y)(-x, -y) = (x)(-x)(y)(-y) = (n_j)_{\restriction_{\pm\{x,y\}}}.
\end{aligned}$$

3. If $n_j$ moves $x$ and fixes $y$, then

$$\begin{aligned}(k_m n_j k_m)\restriction_{\pm\{x,y\}} &= (x,y)(-x,-y)\cdot((x,-x)(y)(-y)\cdot(x,y)(-x,-y)) \\ &= (x,y)(-x,-y)\cdot(x,y,-x,-y) = (x)(-x)(y,-y) = (-n_j)\restriction_{\pm\{x,y\}}.\end{aligned}$$

4. If $n_j$ fixes $x$ and moves $y$, then

$$\begin{aligned}(k_m n_j k_m)\restriction_{\pm\{x,y\}} &= (x,y)(-x,-y)\cdot((x)(-x)(y,-y)\cdot(x,y)(-x,-y)) \\ &= (x,y)(-x,-y)\cdot(x,-y,-x,y) = (x,-x)(y)(-y) = (-n_j)\restriction_{\pm\{x,y\}}.\end{aligned}$$

Consider $k_m = \psi_m L_{i_m}$ acting on elements of $N^*$, $T_x T_e = (x,-x)(e,-e)$ (where $1 \neq x \in Q_n/\{1,-1\}$) and $L_{-1}T_e = (1,-1)(e,-e)$.

1. Let $m < n$, i.e., $i_m \neq e$, then
   (a) If $x = i_m$, then $k_m(x) \in \pm\{i_m^2\} = \pm\{1\}$, and $k_m(e) \in \pm\{i_m e\}$. It follows that $(\phi_{k_m})\restriction_{\pm\{x,1,e,i_m e\}} = -id$ and $(\phi_{k_m}) = id$ otherwise.
   (b) If $x = i_m e$, then $k_m(x) \in \pm\{i_m^2 e\} = \pm\{e\}$, and $k_m(e) \in \pm\{i_m e\} = \pm\{x\}$. It follows that $(\phi_{k_m}) = id$.
   (c) If $k_m$ is acting on $L_{-1}T_e$, then $k_m(-1) \in \pm\{i_m\}$, and $k_m(e) \in \pm\{i_m e\}$. It follows that $(\phi_{k_m})\restriction_{\pm\{1,e,i_m,i_m e\}} = -id$ and $(\phi_{k_m}) = id$ otherwise.
   (d) In all other cases, $k_m(x) \in \pm\{i_m x\}$, and $k_m(e) \in \pm\{i_m e\}$. It follows that $(\phi_{k_m})\restriction_{\pm\{x,i_m x,e,i_m e\}} = -id$ and $(\phi_{k_m}) = id$ otherwise.

2. If $i_m = e$, then
   (a) If $k_n$ is acting on $L_{-1}T_e$, then $k_n(-1) \in \pm\{e\}$, and $k_n(e) \in \pm\{e^2\} = \pm\{1\}$. It follows that $(\phi_{k_n}) = -id$ and $\phi_{k_n} = id$.
   (b) In all other cases, $k_n(x) \in \pm\{i_n x\}$, and $k_n(e) \in \pm\{1\}$. It follows that $(\phi_{k_n})\restriction_{\pm\{x,i_n x,e,1\}} = -id$ and $(\phi_{k_n}) = id$ otherwise.

Summarizing,

$$
\begin{aligned}
\phi_{k_m}(L_{-1}T_e) &= \phi_{k_m}(T_{i_k}T_e) = L_{-1}T_e \cdot T_{i_k}T_e \cdot T_{i_k e}T_e, \\
\phi_{k_m}(T_{i_k e}T_e) &= id, \\
\phi_{k_m}(T_xT_e) &= T_xT_e \cdot T_{i_k x}T_e \cdot T_{i_k e}T_e, \text{ where } x \notin \pm\{i_k, i_k e\}, m < n, \\
\phi_{k_n}(T_xT_e) &= L_{-1}T_e \cdot T_xT_e \cdot T_{xe}T_e, \\
\phi_{k_n}(L_{-1}T_e) &= id.
\end{aligned}
$$

This information allows us to construct Tables 4.1, 4.2.

$$
\phi_{k_m}(N^*) =
$$

$$
= \left(\begin{array}{cccc|cccc|c|ccccc}
1 & 0 & 0 & 0\dots0 & 1 & 0 & 0 & 0\dots0 & 1 & 0\dots0 & 0 & 0\dots0 & 0 \\
0 & 1 & 0 & 0\dots0 & 0 & 1 & 0 & 0\dots0 & 1 & 0\dots0 & 0 & 0\dots0 & 0 \\
0 & 0 & 1 & 0\dots0 & 0 & 0 & 1 & 0\dots0 & 1 & 0\dots0 & 0 & 0\dots0 & 0 \\
\dots & & & & & & & & & & & & \\
\hline
1 & 0 & 0 & 0\dots0 & 1 & 0 & 0 & 0\dots0 & 1 & 0\dots0 & 0 & 0\dots0 & 0 \\
0 & 1 & 0 & 0\dots0 & 0 & 1 & 0 & 0\dots0 & 1 & 0\dots0 & 0 & 0\dots0 & 0 \\
0 & 0 & 1 & 0\dots0 & 0 & 0 & 1 & 0\dots0 & 1 & 0\dots0 & 0 & 0\dots0 & 0 \\
\dots & & & & & & & & & & & & \\
\hline
0 & 0 & 0 & 0\dots0 & 0 & 0 & 0 & 0\dots0 & 0 & 0\dots0 & 0 & 0\dots0 & 0 \\
\hline
\dots & & & & & & & & & & & & \\
0 & 0 & 0 & 0\dots0 & 0 & 0 & 0 & 0\dots0 & 1 & 0\dots0 & 1 & 0\dots0 & 1 \\
\dots & & & & & & & & & & & & \\
0 & 0 & 0 & 0\dots0 & 0 & 0 & 0 & 0\dots0 & 1 & 0\dots0 & 1 & 0\dots0 & 1
\end{array}\right)
\left(\begin{array}{c}
L_{-1}T_e \\
T_{i_1}T_e \\
T_{i_2}T_e \\
\dots \\
\hline
T_{i_m}T_e \\
T_{i_1 i_m}T_e \\
T_{i_2 i_m}T_e \\
\dots \\
\hline
T_{i_m e}T_e \\
\hline
\dots \\
T_{i_1 \dots i_{m-1} i_{m+1} \dots e}T_e \\
\dots \\
T_{i_1 i_2 \dots e}T_e
\end{array}\right)
$$

Table 4.1: Action of $k_m$ on $N^*$, $m < n$

$$
\phi_{k_n}(N^*) = \left(\begin{array}{c|cccc|cccc}
0 & 0 & 0 & 0\dots0 & 0 & 0 & 0 & 0\dots0 & 0 \\
\hline
1 & 1 & 0 & 0\dots0 & 0 & 1 & 0 & 0\dots0 & 0 \\
1 & 0 & 1 & 0\dots0 & 0 & 0 & 1 & 0\dots0 & 0 \\
\dots & & & & & & & & \\
1 & 0 & 0 & 0\dots0 & 1 & 0 & 0 & 0\dots0 & 1 \\
\hline
1 & 1 & 0 & 0\dots0 & 0 & 1 & 0 & 0\dots0 & 0 \\
1 & 0 & 1 & 0\dots0 & 0 & 0 & 1 & 0\dots0 & 0 \\
\dots & & & & & & & & \\
1 & 0 & 0 & 0\dots0 & 1 & 0 & 0 & 0\dots0 & 1
\end{array}\right)
\left(\begin{array}{c}
L_{-1}T_e \\
\hline
T_{i_1}T_e \\
T_{i_2}T_e \\
\dots \\
T_{i_1 i_2 \dots i_{n-1}}T_e \\
\hline
T_{i_1 e}T_e \\
T_{i_2 e}T_e \\
\dots \\
T_{i_1 i_2 \dots e}T_e
\end{array}\right)
$$

Table 4.2: Action of $k_n$ on $N^*$

Consider, for example, $Q_3 = \mathbb{O}_{16}$, the octonion loop. The group $Inn(\mathbb{O}_{16}) \times Z(\mathbb{O}_{16})$ is generated by

$$\{n_1, \ldots, n_7\} = \{L_{-1}T_{i_3}, T_{i_1}T_{i_3}, T_{i_2}T_{i_3}, T_{i_1i_2}T_{i_3}, T_{i_1i_3}T_{i_3}, T_{i_2i_3}T_{i_3}, T_{i_1i_2i_3}T_{i_3}\}.$$

The group $K$ is generated by

$$\{k_1, k_2, k_3\} = \{T_{i_2}T_{i_3}T_{i_2i_3}L_{i_1}, T_{i_1i_2}T_{i_3}T_{i_1i_2i_3}L_{i_2}, T_{i_1i_3}T_{i_2i_3}T_{i_1i_2}L_{i_3}\}.$$

Tables 4.3, 4.4, and 4.5 show the linear transformations induced by the actions of $k_1, k_2$, and $k_3$ on the basis of $Inn(\mathbb{O}_{16}) \times Z(\mathbb{O}_{16})$.

$$(k_1)^{-1}\left(\begin{array}{c} L_{-1}T_{i_3} \\ \hline T_{i_1}T_{i_3} \\ T_{i_2}T_{i_3} \\ T_{i_1i_2}T_{i_3} \\ \hline T_{i_1i_3}T_{i_3} \\ T_{i_2i_3}T_{i_3} \\ T_{i_1i_2i_3}T_{i_3} \end{array}\right) k_1 = \left(\begin{array}{c|ccc|ccc} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right)\left(\begin{array}{c} L_{-1}T_{i_3} \\ \hline T_{i_1}T_{i_3} \\ T_{i_2}T_{i_3} \\ T_{i_1i_2}T_{i_3} \\ \hline T_{i_1i_3}T_{i_3} \\ T_{i_2i_3}T_{i_3} \\ T_{i_1i_2i_3}T_{i_3} \end{array}\right)$$

Table 4.3: Action of $k_1$ on the basis of $Inn(\mathbb{O}_{16}) \times Z(\mathbb{O}_{16})$

$$(k_2)^{-1}\left(\begin{array}{c} L_{-1}T_{i_3} \\ \hline T_{i_1}T_{i_3} \\ T_{i_2}T_{i_3} \\ T_{i_1i_2}T_{i_3} \\ \hline T_{i_1i_3}T_{i_3} \\ T_{i_2i_3}T_{i_3} \\ T_{i_1i_2i_3}T_{i_3} \end{array}\right) k_2 = \left(\begin{array}{c|ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right)\left(\begin{array}{c} L_{-1}T_{i_3} \\ \hline T_{i_1}T_{i_3} \\ T_{i_2}T_{i_3} \\ T_{i_1i_2}T_{i_3} \\ \hline T_{i_1i_3}T_{i_3} \\ T_{i_2i_3}T_{i_3} \\ T_{i_1i_2i_3}T_{i_3} \end{array}\right)$$

Table 4.4: Action of $k_2$ on the basis of $Inn(\mathbb{O}_{16}) \times Z(\mathbb{O}_{16})$

$$(k_3)^{-1}\left(\begin{array}{c} L_{-1}T_{i_3} \\ \hline T_{i_1}T_{i_3} \\ T_{i_2}T_{i_3} \\ T_{i_1i_2}T_{i_3} \\ \hline T_{i_1i_3}T_{i_3} \\ T_{i_2i_3}T_{i_3} \\ T_{i_1i_2i_3}T_{i_3} \end{array}\right)k_3 = \left(\begin{array}{c|ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)\left(\begin{array}{c} L_{-1}T_{i_3} \\ \hline T_{i_1}T_{i_3} \\ T_{i_2}T_{i_3} \\ T_{i_1i_2}T_{i_3} \\ \hline T_{i_1i_3}T_{i_3} \\ T_{i_2i_3}T_{i_3} \\ T_{i_1i_2i_3}T_{i_3} \end{array}\right)$$

Table 4.5: Action of $k_3$ on the basis of $Inn(\mathbb{O}_{16}) \times Z(\mathbb{O}_{16})$

## 4.4 Left and Right Inner Mapping Groups

It is well known that $Mlt_l(Q) \cong Mlt_r(Q)$ and $Inn_l(Q) \cong Inn_r(Q)$ in any inverse property loop $Q$. We give the proofs in Theorem 4.4.1 and Corollary 4.4.3 for completeness.

**Theorem 4.4.1.** *Let $Q$ be an inverse property loop. Then $Mlt_l(Q) \cong Mlt_r(Q)$.*

*Proof.* Define a partial mapping $f : Mlt_l(Q) \to Mlt_r(Q)$ by $f(L_a) = R_a^{-1}$. We want to extend this mapping to a homomorphism. Let $S \in Mlt_l(Q)$, then

$$S = \prod_{i=1}^{n} L_{a_i}^{\epsilon_i}, \quad a_i \in Q, \epsilon_i \in \{0, 1\}.$$

To verify that a mapping

$$f(S) = f(\prod_{i=1}^{n} L_{a_i}^{\epsilon_i}) = \prod_{i=1}^{n} R_{a_i}^{-\epsilon_i}$$

is well-defined, we show that if

$$S = \prod_{i=1}^{n} L_{a_i}^{\epsilon_i} = \prod_{j=1}^{m} L_{b_j}^{\phi_j},$$

then

$$f(S) = \prod_{i=1}^{n} R_{a_i}^{-\epsilon_i} = \prod_{j=1}^{m} R_{b_j}^{-\phi_j}.$$

Let $x \in Q$, then

$$\begin{aligned} a_n^{\epsilon_n}(\dots a_2^{\epsilon_2}(a_1^{\epsilon_1}x)) &= b_m^{\phi_m}(\dots b_2^{\phi_2}(b_1^{\phi_1}x)), \text{ and} \\ (a_n^{\epsilon_n}(\dots a_2^{\epsilon_2}(a_1^{\epsilon_1}x)))^{-1} &= (b_m^{\phi_m}(\dots b_2^{\phi_2}(b_1^{\phi_1}x)))^{-1}. \end{aligned}$$

Inverse property implies that $(xy)^{-1} = y^{-1}x^{-1}$, thus

$$(a_n^{\epsilon_n}(\dots a_2^{\epsilon_2}(a_1^{\epsilon_1}x)))^{-1} = ((x^{-1}a_1^{-\epsilon_1})a_2^{-\epsilon_2})\dots a_n^{-\epsilon_n} = \prod_{i=1}^{n} R_{a_i}^{-\epsilon_i}(x),$$

and

$$(b_m^{\phi_m}(\dots b_2^{\phi_2}(b_1^{\phi_1}x)))^{-1} = ((x^{-1}b_1^{-\phi_1})b_2^{-\phi_2})\dots b_m^{-\phi_m} = \prod_{j=1}^{m} R_{b_j}^{-\phi_j}(x).$$

We conclude that

$$\prod_{i=1}^{n} R_{a_i}^{-\epsilon_i} = \prod_{j=1}^{m} R_{b_j}^{-\phi_j}$$

and the mapping $f$ is well-defined. The mapping $f$ is a homomorphism since it has an inverse $g : Mlt_r(Q) \to Mlt_l(Q)$ defined by $g(R_a) = L_a^{-1}$. □

**Corollary 4.4.2.** *Let $Q_n$ be a Cayley–Dickson loop. Then $Mlt_l(Q_n) \cong Mlt_r(Q_n)$.*

**Corollary 4.4.3.** *Let $Q$ be an inverse property loop. Then $Inn_l(Q) \cong Inn_r(Q)$.*

*Proof.* Note that $f \restriction_{Inn_l(Q)}$ is an isomorphism from $Inn_l(Q)$ to $Inn_r(Q)$. If

$$\begin{aligned} S &= \prod_{i=1}^{n} L_{a_i}^{\epsilon_i} \in Inn_l(Q), \text{ then} \\ S(1) &= a_n^{\epsilon_n}(\dots a_2^{\epsilon_2}(a_1^{\epsilon_1}1)) = 1. \end{aligned}$$

Taking the inverse, we have

$$(a_n^{\epsilon_n}(\dots a_2^{\epsilon_2}(a_1^{\epsilon_1}1)))^{-1} = (((1a_1^{-\epsilon_1})a_2^{-\epsilon_2})\dots a_n^{-\epsilon_n}) = 1,$$

thus

$$f(Inn_l(Q)) = \prod_{i=1}^{n} R_{a_i}^{-\epsilon_i} \in Inn_r(Q). \qquad \square$$

In fact, a stronger statement holds for the Cayley–Dickson loops. As can be seen in the following Lemma, when $Q_n$ is a Cayley–Dickson loop, the left inner mapping groups $Inn_l(Q_n)$ are equal to the right inner mapping groups $Inn_r(Q_n)$.

**Lemma 4.4.4.** *Let $Q_n$ be a Cayley–Dickson loop. Then $Inn_l(Q_n) = Inn_r(Q_n)$, and $Inn(Q_n) = \langle T_x, L_{x,y} \mid x, y \in Q_n\rangle$.*

*Proof.* For all $x, y \in Q_n$, we have $L_{x,y} = R_{x,y}$ by Corollary 4.1.3. $\square$

Lemma 4.4.5 serves a purpose similar to that of Lemma 3.2.2, providing information about associators. Lemmas 4.4.5, 4.4.7 are used in the proof of Theorem 4.4.8.

**Lemma 4.4.5.** *Let $Q_n$ be a Cayley–Dickson loop, $i_k$ its canonical generator, $x \in Q_k$, $y \in Q_k e$, $n \geq 4$, and $k < n$. Then*

$$[i_k, x, y] = [x, i_k, y] = \begin{cases} 1, & \text{when } y \in Q_k e \setminus \pm\{e, i_k e, xe, xi_k e\}, \\ -1, & \text{otherwise.} \end{cases}$$

*Moreover, if $x \notin \pm\{1, i_k\}$, then*

$$\langle i_k, x, y\rangle \cong \begin{cases} \tilde{\mathbb{O}}_{16}, & \text{when } y \in Q_k e \setminus \pm\{e, i_k e, xe, xi_k e\}, \\ \mathbb{O}_{16}, & \text{otherwise.} \end{cases}$$

*Proof.* Since $x \in Q_k$ and $y \in Q_k e$, we get $y \notin \langle i_k, x\rangle$. Consider the loop $\langle i_k, x, y\rangle$. If $x \in \pm\{1, i_k\}$, then $\langle i_k, x, y\rangle \cong \mathbb{H}_8$ and $[i_k, x, y] = [x, i_k, y] = 1$. If $x \notin \pm\{1, i_k\}$, then $\langle i_k, x\rangle \cong \mathbb{H}_8$ and $|\langle i_k, x, y\rangle| = 16$ by Lemma 2.5.1. In this case, if $y \in \pm\{e, i_k e, xe, xi_k e\}$, then $\langle i_k, x, y\rangle = \pm\{1, x, i_k, xi_k, e, xe, i_k e, xi_k e\} \cong \mathbb{O}_{16}$ and $[i_k, x, y] = [x, i_k, y] = -1$ by Lemmas 3.2.2 and 2.4.2. It remains to consider $x \in Q_k \setminus \pm\{1, i_k\}$, $y \in Q_k e \setminus \pm$

$\{e, i_k e, xe, xi_k e\}$. We can write $y = ze$ for some $z \in Q_k$, then

$$\begin{aligned}
(i_k x)(ze) &= [i_k x, z, e]((i_k x)z)e = [i_k x, z, e][i_k, x, z](i_k(xz))e \\
&= [i_k x, z, e][i_k, x, z][i_k, xz, e]i_k((xz)e) \\
&= [i_k x, z, e][i_k, x, z][i_k, xz, e][x, z, e]i_k(x(ze)) \\
&= i_k(x(ze)), \\
(xi_k)(ze) &= [xi_k, z, e]((xi_k)z)e = [xi_k, z, e][x, i_k, z](x(i_k z))e \\
&= [xi_k, z, e][x, i_k, z][x, i_k z, e]x((i_k z)e) \\
&= [xi_k, z, e][x, i_k, z][x, i_k z, e][i_k, z, e]x(i_k(ze)) = x(i_k(ze)),
\end{aligned}$$

since $x, z \in Q_k$, and

$$\begin{aligned}
[i_k x, z, e] &= [i_k, x, z] = [i_k, xz, e] = [x, z, e] = -1, \\
[xi_k, z, e] &= [x, i_k, z] = [x, i_k z, e] = [i_k, z, e] = -1
\end{aligned}$$

by Lemmas 3.2.2 and 2.4.2. Thus

$$\begin{aligned}
[i_k, x, ze] &= [i_k, x, y] = 1, \\
[x, i_k, ze] &= [x, i_k, y] = 1.
\end{aligned}$$

If $|\langle i_k, x, y\rangle| = 16$ and $[i_k, x, y] = 1$, then $\langle i_k, x, y\rangle \cong \tilde{\mathbb{O}}_{16}$ by Lemmas 3.2.2 and 3.2.1. $\square$

**Lemma 4.4.6.** *Let $Q_n$ be a Cayley–Dickson loop, and let $x, y \in Q_n$ such that $x = (\bar{x}, x_n)$, $y = (\bar{y}, y_n)$, $\bar{x}, \bar{y} \in Q_{n-1}$, $x_n, y_n \in \{0, 1\}$. Then*

$$\begin{aligned}
L_{x,y}(z) &= [\bar{x}, \bar{y}]L_{x,y}(ze), \qquad (4.4.1) \\
L_{x,e} &= L_{xe,e}.
\end{aligned}$$

*Proof.* Let $z = (\bar{z}, z_n)$, $\bar{z} \in Q_{n-1}$, $z_n \in \{0,1\}$. By Lemma 2.4.4, $[\bar{x},\bar{y},\bar{z}] = [\bar{z},\bar{y},\bar{x}]$ for any $\bar{x},\bar{y},\bar{z} \in Q_{n-1}$. Using Lemma 2.4.10,

$$\begin{aligned}
[(\bar{y},0),(\bar{x},0),(\bar{z},0)] &= [\bar{y},\bar{x},\bar{z}],\\
[(\bar{y},0),(\bar{x},0),(\bar{z},0)] &= [\bar{y},\bar{x}][\bar{z},\bar{x},\bar{y}] = [\bar{x},\bar{y}][\bar{y},\bar{x},\bar{z}],\\
[(\bar{y},0),(\bar{x},1),(\bar{z},0)] &= [\bar{y},\bar{z}][\bar{x},\bar{y},\bar{z}][\bar{x},\bar{z},\bar{y}],\\
[(\bar{y},0),(\bar{x},1),(\bar{z},1)] &= [\bar{x},\bar{y}][\bar{y},\bar{z}][\bar{z},\bar{y},\bar{x}][\bar{y},\bar{z},\bar{x}] = [\bar{x},\bar{y}][\bar{y},\bar{z}][\bar{x},\bar{y},\bar{z}][\bar{x},\bar{z},\bar{y}],\\
[(\bar{y},1),(\bar{x},0),(\bar{z},0)] &= [\bar{x},\bar{z}][\bar{y},\bar{x},\bar{z}],\\
[(\bar{y},1),(\bar{x},0),(\bar{z},1)] &= [\bar{x},\bar{y}][\bar{x},\bar{z}][\bar{z},\bar{x},\bar{y}] = [\bar{x},\bar{y}][\bar{x},\bar{z}][\bar{y},\bar{x},\bar{z}],\\
[(\bar{y},1),(\bar{x},1),(\bar{z},0)] &= [\bar{z},\bar{y}][\bar{z},\bar{x}][\bar{x},\bar{y},\bar{z}][\bar{x},\bar{z},\bar{y}],\\
[(\bar{y},1),(\bar{x},1),(\bar{z},1)] &= [\bar{y},\bar{x}][\bar{y},\bar{z}][\bar{x},\bar{z}][\bar{z},\bar{y},\bar{x}][\bar{y},\bar{z},\bar{x}]\\
&= [\bar{x},\bar{y}][\bar{z},\bar{y}][\bar{z},\bar{x}][\bar{x},\bar{y},\bar{z}][\bar{x},\bar{z},\bar{y}],
\end{aligned}$$

and (4.4.1) follows.

If $x \in \pm\{1,e\}$, then $L_{x,e} = L_{xe,e} = id$. Otherwise,

$$L_{x,e}(z) = [e,x,z]z = \begin{cases} z, & \text{if } z \in \pm\{1,x,e,xe\},\\ -z & \text{otherwise,} \end{cases}$$

and

$$L_{xe,e}(z) = [e,xe,z]z = \begin{cases} z, & \text{if } z \in \pm\{1,x,e,xe\},\\ -z & \text{otherwise,} \end{cases}$$

thus $L_{x,e} = L_{xe,e}$. □

**Lemma 4.4.7.** *Let $Q_n$ be a Cayley–Dickson loop, $n \geq 4$. Then an inner mapping on $Q_n$*

$$h = \prod_{x \in Q_{n-2}/\{1,-1\}} L_{x,i_{n-1}}$$

*can be written as the following permutation*

$$h = \prod_{z \in (Q_n/\{1,-1\}) \setminus (Q_{n-1}/\{1,-1\})} (z, -z).$$

*Proof.* Let $x \in Q_{n-2}/\{1,-1\}$. By (4.1.5),

$$L_{x,i_{n-1}}(z) = [i_{n-1}, x, z]z.$$

If $z \in \langle x, i_{n-1} \rangle = \pm\{1, x, i_{n-1}, xi_{n-1}\}$, then $[i_{n-1}, x, z] = 1$. If $z \in Q_{n-1} \setminus \pm\{1, x, i_{n-1}, xi_{n-1}\}$, then $[i_{n-1}, x, z] = -1$ by Lemmas 3.2.2, 2.4.2. If $z \in \{e, xe, i_{n-1}e, xi_{n-1}e\}$, then

$$\langle i_{n-1}, x, z \rangle = \{1, x, i_{n-1}, xi_{n-1}, e, xe, i_{n-1}e, xi_{n-1}e\} \cong \mathbb{O}_{16}$$

and $[i_{n-1}, x, z] = -1$ by Lemmas 3.2.2, 2.4.2. If $z \in Q_{n-1}e \setminus \{e, xe, i_{n-1}e, xi_{n-1}e\}$, then $[i_{n-1}, x, z] = 1$ by Lemma 4.4.5. Summarizing, we have

$$L_{x,i_{n-1}}(z) = \begin{cases} z, & \text{when } z \in \pm\{1, x, i_{n-1}, xi_{n-1}\} \cup (Q_{n-1}e \setminus \{e, xe, i_{n-1}e, xi_{n-1}e\}), \\ -z, & \text{otherwise.} \end{cases}$$

Next, consider a mapping

$$h = \prod_{x \in Q_{n-2}/\{1,-1\}} L_{x,i_{n-1}}.$$

If $z \in \pm\{1, i_{n-1}\}$, then clearly $h(z) = z$. If $z \in Q_{n-2} \setminus \pm \{1\}$, then $L_{x,i_{n-1}}(z) = -z$ for all $x \neq \pm z$, there is an even number (in fact, $2^{n-2} - 2$) of such mappings, and therefore $h(z) = z$. If $z \in Q_{n-2}i_{n-1} \setminus \pm \{i_{n-1}\}$, then $z = yi_{n-1}$ for some $y \in Q_{n-2}$, and $L_{x,i_{n-1}}(z) = -z$ for all $x \neq \pm y$, there is $2^{n-2} - 2$ such mappings, and therefore $h(z) = z$. We get $h(z) = z$ for $z \in Q_{n-1}$. Consider $z \in Q_{n-1}e$. If $z \in \pm\{e, i_{n-1}e\}$, then $L_{x,i_{n-1}}(z) = -z$ for all $x \neq 1$, there is $2^{n-2} - 1$ such mappings, and thus $h(z) = -z$.

Finally, if $z \in Q_{n-1}e \backslash \{e, i_{n-1}e\}$, then either $z = ye$, or $z = yi_{n-1}e$ for some $y \in Q_{n-2}$, and $L_{x,i_{n-1}}(z) = -z$ only when $x = \pm y$, again, $h(z) = -z$. We get $h(z) = -z$ for $z \in Q_{n-1}e$. □

**Theorem 4.4.8.** *Let $Q_n$ be a Cayley–Dickson loop. Then $Inn_l(Q_n)$ is an elementary abelian 2-group of order $2^{2^{n-1}-1}$.*

*Proof.* Let $x \in Q_{n-1}/\{1,-1\}$, $x \neq 1$. Then by Lemma 4.1.2

$$L_{x,e}L_{i_{n-1},e} = (x,-x)(i_{n-1},-i_{n-1})(xe,-xe)(i_{n-1}e,-i_{n-1}e).$$

For every $f \in Inn_l(Q_n)$, there is $\tilde{f} = L_{x,e}L_{i_{n-1},e}f \in Inn_l(Q_n)$ such that

$$\tilde{f}(z) = \begin{cases} -f(z), & \text{when } z \in \{x, i_{n-1}, xe, i_{n-1}e\}, \\ f(z), & \text{otherwise.} \end{cases}$$

There are $2^{n-1} - 2$ distinct inner mappings $L_{x,e}L_{i_{n-1},e}$, $x \in Q_{n-1}/\{1,-1\}$, $x \neq 1$, they generate a group of order $2^{2^{n-1}-2}$. Let

$$h = \prod_{y \in Q_{n-2}/\{1,-1\}} L_{y,i_{n-1}} = \prod_{z \in (Q_n/\{1,-1\}) \backslash (Q_{n-1}/\{1,-1\})} (z,-z).$$

be the mapping constructed in Lemma 4.4.7. For every $f \in Inn_l(Q_n)$, a mapping $\tilde{f} = hf$ satisfies

$$\tilde{f}(z) = \begin{cases} f(z), & \text{when } z \in Q_{n-1}, \\ -f(z), & \text{otherwise.} \end{cases}$$

The group

$$G = \langle L_{x,e}L_{i_{n-1},e}, h \mid 1 \neq x \in Q_{n-1}/\{1,-1\} \rangle$$

therefore has order $2^{2^{n-1}-1}$ and is a subgroup of $Inn_l(Q_n)$.

To show that $Inn_l(Q_n) = G$, recall that $L_{x,y}(z) = [\bar{x},\bar{y}]L_{x,y}(ze)$ for $\bar{x},\bar{y} \in Q_{n-1}$, by (4.4.1). The value of $L_{x,y}(ze)$ is therefore uniquely determined by that of $L_{x,y}(z)$, moreover, $L_{x,y}(1) = 1$, thus $Inn_l(Q_n)$ has order at most $2^{\frac{|Q_{n-1}|}{2}-1} = 2^{2^{n-1}-1}$. □

## 4.5 Left and Right Multiplication Groups

Let $Q_n$ be a Cayley–Dickson loop. A group $Mlt_l(Q_n)$ is a proper subgroup of $Mlt(Q_n)$ by Theorems 4.1.4, 4.4.8, we have $Mlt_l(Q_n)_1 = Inn_l(Q_n) < Inn(Q_n) = Mlt(Q_n)_1$. We showed in Corollary 4.4.2 that $Mlt_l(Q_n) \cong Mlt_r(Q_n)$.

**Theorem 4.5.1.** *Let $Q_n$ be a Cayley–Dickson loop, $n \geq 2$. Then $Mlt_l(Q_n) \cong (Inn_l(Q_n) \times Z(Q_n)) \rtimes K$, where $K$ is the group constructed in Lemma 4.2.6. In particular, $Mlt_l(Q_n) \cong ((\mathbb{Z}_2)^{2^{n-1}-1} \times \mathbb{Z}_2) \rtimes (\mathbb{Z}_2)^n$.*

*Proof.* Since $Z(Q_n) \leq Mlt_l(Q_n)$, let $N = \langle Inn_l(Q_n), Z(Q_n)\rangle = Inn_l(Q_n)Z(Q_n)$. A group $Inn_l(Q_n)$ stabilizes 1, therefore $Inn_l(Q_n) \cap Z(Q_n) = 1$. The index $[N : Inn_l(Q_n)] = 2$, therefore $Inn_l(Q_n) \trianglelefteq N$, and $Z(Q_n) \trianglelefteq Mlt_l(Q_n)$ implies $Z(Q_n) \trianglelefteq N$. It follows that $N = Inn_l(Q_n) \times Z(Q_n)$. Let $G = Mlt_l(Q_n)$ and $K$ be the group constructed in Lemma 4.2.6. We want to show that $G = N \rtimes K$.

1. Let $\alpha \in N, g \in G$. There exist $x \in Q_n, \beta \in Inn_l(Q_n)$ such that $g = \beta L_x$. Consider $g\alpha g^{-1}$ acting on 1,

$$\begin{aligned} g\alpha g^{-1}(1) &= \beta L_x \alpha(\beta L_x)^{-1}(1) = \beta L_x \alpha L_x^{-1} \underbrace{\beta^{-1}(1)}_{1} \\ &= \beta \underbrace{L_x \alpha L_x^{-1}(1)}_{\pm 1} = \pm\beta(1) = \pm 1. \end{aligned}$$

   This shows that $g\alpha g^{-1} \in Inn_l(Q_n) \cup (-Inn_l(Q_n)) = N$, so $N$ is normal in $G$. Recall a mapping $h$ constructed in Lemma 4.4.7,

$$h = \prod_{z \in (Q_n/\{1,-1\}) \setminus (Q_{n-1}/\{1,-1\})} (z, -z).$$

Note that by Lemma 4.1.2

$$T_x T_{xe} T_e = \prod_{1,e,x,xe\neq z\in Q_n/\{1,-1\}} (z,-z) = L_{x,e},$$

which allows to rewrite the construction in Lemma 4.2.6 as follows:

$$\begin{aligned}
s_{1,2} &= \{1, i_2\}, \quad s_{2,2} = \{1, i_1 i_2\}, \\
s_{k,n} &= \{x, i_n x \mid x \in s_{k,n-1}\}, \quad k \in \{1,\dots,n-1\}, \\
s_{n,n} &= \left\{\prod_{j=1}^{n} i_j^{p_j} \mid p_j \in \{0,1\}, \sum_{j=1}^{n} p_j \in 2\mathbb{Z}\right\}, \\
\bar{s}_{n,n} &= \left\{\prod_{j=1}^{n} i_j^{p_j} \mid p_j \in \{0,1\}, \sum_{j=1}^{n} p_j \notin 2\mathbb{Z}\right\}, \\
g_{k,n} &= (\prod_{x\in s_{k,n}} T_x) L_{i_k} = (\prod_{x\in s_{k,n-1}} T_x T_{xe}) T_e L_{i_k} \\
&= (\prod_{x\in s_{k,n-1}} T_x T_{xe})(\prod_{x\in\{1,\dots,2^{n-2}-1\}} T_e) L_{i_k} \\
&= (\prod_{x\in s_{k,n-1}} T_x T_{xe} T_e) L_{i_k} \\
&= (\prod_{x\in s_{k,n-1}} L_{x,e}) L_{i_k}, \quad k \in \{1,\dots,n-1\}, \\
g_{n,n} &= (\prod_{x\in s_{n,n}} T_x) L_{i_k} = (\prod_{x\in s_{n-1,n-1}} T_x \prod_{x\in \bar{s}_{n-1,n-1}} T_{xe}) L_{i_k} \\
&= (\prod_{x\in \bar{s}_{n,n}} (x,-x)) L_{i_k} \\
&= (\prod_{x\in \bar{s}_{n-1,n-1}} (x,-x))(\prod_{x\in s_{n-1,n-1}} (xe,-xe)) L_{i_k} \\
&= (\prod_{x\in \bar{s}_{n-1,n-1}} (x,-x)(xe,-xe))(\prod_{x\in Q_{n-1}e} (x,-x)) L_{i_k} \\
&= (\prod_{x\in s_{n-1,n-1}} L_{x,e}) h L_{i_k}, \\
K &= K_n = \langle g_{1,n}, g_{2,n}, \dots, g_{n,n} \rangle.
\end{aligned}$$

Thus $K \leq Mlt_l(Q_n)$.

2. By (4.2.1), (4.2.2), $K$ contains a unique element $g$ such that $g(1) \in \{1,-1\}$. Since $K$ is a group, $g = id$, thus $N \cap K = id$.

3. We established that $N \trianglelefteq G, K \leq G$, and $N \cap K = id$, therefore $N \rtimes K \leq G$. Recall that

$$\begin{aligned} [Mlt_l(Q_n) : Inn_l(Q_n)] &= |Q_n|, \text{ thus} \\ [Mlt_l(Q_n) : (Inn_l(Q_n) \times Z(Q_n))] &= [Mlt_l(Q_n) : Inn_l(Q_n)]/2 = 2^n = |K|, \end{aligned}$$

and $(Inn_l(Q_n) \times Z(Q_n)) \rtimes K \cong Mlt_l(Q_n)$ follows. $\square$

# Chapter 5

# Subloops

In this chapter we describe the progress on the study of the subloop structure of the Cayley–Dickson loops, and state several open problems along the way.

## 5.1 Number of Subloops

We count the number of subloops of a given size of a Cayley–Dickson loop $Q_n$ using the vector space structure of $Q_n/Z(Q_n)$.

**Theorem 5.1.1.** *Cayley–Dickson loop $Q_n$ contains one subloop of orders 1 and 2, and*

$$\eta(k) = \prod_{j=1}^{k-1} \frac{(2^{n-j+1} - 1)}{(2^{k-j} - 1)} \tag{5.1.1}$$

*subloops of order $2^k$, $2 \le k \le n$. Moreover, $Q_n$ contains the same number of subloops of order $2^k$ and $2^{n-k+2}$, whenever $1 \le k \le n$.*

*Proof.* The only subloop of $Q_n$ of order 1 is $\langle 1 \rangle$, the subloop of order 2 is $\langle -1 \rangle$. Each element $x \in Q_n \setminus \pm\{1\}$ has order 4 and thus generates a subloop $\langle x \rangle = \pm\{1, x\}$. There are $2^n - 1$ such subloops. Let $n \ge 3$, $3 \le k \le n$. By Lemma 2.3.2, the center of $Q_n$ is $Z(Q_n) = \{1, -1\}$. By Theorem 2.3.1, the group $Q_n/Z(Q_n)$ is a vector space over $\mathbb{Z}_2$. The order of $Q_n$ is $2^{n+1}$, and every minimal generating set is of size $n$ by Lemma 2.5.1-(4). These generating sets are in one-to-one correspondence with bases in the vector space $Q_n/Z(Q_n)$. Hence to find the number of subloops of order $2^k$ (such subloops are $(k-1)$-generated by Lemma 2.5.1-(4)) we need to find the number of possibilities to choose $k-1$ linearly independent vectors in $Q_n/Z(Q_n)$. There are

$$\begin{aligned}\eta(k) &= \frac{(2^n-1)(2^n-2)\dots(2^n-2^{k-2})}{(2^{k-1}-1)(2^{k-1}-2)\dots(2^{k-1}-2^{k-2})} = \frac{\prod_{j=1}^{k-1}(2^n-2^{j-1})}{\prod_{j=1}^{k-1}(2^{k-1}-2^{j-1})} \\ &= \prod_{j=1}^{k-1}\frac{(2^n-2^{j-1})}{(2^{k-1}-2^{j-1})} = \prod_{j=1}^{k-1}\frac{(2^{n-j+1}-1)}{(2^{k-j}-1)}\end{aligned}$$

such possibilities. Moreover,

$$\begin{aligned}\eta(k) &= \prod_{j=1}^{k-1}\frac{(2^{n-j+1}-1)}{(2^{k-j}-1)} = \prod_{j=1}^{k-1}\frac{(2^{n-j+1}-1)}{(2^{k-j}-1)}\cdot\frac{(2^{n-k+1}-1)(2^{n-k}-1)\dots(2^k-1)}{(2^{n-k+1}-1)(2^{n-k}-1)\dots(2^k-1)} \\ &= \frac{(2^n-1)(2^{n-1}-1)\dots(2^{n-k+2}-1)(2^{n-k+1}-1)(2^{n-k}-1)\dots(2^k-1)}{(2^{n-k+1}-1)(2^{n-k}-1)\dots(2^k-1)(2^{k-1}-1)(2^{k-2}-1)\dots(2-1)} \\ &= \prod_{j=1}^{n-k+1}\frac{(2^{n-j+1}-1)}{(2^{n-k+2-j}-1)} = \eta(n-k+2). \qquad \square\end{aligned}$$

A loop $Q$ is *subdirectly irreducible* if there is a nontrivial $M \trianglelefteq Q$ such that for all nontrivial $N \trianglelefteq Q$ we have $M \le N$. Cayley–Dickson loops $Q_n$ are Hamiltonian and subdirectly irreducible (with $M = \{1,-1\}$ by Lemma 2.3.2). The subspaces of a vector space form a modular lattice, thus $Q_n$ has a modular subloop lattice. The Hasse diagram of the subloop lattice of the octonion loop $\mathbb{O}_{16}$ and, in fact, of any subloop $\langle x, y, z\rangle$ of order 16 of $Q_n$ is shown in Figure 5.1 (figure is similar to the diagrams of Tilman Piesk). In the figure, each of 16 cells of a table corresponds to an element of $\langle x, y, z\rangle$, see the legend in the bottom right corner.

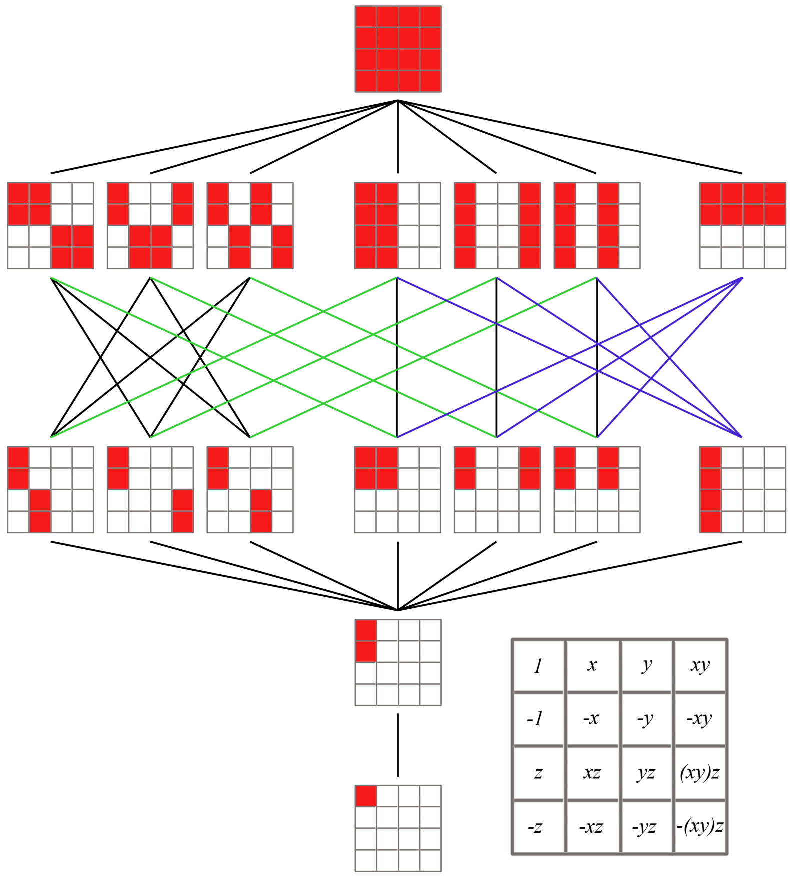


Figure 5.1: Subloop lattice of $\langle x, y, z \rangle$ of order 16

## 5.2 Subloops of Order 32

The loop $\mathbb{T}_{64}$ contains maximal subloops of four isomorphism types: the sedenion loop $\mathbb{S}_{32}$ and the quasisedenion loops $\tilde{\mathbb{S}}^1_{32}$, $\tilde{\mathbb{S}}^2_{32}$, $\tilde{\mathbb{S}}^3_{32}$ (see [7]). As a step toward the understanding of the subloop structure of the Cayley–Dickson loops, we would like to extend the results of Theorem 2.2.1 and Lemma 3.2.1 and answer the following question, confirmed by GAP calculations with the Cayley–Dickson loops of order up to 128.

**Question 5.2.1.** *Let $Q_n$ be a Cayley–Dickson loop. Is every subloop of order* 32 *of $Q_n$ isomorphic to a maximal subloop of $\mathbb{T}_{64}$ (the sedenion loop $\mathbb{S}_{32}$, or one of the quasisedenion loops $\tilde{\mathbb{S}}^1_{32}, \tilde{\mathbb{S}}^2_{32}, \tilde{\mathbb{S}}^3_{32}$)?*

We would like to prove this statement by extending the approach described in Section 3.2. Let $S = \langle a, b, c\rangle$ such that $|S| = 16$, let $u \notin S$ and $T = S \cup Su$. To specify $T$ it suffices to know the associators $[x, y, u]$, where $x, y \in S = \pm\{1, a, b, ab, c, ac, bc, (ab)c\}$. Using lemmas from Section 2.4, we systematically consider all associators:

$$
\begin{array}{ll}
[a,b,u], & [ab,ac,u], \\
[a,c,u], & [ab,bc,u] = [ab,ac,u], \\
[a,ab,u] = [a,b,u], & [ab,abc,u] = [ab,c,u], \\
[a,ac,u] = [a,c,u], & [ac,a,u], \\
[a,bc,u], & [ac,b,u], \\
[a,abc,u] = [a,bc,u], & [ac,c,u] = [ac,a,u], \\
[b,a,u], & [ac,ab,u], \\
[b,c,u], & [ac,bc,u] = [ac,ab,u], \\
[b,ab,u] = [b,a,u], & [ac,abc,u] = [ac,b,u], \\
[b,ac,u], & [bc,a,u], \\
[b,bc,u] = [b,c,u], & [bc,b,u], \\
[b,abc,u] = [b,ac,u], & [bc,c,u] = [bc,b,u], \\
[c,a,u], & [bc,ab,u], \\
[c,b,u], & [bc,ac,u] = [bc,ab,u], \\
[c,ab,u], & [bc,abc,u] = [bc,a,u], \\
[c,ac,u] = [c,a,u], & [abc,a,u], \\
[c,bc,u] = [c,b,u], & [abc,b,u], \\
[c,abc,u] = [c,ab,u], & [abc,c,u], \\
[ab,a,u], & [abc,ab,u] = [abc,c,u], \\
[ab,b,u] = [ab,a,u], & [abc,ac,u] = [abc,b,u], \\
[ab,c,u], & [abc,bc,u] = [abc,a,u].
\end{array}
$$

Table 5.1 summarizes these calculations and shows the associators $[x, y, u]$.

| $x \backslash y$ | $a$ | $b$ | $ab$ | $c$ | $ac$ | $bc$ | $(ab)c$ |
|---|---|---|---|---|---|---|---|
| $a$ | 1 | $[a,b,u]$ | $[a,b,u]$ | $[a,c,u]$ | $[a,c,u]$ | $[a,bc,u]$ | $[a,bc,u]$ |
| $b$ | $[b,a,u]$ | 1 | $[b,a,u]$ | $[b,c,u]$ | $[b,ac,u]$ | $[b,c,u]$ | $[b,ac,u]$ |
| $ab$ | $[ab,a,u]$ | $[ab,a,u]$ | 1 | $[ab,c,u]$ | $[ab,ac,u]$ | $[ab,ac,u]$ | $[ab,c,u]$ |
| $c$ | $[c,a,u]$ | $[c,b,u]$ | $[c,ab,u]$ | 1 | $[c,a,u]$ | $[c,b,u]$ | $[c,ab,u]$ |
| $ac$ | $[ac,a,u]$ | $[ac,b,u]$ | $[ac,ab,u]$ | $[ac,a,u]$ | 1 | $[ac,ab,u]$ | $[ac,b,u]$ |
| $bc$ | $[bc,a,u]$ | $[bc,b,u]$ | $[bc,ab,u]$ | $[bc,b,u]$ | $[bc,ab,u]$ | 1 | $[bc,a,u]$ |
| $(ab)c$ | $[abc,a,u]$ | $[abc,b,u]$ | $[abc,c,u]$ | $[abc,c,u]$ | $[abc,b,u]$ | $[abc,a,u]$ | 1 |

Table 5.1: Associators $[x, y, u]$ of $\langle a, b, c, u\rangle$ of order 32

Thus we need 21 associators to determine $T$. Experiments in GAP show that some of the combinations of these associators indeed result in loops isomorphic to one of the maximal subloops of $\mathbb{T}_{64}$. However, there exist combinations such that $T$ is not of one of the 4 types. This could either be an indication that there are additional relations between the 21 associators, or, less likely, it could mean that not every subloop of order 32 in a Cayley–Dickson loop is a subloop of $\mathbb{T}_{64}$.

## 5.3 Incidence Tetrahedra for Sedenion and Quasisedenion Loops

In Figure 5.2 we provide the incidence tetrahedron for the sedenion loop, generalizing the idea of the octonion multiplication Fano plane. The tetrahedron contains 15 points (representing non-identity sedenion units) and 35 lines (representing multiplication of these units), with exactly 7 lines through every point and exactly 3 points on every line. The arrows point in the direction of multiplication. Tetrahedron contains

- 4 Fano plane faces and 1 additional internal point

- 4 lines from a vertex to the middle of the opposite face
- 3 lines from an edge middle to the opposite edge middle
- 6 lines from a face middle to a face middle

The Fano plane faces are the copies of the octonion loop multiplication plane. The vertex 8 represents a generator used to construct $\mathbb{S}_{32}$ from $\mathbb{O}_{16}$. It is connected to the points $1, \ldots, 7$ of the $\mathbb{O}_{16}$ plane by

$$8 \cdot (8 + j) = j, \quad j \in \{1, \ldots, 7\}.$$

The anti-commutativity law holds

$$j \cdot k = m \Rightarrow k \cdot j = -m.$$

Together with the multiplicative identity and the fact that $\{1, \ldots 7\}$ are square roots of $-1$, the tetrahedron is sufficient to construct the multiplication table of the sedenion loop.

Incidence tetrahedra for the quasisedenion loops $\tilde{\mathbb{S}}^1_{32}, \tilde{\mathbb{S}}^2_{32}, \tilde{\mathbb{S}}^3_{32}$ are provided in Figures 5.3, 5.4, and 5.5.

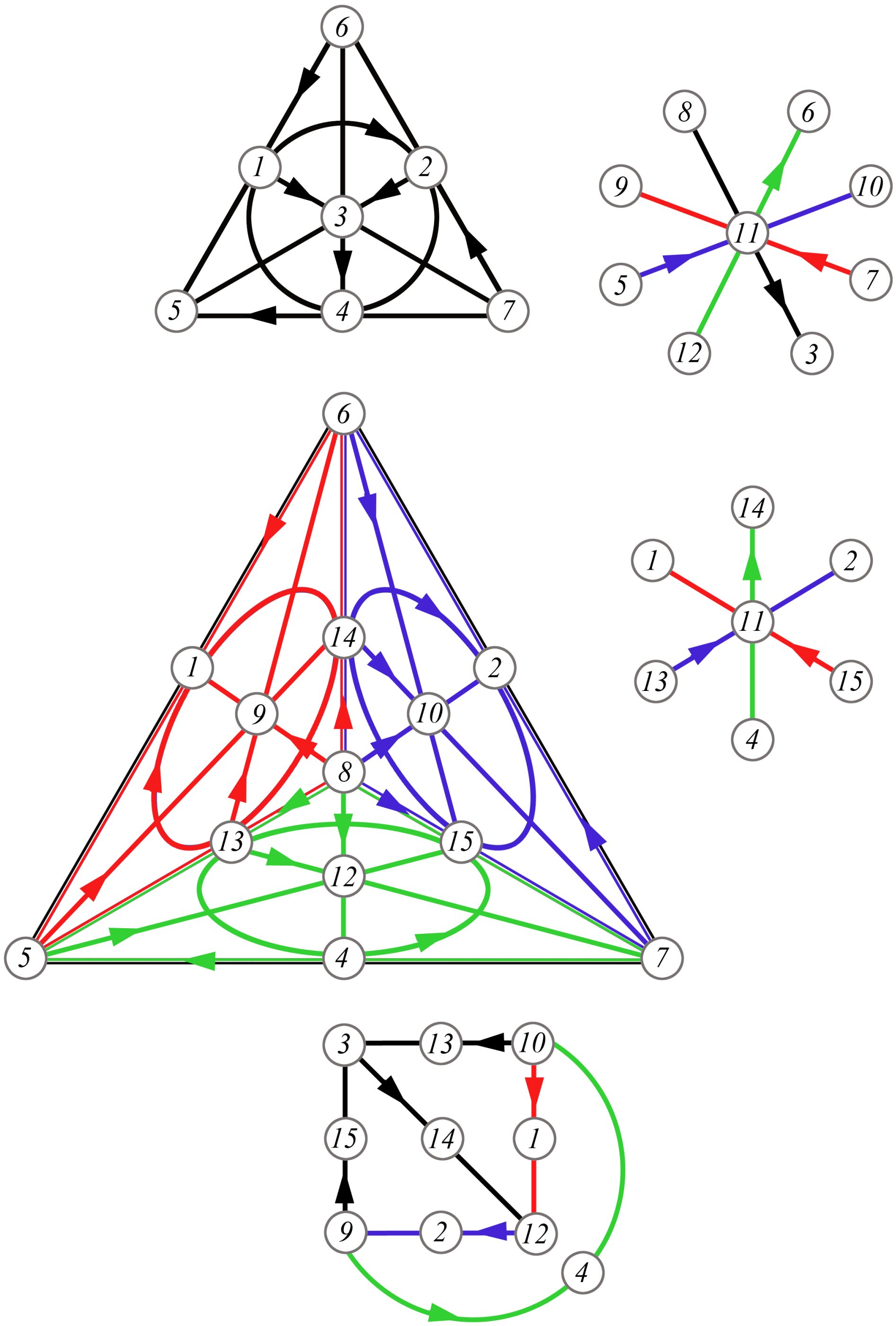


Figure 5.2: Sedenion loop multiplication tetrahedron

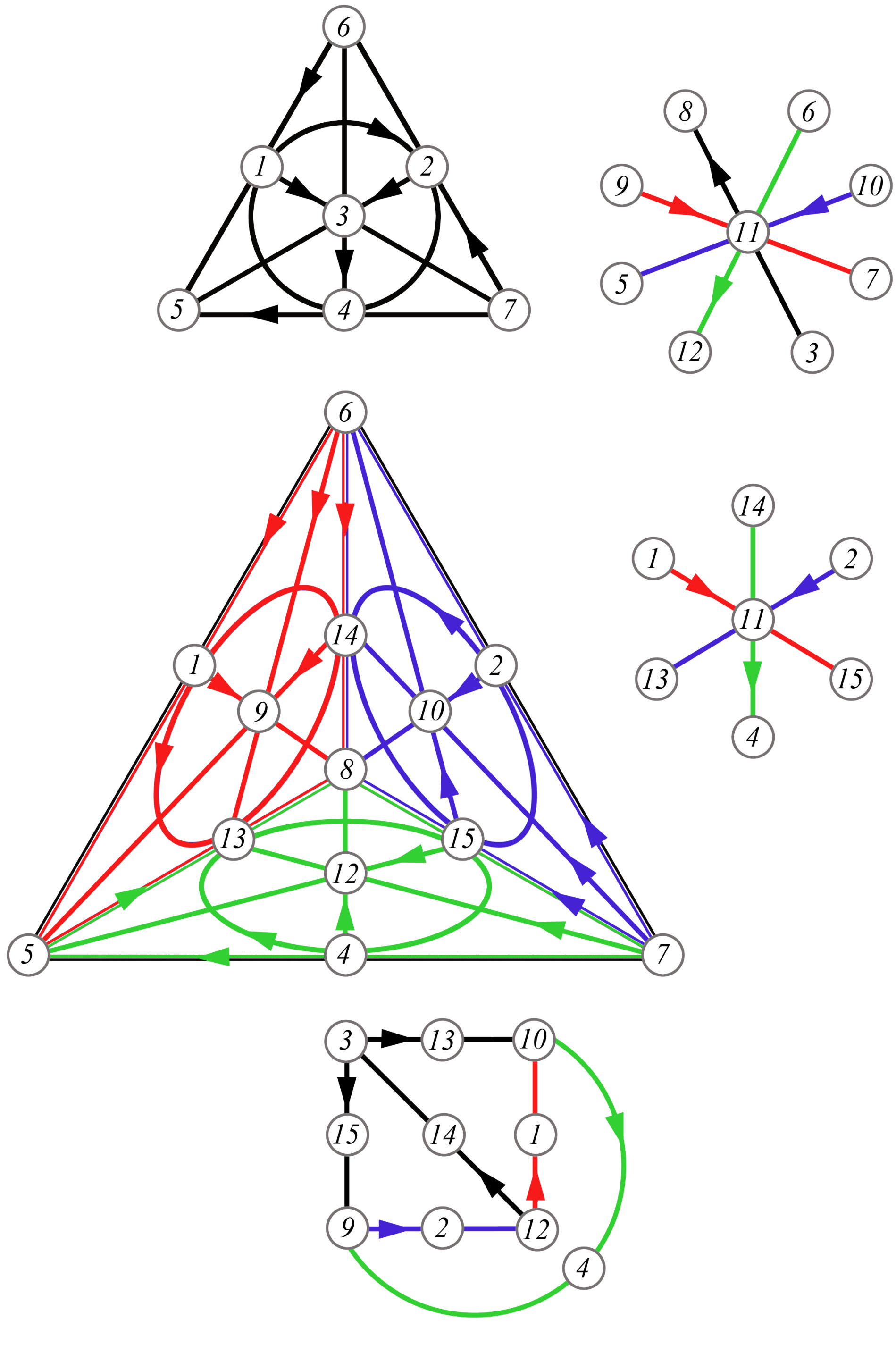

Figure 5.3: Quasisedenion loop $\tilde{\mathbb{S}}_{32}^{1}$ multiplication tetrahedron

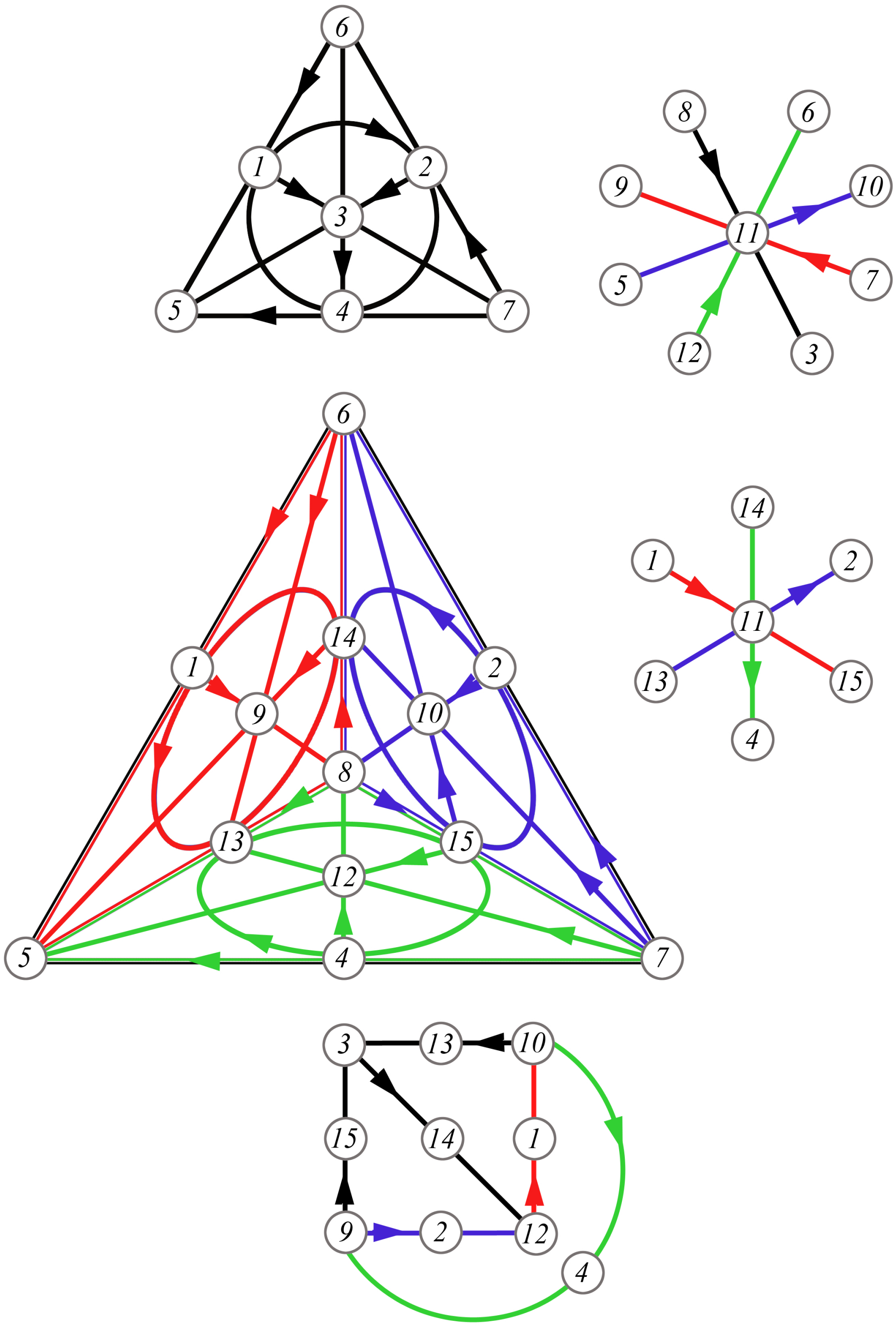


Figure 5.4: Quasisedenion loop $\tilde{\mathbb{S}}^2_{32}$ multiplication tetrahedron

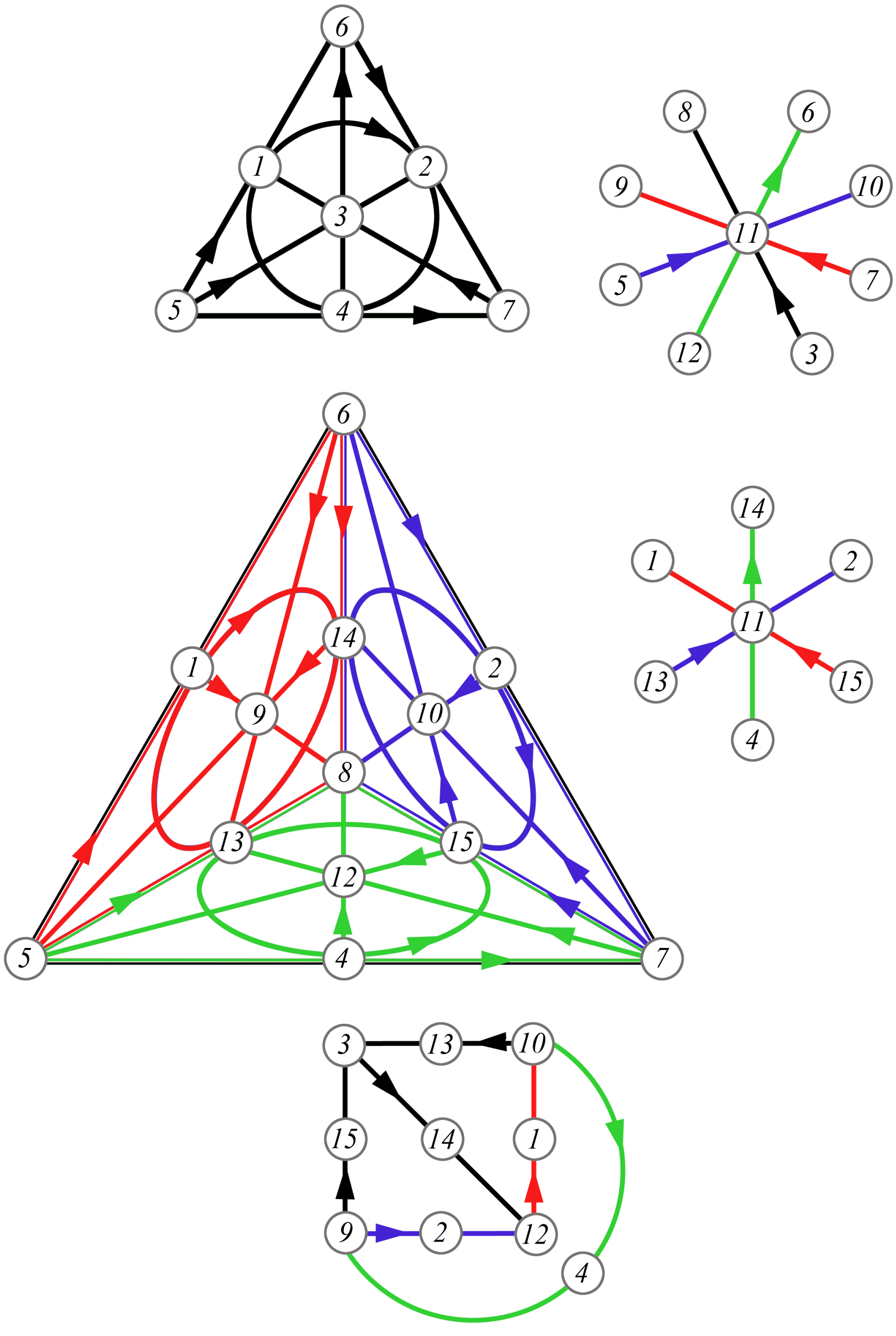


Figure 5.5: Quasisedenion loop $\tilde{\mathbb{S}}^3_{32}$ multiplication tetrahedron

## 5.4 Isomorphism Types of Maximal Subloops

We would like to find an invariant that distinguishes the isomorphism types of maximal (index 2) subloops of the Cayley–Dickson loops. The quaternion and octonion loops contain one type of such subloop: complex and quaternion groups, respectively (see Theorem 2.2.1). Subloops of index 2 of the sedenion loop $\mathbb{S}_{32}$ are either isomorphic to the octonion loop $\mathbb{O}_{16}$, or the quasioctonion loop $\tilde{\mathbb{O}}_{16}$ (see Lemma 3.2.1). The loop $\mathbb{T}_{64}$ contains the sedenion loop $\mathbb{S}_{32}$ and three pairwise nonisomorphic quasisedenion loops $\tilde{\mathbb{S}}^1_{32}$, $\tilde{\mathbb{S}}^2_{32}$, $\tilde{\mathbb{S}}^3_{32}$. GAP calculations show that the loops $Q_6$ (of order 128) and $Q_7$ (of order 256) contain 8 and 16 pairwise nonisomorphic maximal subloops, respectively.

In Lemma 3.3.4 we establish that starting at $\mathbb{S}_{32}$ every Cayley–Dickson loop contains at least two isomorphism types of maximal subloops. In particular, any subloop of $Q_n$ of the third type is not a Cayley–Dickson loop. However, we did not prove the following statement, which is confirmed in GAP for $n \leq 7$.

**Conjecture 5.4.1.** *Maximal subloops of the second type of a Cayley–Dickson loop $Q_n$ are isomorphic to $Q_{n-1}$.*

We use the LOOPS package for GAP to computationally distinguish isomorphism types of maximal subloops. The space of possible isomorphisms between two loops of order $n$ contains $n!$ bijections, hence finding an isomorphism can be computationally hard. This problem is partially overcome in the package by using the *discriminator* function (described in [42, p.13]). The function employs the idea that an isomorphism should preserve certain invariants, and precalculates some inexpensive invariants that can reduce the number of possible images of an element. In particular, for $x \in Q$, let $I(x) = (|x|, s, t, p, f, (c_1, c_2, \ldots, c_n))$, where

$$
\begin{aligned}
s &= \left|\{y \in Q \mid x = y^2\}\right|, \\
t &= \left|\{y \in Q \mid x = y^3\}\right|, \\
f &= \left|\{y \in Q \mid x = y^4\}\right|, \\
p &= 1 \text{ if } x \in Z(Q), \text{ else } 0, \\
c_i &= \left|\{y \in Q \mid |y| = i, xy = yx\}\right|.
\end{aligned}
$$

For a loop $Q$ and an invariant $I$, let

$$
\begin{aligned}
d_I &= |\{x \in Q \mid I(x) = I\}|, \\
D(Q) &= \{(I(x), d_{I(x)}) \mid x \in Q\}.
\end{aligned}
$$

None of the above invariants, however, simplify computations for a Cayley–Dickson loop (all its subloops of size bigger than 4 share the same center, every noncentral element $x$ has order 4 and only commutes with elements of $\langle x \rangle$). We modified the *discriminator* function and added an invariant counting the number of associating triples for an element $x \in Q_n$:

$$
r = |\{(y, z) \mid y, z \in Q, x(yz) = (xy)z\}|.
$$

This invariant is very powerful and significantly improves computation time. For example, in the loop $Q_6$ of order 128 it distinguishes 6 out of 8 isomorphism types of maximal subloops (the subloops of 5 distinct isomorphism types have distinct discriminators, and subloops of 3 extremely similar isomorphism types share the same discriminator). Table 5.2 summarizes these observations. Note that the number of maximal subloops is given by (5.1.1).

| $Q_n$ | Max. subloops | Isom. classes | Representatives | Discr. types | Nonisom. w/same discr. |
|---|---|---|---|---|---|
| $Q_1 = \mathbb{C}_4$ | 1 | 1 | $\mathbb{R}_2$ | 1 | none |
| $Q_2 = \mathbb{H}_8$ | 3 | 1 | $\mathbb{C}_4$ | 1 | none |
| $Q_3 = \mathbb{O}_{16}$ | 7 | 1 | $\mathbb{H}_8$ | 1 | none |
| $Q_4 = \mathbb{S}_{32}$ | 15 | 2 | $\mathbb{O}_{16}$ and $\tilde{\mathbb{O}}_{16}$ | 2 | none |
| $Q_5 = \mathbb{T}_{64}$ | 31 | 4 | $\mathbb{S}_{32}$, $\tilde{\mathbb{S}}_{32}^1$, $\tilde{\mathbb{S}}_{32}^2$, $\tilde{\mathbb{S}}_{32}^3$ | 4 | none |
| $Q_6$ | 63 | 8 | $\mathbb{T}_{64}$, $\tilde{\mathbb{T}}_{64}^1, \dots, \tilde{\mathbb{T}}_{64}^7$ | 6 | 3 |
| $Q_7$ | 127 | 16 | | 8 | 7 and 3 |

Table 5.2: Subloops of index 2 of $Q_n$, $n \le 7$

We arrive at the following conjecture:

**Conjecture 5.4.2.** *There are $2^{n-3}$ isomorphism classes of maximal subloops of a Cayley–Dickson loop $Q_n$.*

Note that Corollary 3.2.3 might help to reflect the associating triples invariant. Observations described in Section 5.2 result in the following conjecture.

**Conjecture 5.4.3.** *If $S$ is a subloop of a Cayley–Dickson loop $Q_n$, then there exists $m \le n+1$ such that $S$ is a maximal subloop of $Q_m$.*

Conjecture 5.4.3 can be reduced to a slightly simpler Conjecture 5.4.4, as can be seen in Lemma 5.4.5.

**Conjecture 5.4.4.** *If $S$ is a subloop of a Cayley–Dickson loop $Q_n$ of index 4, then $S$ is a maximal subloop of $Q_{n-1}$.*

**Lemma 5.4.5.** *Let $Q_n$ be a Cayley–Dickson loop. If every subloop of index 4 of $Q_n$ is maximal in $Q_{n-1}$, then every subloop of $Q_n$ is maximal in $Q_m$, for some $m \le n+1$.*

*Proof.* Let $S \le Q_n$. If $S = Q_n$, then $S$ is maximal in $Q_{n+1}$. If $S$ is maximal in $Q_n$, we are done. Otherwise, $S$ is maximal in some proper subloop $K$ of $Q_n$. Proceed by induction on index of $S$ in $Q_n$. If index of $S$ is 4, then $S$ is maximal in $Q_{n-1}$. Suppose that every subloop of index $2^m$ is maximal in $Q_{n-m+1}$. If the index of $S$

is $2^{m+1}$, then $K$ has index $2^m$ and is maximal in $Q_{n-m+1}$, thus $S$ has index 4 in $Q_{n-m+1}$ and is maximal in $Q_{n-m}$. □

We showed in Theorem 2.6.1 that every Cayley–Dickson loop is Hamiltonian. The answer to the following question would be of interest.

**Question 5.4.6.** *Is every nonassociative, diassociative Hamiltonian loop of order* $2^k$ *a subloop of some Cayley–Dickson loop?*

Note that due to Theorem 2.6.3 the requirement that the order of a loop is $2^k$ cannot be omitted.

# Bibliography

[1] G. Appa, D. Magos, I. Mourtos, and J. C. M. Janssen. On the orthogonal latin squares polytope. *Discrete Mathematics*, 306:171187, 2006.

[2] J. C. Baez. The octonions. *Bull. Amer. Math. Soc.*, 39:145–205, 2002.

[3] V. D. Belousov. *Foundations of the Theory of Quasigroups and Loops.* Nauka, 1967.

[4] R. H. Bruck. *A Survey of Binary Systems.* Springer-Verlag, 3rd edition, 1971.

[5] R. H. Bruck and L. J. Paige. Loops whose inner mappings are automorphisms. *Ann. of Math.*, 63(2):308–323, 1956.

[6] R. E. Cawagas. On the structure and zero divisors of the Cayley–Dickson sedenion algebra. *Discuss. Math. Gen. Algebra Appl.*, 24:251–265, 2004.

[7] R. E. Cawagas, A. S. Carrascal, L. A. Bautista, J. P. Sta. Maria, J. D. Urrutia, and B. Nobles. The subalgebra structure of the Cayley–Dickson algebra of dimension 32. arXiv:0907.2047v3.

[8] A. Cayley. On Jacobi's elliptic functions, in reply to the Rev. B. Bronwin; and on quaternions (appendix only). *The Collected Mathematical Papers, Johnson Reprint Co., New York*, page 127, 1963.

[9] J. H. Conway and D. A. Smith. *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry.* A K Peters, Ltd., 2003.

[10] C. Culbert. Cayley–Dickson algebras and loops. *J. Gen. Lie Theory Appl.*, 1(1):1–17, 2007.

[11] L. E. Dickson. On quaternions and their generalization and the history of the eight square theorem. *The Annals of Mathematics, Second Series*, 20, 1919.

[12] A. Drápal, M. Kinyon, and P. Vojtěchovský. *Loop Theory.* Manuscript in preparation.

[13] R. Euler, R. E. Burkard, and R. Grommes. On latin squares and the facial structure of related polytopes. *Discrete Mathematics*, 62:155–181, 1986.

[14] R. M. Falcón. 0/1-polytopes related to latin squares autotopisms. *Proceedings of VI Jornadas de Matemática Discreta y Algorítmica*, pages 311–319, 2008.

[15] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[16] I. N. Herstein. *Abstract Algebra*. Prentice-Hall, 3rd edition, 1995.

[17] A. Hurwitz. Ueber die Composition der quadratischen Formen von beliebig vielen Variabeln (in German). *Nachr. Ges. Wiss. Gottingen*, pages 309–316, 1898.

[18] P. Jedlička, M. Kinyon, and P. Vojtěchovský. The structure of commutative automorphic loops. *Trans. Amer. Math. Soc.*, 363:365–384, 2011.

[19] E. C. Johnsen and T. Storer. Combinatorial structures in loops. I. Elements of the decomposition theory. *J. Combin. Theory Ser. A*, 14:149–166, 1973.

[20] E. C. Johnsen and T. Storer. Combinatorial structures in loops. II. Commutative inverse property cyclic neofields of prime-power order. *Pacific J. Math.*, 52:115–127, 1974.

[21] E. C. Johnsen and T. Storer. Combinatorial structures in loops. III. Difference sets in special cyclic neofields. *J. Number Theory*, 8:109–130, 1976.

[22] M. Kinyon, K. Kunen, and J. D. Phillips. A generalization of Moufang and Steiner loops. *Algebra Universalis*, 48(1):81–101, 2002.

[23] M. Kinyon, K. Kunen, J. D. Phillips, and P. Vojtěchovský. The structure of automorphic loops. preprint.

[24] J. Kirshtein. Maximal subloops of Cayley–Dickson loops. In preparation.

[25] J. Kirshtein. Multiplication groups and inner mapping groups of Cayley–Dickson loops. Submitted.

[26] J. Kirshtein. Automorphism groups of Cayley–Dickson loops. *J. Gen. Lie Theory Appl.*, 6, 2012.

[27] M. Koca and R. Koç. Octonions and the group of order 1344. *Turk. J. Phys.*, 19:304–319, 1995.

[28] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8, 1988.

[29] S. V. Ludkovsky. Differentiable functions of Cayley–Dickson numbers and line integration. *J. of Mathem. Sciences*, 141, 2007.

[30] S. V. Ludkovsky. *Analysis over Cayley–Dickson numbers and its applications: Hypercomplex holomorphic functions, meromorphic functions, partial differential equations, operational calculus.* Lambert, 2010.

[31] R. Moufang. Zur Struktur von Alternativkörpern (in German). *Math. Ann.*, 110:416–430, 1935.

[32] G. P. Nagy and P. Vojtěchovský. *LOOPS, Package for GAP 4, http://www.math.du.edu/loops*, 2006.

[33] D. A. Norton. Hamiltonian loops. *Proc. Amer. Math. Soc.*, 3:56–65, 1952.

[34] H. O. Pflugfelder. *Quasigroups and Loops: Introduction.* Heldermann, 1990.

[35] H. O. Pflugfelder. Historical notes on loop theory. *Comment. Math. Univ. Carolin.*, 41, 2000.

[36] J. J. Rotman. *An Introduction to the Theory of Groups.* Springer-Verlag, 1994.

[37] J. J. Rotman. *Advanced Modern Algebra.* American Mathematical Society, 2nd edition, 2010.

[38] R. D. Schafer. On the algebras formed by the Cayley–Dickson process. *Amer. J. Math.*, 76:435–446, 1954.

[39] T. A. Springer and F. D. Veldkamp. *Octonions, Jordan Algebras and Exceptional Groups.* Springer-Verlag, 2000.

[40] J. Vince. *Quaternions for Computer Graphics.* Springer-Verlag, 2011.

[41] P. Vojtěchovský. Connections between codes, groups, and loops. Ph.D. Thesis, Charles University, 2003.

[42] P. Vojtěchovský. Toward the classification of Moufang loops of order 64. *European J. Combin.*, 27, 2006.

[43] H. J. Zassenhaus. *The Theory of Groups.* Dover, 2nd edition, 1999.

# Appendix A

# Multiplication Tables

Below we provide multiplication tables of the Cayley–Dickson loops $Q_n$, $n \le 5$, and for the quasioctonion and quasisedenion loops.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 |
| 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 |
| 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 |
| 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 |
| 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 |
| 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 |
| 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 |

Table A.1: Quaternion group multiplication table

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 |
| 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 |
| 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 |
| 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 |
| 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 |
| 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 |
| 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 |
| 9 | 10 | 12 | 11 | 14 | 13 | 16 | 15 | 2 | 1 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | 9 | 11 | 12 | 13 | 14 | 15 | 16 | 1 | 2 | 4 | 3 | 6 | 5 | 8 | 7 |
| 11 | 12 | 9 | 10 | 16 | 15 | 13 | 14 | 4 | 3 | 2 | 1 | 8 | 7 | 5 | 6 |
| 12 | 11 | 10 | 9 | 15 | 16 | 14 | 13 | 3 | 4 | 1 | 2 | 7 | 8 | 6 | 5 |
| 13 | 14 | 15 | 16 | 9 | 10 | 12 | 11 | 6 | 5 | 7 | 8 | 2 | 1 | 4 | 3 |
| 14 | 13 | 16 | 15 | 10 | 9 | 11 | 12 | 5 | 6 | 8 | 7 | 1 | 2 | 3 | 4 |
| 15 | 16 | 14 | 13 | 11 | 12 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 2 | 1 |
| 16 | 15 | 13 | 14 | 12 | 11 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 1 | 2 |

Table A.2: Octonion loop multiplication table

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 |
| 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 |
| 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 |
| 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 |
| 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 |
| 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 |
| 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 |
| 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 11 | 12 | 10 | 9 | 15 | 16 | 14 | 13 | 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 |
| 12 | 11 | 9 | 10 | 16 | 15 | 13 | 14 | 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 |
| 13 | 14 | 16 | 15 | 10 | 9 | 11 | 12 | 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 |
| 14 | 13 | 15 | 16 | 9 | 10 | 12 | 11 | 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 |
| 15 | 16 | 13 | 14 | 12 | 11 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 |
| 16 | 15 | 14 | 13 | 11 | 12 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 |

Table A.3: Quasioctonion loop multiplication table

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 |
| 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 | 19 | 20 | 18 | 17 | 24 | 23 | 21 | 22 | 28 | 27 | 25 | 26 | 31 | 32 | 30 | 29 |
| 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 | 20 | 19 | 17 | 18 | 23 | 24 | 22 | 21 | 27 | 28 | 26 | 25 | 32 | 31 | 29 | 30 |
| 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 | 21 | 22 | 23 | 24 | 18 | 17 | 20 | 19 | 30 | 29 | 32 | 31 | 25 | 26 | 27 | 28 |
| 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 | 22 | 21 | 24 | 23 | 17 | 18 | 19 | 20 | 29 | 30 | 31 | 32 | 26 | 25 | 28 | 27 |
| 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 | 23 | 24 | 22 | 21 | 19 | 20 | 18 | 17 | 32 | 31 | 29 | 30 | 28 | 27 | 25 | 26 |
| 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 | 24 | 23 | 21 | 22 | 20 | 19 | 17 | 18 | 31 | 32 | 30 | 29 | 27 | 28 | 26 | 25 |
| 9 | 10 | 12 | 11 | 14 | 13 | 16 | 15 | 2 | 1 | 3 | 4 | 5 | 6 | 7 | 8 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 |
| 10 | 9 | 11 | 12 | 13 | 14 | 15 | 16 | 1 | 2 | 4 | 3 | 6 | 5 | 8 | 7 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 11 | 12 | 9 | 10 | 16 | 15 | 13 | 14 | 4 | 3 | 2 | 1 | 8 | 7 | 5 | 6 | 27 | 28 | 26 | 25 | 31 | 32 | 30 | 29 | 19 | 20 | 18 | 17 | 23 | 24 | 22 | 21 |
| 12 | 11 | 10 | 9 | 15 | 16 | 14 | 13 | 3 | 4 | 1 | 2 | 7 | 8 | 6 | 5 | 28 | 27 | 25 | 26 | 32 | 31 | 29 | 30 | 20 | 19 | 17 | 18 | 24 | 23 | 21 | 22 |
| 13 | 14 | 15 | 16 | 9 | 10 | 12 | 11 | 6 | 5 | 7 | 8 | 2 | 1 | 4 | 3 | 29 | 30 | 32 | 31 | 26 | 25 | 27 | 28 | 21 | 22 | 24 | 23 | 18 | 17 | 19 | 20 |
| 14 | 13 | 16 | 15 | 10 | 9 | 11 | 12 | 5 | 6 | 8 | 7 | 1 | 2 | 3 | 4 | 30 | 29 | 31 | 32 | 25 | 26 | 28 | 27 | 22 | 21 | 23 | 24 | 17 | 18 | 20 | 19 |
| 15 | 16 | 14 | 13 | 11 | 12 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 2 | 1 | 31 | 32 | 29 | 30 | 28 | 27 | 26 | 25 | 23 | 24 | 21 | 22 | 20 | 19 | 18 | 17 |
| 16 | 15 | 13 | 14 | 12 | 11 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 1 | 2 | 32 | 31 | 30 | 29 | 27 | 28 | 25 | 26 | 24 | 23 | 22 | 21 | 19 | 20 | 17 | 18 |
| 17 | 18 | 20 | 19 | 22 | 21 | 24 | 23 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 2 | 1 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 18 | 17 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 1 | 2 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 |
| 19 | 20 | 17 | 18 | 24 | 23 | 21 | 22 | 28 | 27 | 25 | 26 | 31 | 32 | 30 | 29 | 4 | 3 | 2 | 1 | 8 | 7 | 5 | 6 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 |
| 20 | 19 | 18 | 17 | 23 | 24 | 22 | 21 | 27 | 28 | 26 | 25 | 32 | 31 | 29 | 30 | 3 | 4 | 1 | 2 | 7 | 8 | 6 | 5 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 |
| 21 | 22 | 23 | 24 | 17 | 18 | 20 | 19 | 30 | 29 | 32 | 31 | 25 | 26 | 27 | 28 | 6 | 5 | 7 | 8 | 2 | 1 | 4 | 3 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 |
| 22 | 21 | 24 | 23 | 18 | 17 | 19 | 20 | 29 | 30 | 31 | 32 | 26 | 25 | 28 | 27 | 5 | 6 | 8 | 7 | 1 | 2 | 3 | 4 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 |
| 23 | 24 | 22 | 21 | 19 | 20 | 17 | 18 | 32 | 31 | 29 | 30 | 28 | 27 | 25 | 26 | 8 | 7 | 6 | 5 | 3 | 4 | 2 | 1 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 |
| 24 | 23 | 21 | 22 | 20 | 19 | 18 | 17 | 31 | 32 | 30 | 29 | 27 | 28 | 26 | 25 | 7 | 8 | 5 | 6 | 4 | 3 | 1 | 2 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 17 | 18 | 20 | 19 | 22 | 21 | 24 | 23 | 10 | 9 | 11 | 12 | 13 | 14 | 15 | 16 | 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 |
| 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 18 | 17 | 19 | 20 | 21 | 22 | 23 | 24 | 9 | 10 | 12 | 11 | 14 | 13 | 16 | 15 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 27 | 28 | 26 | 25 | 31 | 32 | 30 | 29 | 19 | 20 | 17 | 18 | 23 | 24 | 22 | 21 | 12 | 11 | 10 | 9 | 15 | 16 | 14 | 13 | 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 |
| 28 | 27 | 25 | 26 | 32 | 31 | 29 | 30 | 20 | 19 | 18 | 17 | 24 | 23 | 21 | 22 | 11 | 12 | 9 | 10 | 16 | 15 | 13 | 14 | 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 |
| 29 | 30 | 32 | 31 | 26 | 25 | 27 | 28 | 21 | 22 | 24 | 23 | 17 | 18 | 19 | 20 | 14 | 13 | 16 | 15 | 10 | 9 | 11 | 12 | 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 |
| 30 | 29 | 31 | 32 | 25 | 26 | 28 | 27 | 22 | 21 | 23 | 24 | 18 | 17 | 20 | 19 | 13 | 14 | 15 | 16 | 9 | 10 | 12 | 11 | 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 |
| 31 | 32 | 29 | 30 | 28 | 27 | 26 | 25 | 23 | 24 | 21 | 22 | 20 | 19 | 17 | 18 | 16 | 15 | 13 | 14 | 12 | 11 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 |
| 32 | 31 | 30 | 29 | 27 | 28 | 25 | 26 | 24 | 23 | 22 | 21 | 19 | 20 | 18 | 17 | 15 | 16 | 14 | 13 | 11 | 12 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 |

Table A.4: Sedenion loop multiplication table

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 |
| 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 | 20 | 19 | 17 | 18 | 23 | 24 | 22 | 21 | 27 | 28 | 26 | 25 | 32 | 31 | 29 | 30 |
| 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 | 19 | 20 | 18 | 17 | 24 | 23 | 21 | 22 | 28 | 27 | 25 | 26 | 31 | 32 | 30 | 29 |
| 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 | 22 | 21 | 24 | 23 | 17 | 18 | 19 | 20 | 29 | 30 | 31 | 32 | 26 | 25 | 28 | 27 |
| 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 | 21 | 22 | 23 | 24 | 18 | 17 | 20 | 19 | 30 | 29 | 32 | 31 | 25 | 26 | 27 | 28 |
| 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 | 24 | 23 | 21 | 22 | 20 | 19 | 17 | 18 | 31 | 32 | 30 | 29 | 27 | 28 | 26 | 25 |
| 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 | 23 | 24 | 22 | 21 | 19 | 20 | 18 | 17 | 32 | 31 | 29 | 30 | 28 | 27 | 25 | 26 |
| 9 | 10 | 12 | 11 | 14 | 13 | 16 | 15 | 2 | 1 | 3 | 4 | 5 | 6 | 7 | 8 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 10 | 9 | 11 | 12 | 13 | 14 | 15 | 16 | 1 | 2 | 4 | 3 | 6 | 5 | 8 | 7 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 |
| 11 | 12 | 9 | 10 | 16 | 15 | 13 | 14 | 4 | 3 | 2 | 1 | 8 | 7 | 5 | 6 | 28 | 27 | 25 | 26 | 32 | 31 | 29 | 30 | 20 | 19 | 17 | 18 | 24 | 23 | 21 | 22 |
| 12 | 11 | 10 | 9 | 15 | 16 | 14 | 13 | 3 | 4 | 1 | 2 | 7 | 8 | 6 | 5 | 27 | 28 | 26 | 25 | 31 | 32 | 30 | 29 | 19 | 20 | 18 | 17 | 23 | 24 | 22 | 21 |
| 13 | 14 | 15 | 16 | 9 | 10 | 12 | 11 | 6 | 5 | 7 | 8 | 2 | 1 | 4 | 3 | 30 | 29 | 31 | 32 | 25 | 26 | 28 | 27 | 22 | 21 | 23 | 24 | 17 | 18 | 20 | 19 |
| 14 | 13 | 16 | 15 | 10 | 9 | 11 | 12 | 5 | 6 | 8 | 7 | 1 | 2 | 3 | 4 | 29 | 30 | 32 | 31 | 26 | 25 | 27 | 28 | 21 | 22 | 24 | 23 | 18 | 17 | 19 | 20 |
| 15 | 16 | 14 | 13 | 11 | 12 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 2 | 1 | 32 | 31 | 30 | 29 | 27 | 28 | 25 | 26 | 24 | 23 | 22 | 21 | 19 | 20 | 17 | 18 |
| 16 | 15 | 13 | 14 | 12 | 11 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 1 | 2 | 31 | 32 | 29 | 30 | 28 | 27 | 26 | 25 | 23 | 24 | 21 | 22 | 20 | 19 | 18 | 17 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 |
| 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 19 | 20 | 18 | 17 | 23 | 24 | 22 | 21 | 27 | 28 | 26 | 25 | 32 | 31 | 29 | 30 | 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 |
| 20 | 19 | 17 | 18 | 24 | 23 | 21 | 22 | 28 | 27 | 25 | 26 | 31 | 32 | 30 | 29 | 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 |
| 21 | 22 | 24 | 23 | 18 | 17 | 19 | 20 | 29 | 30 | 31 | 32 | 26 | 25 | 28 | 27 | 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 |
| 22 | 21 | 23 | 24 | 17 | 18 | 20 | 19 | 30 | 29 | 32 | 31 | 25 | 26 | 27 | 28 | 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 |
| 23 | 24 | 21 | 22 | 20 | 19 | 18 | 17 | 31 | 32 | 30 | 29 | 27 | 28 | 26 | 25 | 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 |
| 24 | 23 | 22 | 21 | 19 | 20 | 17 | 18 | 32 | 31 | 29 | 30 | 28 | 27 | 25 | 26 | 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 |
| 25 | 26 | 28 | 27 | 30 | 29 | 32 | 31 | 18 | 17 | 19 | 20 | 21 | 22 | 23 | 24 | 9 | 10 | 12 | 11 | 14 | 13 | 16 | 15 | 2 | 1 | 3 | 4 | 5 | 6 | 7 | 8 |
| 26 | 25 | 27 | 28 | 29 | 30 | 31 | 32 | 17 | 18 | 20 | 19 | 22 | 21 | 24 | 23 | 10 | 9 | 11 | 12 | 13 | 14 | 15 | 16 | 1 | 2 | 4 | 3 | 6 | 5 | 8 | 7 |
| 27 | 28 | 25 | 26 | 32 | 31 | 29 | 30 | 20 | 19 | 18 | 17 | 24 | 23 | 21 | 22 | 11 | 12 | 9 | 10 | 16 | 15 | 13 | 14 | 4 | 3 | 2 | 1 | 8 | 7 | 5 | 6 |
| 28 | 27 | 26 | 25 | 31 | 32 | 30 | 29 | 19 | 20 | 17 | 18 | 23 | 24 | 22 | 21 | 12 | 11 | 10 | 9 | 15 | 16 | 14 | 13 | 3 | 4 | 1 | 2 | 7 | 8 | 6 | 5 |
| 29 | 30 | 31 | 32 | 25 | 26 | 28 | 27 | 22 | 21 | 23 | 24 | 18 | 17 | 20 | 19 | 13 | 14 | 15 | 16 | 9 | 10 | 12 | 11 | 6 | 5 | 7 | 8 | 2 | 1 | 4 | 3 |
| 30 | 29 | 32 | 31 | 26 | 25 | 27 | 28 | 21 | 22 | 24 | 23 | 17 | 18 | 19 | 20 | 14 | 13 | 16 | 15 | 10 | 9 | 11 | 12 | 5 | 6 | 8 | 7 | 1 | 2 | 3 | 4 |
| 31 | 32 | 30 | 29 | 27 | 28 | 25 | 26 | 24 | 23 | 22 | 21 | 19 | 20 | 18 | 17 | 15 | 16 | 14 | 13 | 11 | 12 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 2 | 1 |
| 32 | 31 | 29 | 30 | 28 | 27 | 26 | 25 | 23 | 24 | 21 | 22 | 20 | 19 | 17 | 18 | 16 | 15 | 13 | 14 | 12 | 11 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 1 | 2 |

Table A.5: Quasisedenion loop $\tilde{\mathbb{S}}_{32}^{1}$ multiplication table

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 |
| 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 | 20 | 19 | 17 | 18 | 23 | 24 | 22 | 21 | 27 | 28 | 26 | 25 | 32 | 31 | 29 | 30 |
| 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 | 19 | 20 | 18 | 17 | 24 | 23 | 21 | 22 | 28 | 27 | 25 | 26 | 31 | 32 | 30 | 29 |
| 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 | 22 | 21 | 24 | 23 | 17 | 18 | 19 | 20 | 29 | 30 | 31 | 32 | 26 | 25 | 28 | 27 |
| 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 | 21 | 22 | 23 | 24 | 18 | 17 | 20 | 19 | 30 | 29 | 32 | 31 | 25 | 26 | 27 | 28 |
| 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 | 24 | 23 | 21 | 22 | 20 | 19 | 17 | 18 | 31 | 32 | 30 | 29 | 27 | 28 | 26 | 25 |
| 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 | 23 | 24 | 22 | 21 | 19 | 20 | 18 | 17 | 32 | 31 | 29 | 30 | 28 | 27 | 25 | 26 |
| 9 | 10 | 12 | 11 | 14 | 13 | 16 | 15 | 2 | 1 | 3 | 4 | 5 | 6 | 7 | 8 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 |
| 10 | 9 | 11 | 12 | 13 | 14 | 15 | 16 | 1 | 2 | 4 | 3 | 6 | 5 | 8 | 7 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 11 | 12 | 9 | 10 | 16 | 15 | 13 | 14 | 4 | 3 | 2 | 1 | 8 | 7 | 5 | 6 | 27 | 28 | 26 | 25 | 32 | 31 | 29 | 30 | 19 | 20 | 18 | 17 | 24 | 23 | 21 | 22 |
| 12 | 11 | 10 | 9 | 15 | 16 | 14 | 13 | 3 | 4 | 1 | 2 | 7 | 8 | 6 | 5 | 28 | 27 | 25 | 26 | 31 | 32 | 30 | 29 | 20 | 19 | 17 | 18 | 23 | 24 | 22 | 21 |
| 13 | 14 | 15 | 16 | 9 | 10 | 12 | 11 | 6 | 5 | 7 | 8 | 2 | 1 | 4 | 3 | 29 | 30 | 31 | 32 | 26 | 25 | 28 | 27 | 21 | 22 | 23 | 24 | 18 | 17 | 20 | 19 |
| 14 | 13 | 16 | 15 | 10 | 9 | 11 | 12 | 5 | 6 | 8 | 7 | 1 | 2 | 3 | 4 | 30 | 29 | 32 | 31 | 25 | 26 | 27 | 28 | 22 | 21 | 24 | 23 | 17 | 18 | 19 | 20 |
| 15 | 16 | 14 | 13 | 11 | 12 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 2 | 1 | 31 | 32 | 30 | 29 | 27 | 28 | 26 | 25 | 23 | 24 | 22 | 21 | 19 | 20 | 18 | 17 |
| 16 | 15 | 13 | 14 | 12 | 11 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 1 | 2 | 32 | 31 | 29 | 30 | 28 | 27 | 25 | 26 | 24 | 23 | 21 | 22 | 20 | 19 | 17 | 18 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 |
| 19 | 20 | 18 | 17 | 23 | 24 | 22 | 21 | 28 | 27 | 25 | 26 | 32 | 31 | 29 | 30 | 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 12 | 11 | 9 | 10 | 16 | 15 | 13 | 14 |
| 20 | 19 | 17 | 18 | 24 | 23 | 21 | 22 | 27 | 28 | 26 | 25 | 31 | 32 | 30 | 29 | 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 11 | 12 | 10 | 9 | 15 | 16 | 14 | 13 |
| 21 | 22 | 24 | 23 | 18 | 17 | 19 | 20 | 30 | 29 | 31 | 32 | 25 | 26 | 28 | 27 | 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 14 | 13 | 15 | 16 | 9 | 10 | 12 | 11 |
| 22 | 21 | 23 | 24 | 17 | 18 | 20 | 19 | 29 | 30 | 32 | 31 | 26 | 25 | 27 | 28 | 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 13 | 14 | 16 | 15 | 10 | 9 | 11 | 12 |
| 23 | 24 | 21 | 22 | 20 | 19 | 18 | 17 | 32 | 31 | 30 | 29 | 27 | 28 | 25 | 26 | 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 16 | 15 | 14 | 13 | 11 | 12 | 9 | 10 |
| 24 | 23 | 22 | 21 | 19 | 20 | 17 | 18 | 31 | 32 | 29 | 30 | 28 | 27 | 26 | 25 | 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 15 | 16 | 13 | 14 | 12 | 11 | 10 | 9 |
| 25 | 26 | 28 | 27 | 30 | 29 | 32 | 31 | 17 | 18 | 20 | 19 | 22 | 21 | 24 | 23 | 10 | 9 | 11 | 12 | 13 | 14 | 15 | 16 | 2 | 1 | 3 | 4 | 5 | 6 | 7 | 8 |
| 26 | 25 | 27 | 28 | 29 | 30 | 31 | 32 | 18 | 17 | 19 | 20 | 21 | 22 | 23 | 24 | 9 | 10 | 12 | 11 | 14 | 13 | 16 | 15 | 1 | 2 | 4 | 3 | 6 | 5 | 8 | 7 |
| 27 | 28 | 25 | 26 | 32 | 31 | 29 | 30 | 19 | 20 | 17 | 18 | 24 | 23 | 21 | 22 | 12 | 11 | 10 | 9 | 16 | 15 | 13 | 14 | 4 | 3 | 2 | 1 | 8 | 7 | 5 | 6 |
| 28 | 27 | 26 | 25 | 31 | 32 | 30 | 29 | 20 | 19 | 18 | 17 | 23 | 24 | 22 | 21 | 11 | 12 | 9 | 10 | 15 | 16 | 14 | 13 | 3 | 4 | 1 | 2 | 7 | 8 | 6 | 5 |
| 29 | 30 | 31 | 32 | 25 | 26 | 28 | 27 | 21 | 22 | 23 | 24 | 17 | 18 | 20 | 19 | 14 | 13 | 15 | 16 | 10 | 9 | 12 | 11 | 6 | 5 | 7 | 8 | 2 | 1 | 4 | 3 |
| 30 | 29 | 32 | 31 | 26 | 25 | 27 | 28 | 22 | 21 | 24 | 23 | 18 | 17 | 19 | 20 | 13 | 14 | 16 | 15 | 9 | 10 | 11 | 12 | 5 | 6 | 8 | 7 | 1 | 2 | 3 | 4 |
| 31 | 32 | 30 | 29 | 27 | 28 | 25 | 26 | 23 | 24 | 22 | 21 | 19 | 20 | 17 | 18 | 16 | 15 | 14 | 13 | 11 | 12 | 10 | 9 | 8 | 7 | 6 | 5 | 3 | 4 | 2 | 1 |
| 32 | 31 | 29 | 30 | 28 | 27 | 26 | 25 | 24 | 23 | 21 | 22 | 20 | 19 | 18 | 17 | 15 | 16 | 13 | 14 | 12 | 11 | 9 | 10 | 7 | 8 | 5 | 6 | 4 | 3 | 1 | 2 |

Table A.6: Quasisedenion loop $\tilde{\mathbb{S}}_{32}^{2}$ multiplication table

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 |
| 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 | 20 | 19 | 17 | 18 | 23 | 24 | 22 | 21 | 28 | 27 | 25 | 26 | 31 | 32 | 30 | 29 |
| 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 | 19 | 20 | 18 | 17 | 24 | 23 | 21 | 22 | 27 | 28 | 26 | 25 | 32 | 31 | 29 | 30 |
| 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 | 22 | 21 | 24 | 23 | 17 | 18 | 19 | 20 | 30 | 29 | 32 | 31 | 25 | 26 | 27 | 28 |
| 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 | 21 | 22 | 23 | 24 | 18 | 17 | 20 | 19 | 29 | 30 | 31 | 32 | 26 | 25 | 28 | 27 |
| 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 | 24 | 23 | 21 | 22 | 20 | 19 | 17 | 18 | 32 | 31 | 29 | 30 | 28 | 27 | 25 | 26 |
| 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 | 23 | 24 | 22 | 21 | 19 | 20 | 18 | 17 | 31 | 32 | 30 | 29 | 27 | 28 | 26 | 25 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 26 | 25 | 27 | 28 | 29 | 30 | 31 | 32 | 17 | 18 | 20 | 19 | 22 | 21 | 24 | 23 |
| 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 25 | 26 | 28 | 27 | 30 | 29 | 32 | 31 | 18 | 17 | 19 | 20 | 21 | 22 | 23 | 24 |
| 11 | 12 | 10 | 9 | 15 | 16 | 14 | 13 | 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 28 | 27 | 26 | 25 | 32 | 31 | 29 | 30 | 19 | 20 | 17 | 18 | 24 | 23 | 21 | 22 |
| 12 | 11 | 9 | 10 | 16 | 15 | 13 | 14 | 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 27 | 28 | 25 | 26 | 31 | 32 | 30 | 29 | 20 | 19 | 18 | 17 | 23 | 24 | 22 | 21 |
| 13 | 14 | 16 | 15 | 10 | 9 | 11 | 12 | 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 30 | 29 | 31 | 32 | 26 | 25 | 28 | 27 | 21 | 22 | 23 | 24 | 17 | 18 | 20 | 19 |
| 14 | 13 | 15 | 16 | 9 | 10 | 12 | 11 | 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 29 | 30 | 32 | 31 | 25 | 26 | 27 | 28 | 22 | 21 | 24 | 23 | 18 | 17 | 19 | 20 |
| 15 | 16 | 13 | 14 | 12 | 11 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 32 | 31 | 30 | 29 | 27 | 28 | 26 | 25 | 23 | 24 | 22 | 21 | 19 | 20 | 17 | 18 |
| 16 | 15 | 14 | 13 | 11 | 12 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 31 | 32 | 29 | 30 | 28 | 27 | 25 | 26 | 24 | 23 | 21 | 22 | 20 | 19 | 18 | 17 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 |
| 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 | 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 19 | 20 | 18 | 17 | 23 | 24 | 22 | 21 | 28 | 27 | 25 | 26 | 32 | 31 | 29 | 30 | 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 | 12 | 11 | 9 | 10 | 16 | 15 | 13 | 14 |
| 20 | 19 | 17 | 18 | 24 | 23 | 21 | 22 | 27 | 28 | 26 | 25 | 31 | 32 | 30 | 29 | 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 | 11 | 12 | 10 | 9 | 15 | 16 | 14 | 13 |
| 21 | 22 | 24 | 23 | 18 | 17 | 19 | 20 | 30 | 29 | 31 | 32 | 25 | 26 | 28 | 27 | 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 | 14 | 13 | 15 | 16 | 9 | 10 | 12 | 11 |
| 22 | 21 | 23 | 24 | 17 | 18 | 20 | 19 | 29 | 30 | 32 | 31 | 26 | 25 | 27 | 28 | 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 | 13 | 14 | 16 | 15 | 10 | 9 | 11 | 12 |
| 23 | 24 | 21 | 22 | 20 | 19 | 18 | 17 | 32 | 31 | 30 | 29 | 27 | 28 | 25 | 26 | 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 | 16 | 15 | 14 | 13 | 11 | 12 | 9 | 10 |
| 24 | 23 | 22 | 21 | 19 | 20 | 17 | 18 | 31 | 32 | 29 | 30 | 28 | 27 | 26 | 25 | 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 | 15 | 16 | 13 | 14 | 12 | 11 | 10 | 9 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 18 | 17 | 20 | 19 | 22 | 21 | 24 | 23 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 2 | 1 | 4 | 3 | 6 | 5 | 8 | 7 |
| 26 | 25 | 28 | 27 | 30 | 29 | 32 | 31 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 10 | 9 | 12 | 11 | 14 | 13 | 16 | 15 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 27 | 28 | 26 | 25 | 31 | 32 | 30 | 29 | 19 | 20 | 18 | 17 | 24 | 23 | 21 | 22 | 11 | 12 | 10 | 9 | 16 | 15 | 13 | 14 | 3 | 4 | 2 | 1 | 7 | 8 | 6 | 5 |
| 28 | 27 | 25 | 26 | 32 | 31 | 29 | 30 | 20 | 19 | 17 | 18 | 23 | 24 | 22 | 21 | 12 | 11 | 9 | 10 | 15 | 16 | 14 | 13 | 4 | 3 | 1 | 2 | 8 | 7 | 5 | 6 |
| 29 | 30 | 32 | 31 | 26 | 25 | 27 | 28 | 21 | 22 | 23 | 24 | 18 | 17 | 20 | 19 | 13 | 14 | 15 | 16 | 10 | 9 | 12 | 11 | 5 | 6 | 8 | 7 | 2 | 1 | 3 | 4 |
| 30 | 29 | 31 | 32 | 25 | 26 | 28 | 27 | 22 | 21 | 24 | 23 | 17 | 18 | 19 | 20 | 14 | 13 | 16 | 15 | 9 | 10 | 11 | 12 | 6 | 5 | 7 | 8 | 1 | 2 | 4 | 3 |
| 31 | 32 | 29 | 30 | 28 | 27 | 26 | 25 | 23 | 24 | 22 | 21 | 19 | 20 | 18 | 17 | 15 | 16 | 14 | 13 | 11 | 12 | 10 | 9 | 7 | 8 | 5 | 6 | 4 | 3 | 2 | 1 |
| 32 | 31 | 30 | 29 | 27 | 28 | 25 | 26 | 24 | 23 | 21 | 22 | 20 | 19 | 17 | 18 | 16 | 15 | 13 | 14 | 12 | 11 | 9 | 10 | 8 | 7 | 6 | 5 | 3 | 4 | 1 | 2 |

Table A.7: Quasisedenion loop $\tilde{\mathbb{S}}^3_{32}$ multiplication table

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 2 | -1 | 4 | -3 | 6 | -5 | -8 | 7 | 10 | -9 | -12 | 11 | -14 | 13 | 16 | -15 | 18 | -17 | -20 | 19 | -22 | 21 | 24 | -23 | -26 | 25 | 28 | -27 | 30 | -29 | -32 | 31 |
| 3 | -4 | -1 | 2 | 7 | 8 | -5 | -6 | 11 | 12 | -9 | -10 | -15 | -16 | 13 | 14 | 19 | 20 | -17 | -18 | -23 | -24 | 21 | 22 | -27 | -28 | 25 | 26 | 31 | 32 | -29 | -30 |
| 4 | 3 | -2 | -1 | 8 | -7 | 6 | -5 | 12 | -11 | 10 | -9 | -16 | 15 | -14 | 13 | 20 | -19 | 18 | -17 | -24 | 23 | -22 | 21 | -28 | 27 | -26 | 25 | 32 | -31 | 30 | -29 |
| 5 | -6 | -7 | -8 | -1 | 2 | 3 | 4 | 13 | 14 | 15 | 16 | -9 | -10 | -11 | -12 | 21 | 22 | 23 | 24 | -17 | -18 | -19 | -20 | -29 | -30 | -31 | -32 | 25 | 26 | 27 | 28 |
| 6 | 5 | -8 | 7 | -2 | -1 | -4 | 3 | 14 | -13 | 16 | -15 | 10 | -9 | 12 | -11 | 22 | -21 | 24 | -23 | 18 | -17 | 20 | -19 | -30 | 29 | -32 | 31 | -26 | 25 | -28 | 27 |
| 7 | 8 | 5 | -6 | -3 | 4 | -1 | -2 | 15 | -16 | -13 | 14 | 11 | -12 | -9 | 10 | 23 | -24 | -21 | 22 | 19 | -20 | -17 | 18 | -31 | 32 | 29 | -30 | -27 | 28 | 25 | -26 |
| 8 | -7 | 6 | 5 | -4 | -3 | 2 | -1 | 16 | 15 | -14 | -13 | 12 | 11 | -10 | -9 | 24 | 23 | -22 | -21 | 20 | 19 | -18 | -17 | -32 | -31 | 30 | 29 | -28 | -27 | 26 | 25 |
| 9 | -10 | -11 | -12 | -13 | -14 | -15 | -16 | -1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | -17 | -18 | -19 | -20 | -21 | -22 | -23 | -24 |
| 10 | 9 | -12 | 11 | -14 | 13 | 16 | -15 | -2 | -1 | -4 | 3 | -6 | 5 | 8 | -7 | 26 | -25 | 28 | -27 | 30 | -29 | -32 | 31 | 18 | -17 | 20 | -19 | 22 | -21 | -24 | 23 |
| 11 | 12 | 9 | -10 | -15 | -16 | 13 | 14 | -3 | 4 | -1 | -2 | -7 | -8 | 5 | 6 | 27 | -28 | -25 | 26 | 31 | 32 | -29 | -30 | 19 | -20 | -17 | 18 | 23 | 24 | -21 | -22 |
| 12 | -11 | 10 | 9 | -16 | 15 | -14 | 13 | -4 | -3 | 2 | -1 | -8 | 7 | -6 | 5 | 28 | 27 | -26 | -25 | 32 | -31 | 30 | -29 | 20 | 19 | -18 | -17 | 24 | -23 | 22 | -21 |
| 13 | 14 | 15 | 16 | 9 | -10 | -11 | -12 | -5 | 6 | 7 | 8 | -1 | -2 | -3 | -4 | 29 | -30 | -31 | -32 | -25 | 26 | 27 | 28 | 21 | -22 | -23 | -24 | -17 | 18 | 19 | 20 |
| 14 | -13 | 16 | -15 | 10 | 9 | 12 | -11 | -6 | -5 | 8 | -7 | 2 | -1 | 4 | -3 | 30 | 29 | -32 | 31 | -26 | -25 | -28 | 27 | 22 | 21 | -24 | 23 | -18 | -17 | -20 | 19 |
| 15 | -16 | -13 | 14 | 11 | -12 | 9 | 10 | -7 | -8 | -5 | 6 | 3 | -4 | -1 | 2 | 31 | 32 | 29 | -30 | -27 | 28 | -25 | -26 | 23 | 24 | 21 | -22 | -19 | 20 | -17 | -18 |
| 16 | 15 | -14 | -13 | 12 | 11 | -10 | 9 | -8 | 7 | -6 | -5 | 4 | 3 | -2 | -1 | 32 | -31 | 30 | 29 | -28 | -27 | 26 | -25 | 24 | -23 | 22 | 21 | -20 | -19 | 18 | -17 |
| 17 | -18 | -19 | -20 | -21 | -22 | -23 | -24 | -25 | -26 | -27 | -28 | -29 | -30 | -31 | -32 | -1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 18 | 17 | -20 | 19 | -22 | 21 | 24 | -23 | -26 | 25 | 28 | -27 | 30 | -29 | -32 | 31 | -2 | -1 | -4 | 3 | -6 | 5 | 8 | -7 | -10 | 9 | 12 | -11 | 14 | -13 | -16 | 15 |
| 19 | 20 | 17 | -18 | -23 | -24 | 21 | 22 | -27 | -28 | 25 | 26 | 31 | 32 | -29 | -30 | -3 | 4 | -1 | -2 | -7 | -8 | 5 | 6 | -11 | -12 | 9 | 10 | 15 | 16 | -13 | -14 |
| 20 | -19 | 18 | 17 | -24 | 23 | -22 | 21 | -28 | 27 | -26 | 25 | 32 | -31 | 30 | -29 | -4 | -3 | 2 | -1 | -8 | 7 | -6 | 5 | -12 | 11 | -10 | 9 | 16 | -15 | 14 | -13 |
| 21 | 22 | 23 | 24 | 17 | -18 | -19 | -20 | -29 | -30 | -31 | -32 | 25 | 26 | 27 | 28 | -5 | 6 | 7 | 8 | -1 | -2 | -3 | -4 | -13 | -14 | -15 | -16 | 9 | 10 | 11 | 12 |
| 22 | -21 | 24 | -23 | 18 | 17 | 20 | -19 | -30 | 29 | -32 | 31 | -26 | 25 | -28 | 27 | -6 | -5 | 8 | -7 | 2 | -1 | 4 | -3 | -14 | 13 | -16 | 15 | -10 | 9 | -12 | 11 |
| 23 | -24 | -21 | 22 | 19 | -20 | 17 | 18 | -31 | 32 | 29 | -30 | -27 | 28 | 25 | -26 | -7 | -8 | -5 | 6 | 3 | -4 | -1 | 2 | -15 | 16 | 13 | -14 | -11 | 12 | 9 | -10 |
| 24 | 23 | -22 | -21 | 20 | 19 | -18 | 17 | -32 | -31 | 30 | 29 | -28 | -27 | 26 | 25 | -8 | 7 | -6 | -5 | 4 | 3 | -2 | -1 | -16 | -15 | 14 | 13 | -12 | -11 | 10 | 9 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 17 | -18 | -19 | -20 | -21 | -22 | -23 | -24 | -9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | -1 | -2 | -3 | -4 | -5 | -6 | -7 | -8 |
| 26 | -25 | 28 | -27 | 30 | -29 | -32 | 31 | 18 | 17 | 20 | -19 | 22 | -21 | -24 | 23 | -10 | -9 | 12 | -11 | 14 | -13 | -16 | 15 | 2 | -1 | 4 | -3 | 6 | -5 | -8 | 7 |
| 27 | -28 | -25 | 26 | 31 | 32 | -29 | -30 | 19 | -20 | 17 | 18 | 23 | 24 | -21 | -22 | -11 | -12 | -9 | 10 | 15 | 16 | -13 | -14 | 3 | -4 | -1 | 2 | 7 | 8 | -5 | -6 |
| 28 | 27 | -26 | -25 | 32 | -31 | 30 | -29 | 20 | 19 | -18 | 17 | 24 | -23 | 22 | -21 | -12 | 11 | -10 | -9 | 16 | -15 | 14 | -13 | 4 | 3 | -2 | -1 | 8 | -7 | 6 | -5 |
| 29 | -30 | -31 | -32 | -25 | 26 | 27 | 28 | 21 | -22 | -23 | -24 | 17 | 18 | 19 | 20 | -13 | -14 | -15 | -16 | -9 | 10 | 11 | 12 | 5 | -6 | -7 | -8 | -1 | 2 | 3 | 4 |
| 30 | 29 | -32 | 31 | -26 | -25 | -28 | 27 | 22 | 21 | -24 | 23 | -18 | 17 | -20 | 19 | -14 | 13 | -16 | 15 | -10 | -9 | -12 | 11 | 6 | 5 | -8 | 7 | -2 | -1 | -4 | 3 |
| 31 | 32 | 29 | -30 | -27 | 28 | -25 | -26 | 23 | 24 | 21 | -22 | -19 | 20 | 17 | -18 | -15 | 16 | 13 | -14 | -11 | 12 | -9 | -10 | 7 | 8 | 5 | -6 | -3 | 4 | -1 | -2 |
| 32 | -31 | 30 | 29 | -28 | -27 | 26 | -25 | 24 | -23 | 22 | 21 | -20 | -19 | 18 | 17 | -16 | -15 | 14 | 13 | -12 | -11 | 10 | -9 | 8 | -7 | 6 | 5 | -4 | -3 | 2 | -1 |

Table A.8: Multiplication table of positive elements of $\mathbb{T}_{64}$

# Appendix B

# GAP Programs

Function *CayleyDicksonLoop(n)* outputs a Cayley–Dickson loop of order $n$.

```
#================================================
# n=1 complex numbers
# n=2 quaternions
# n=3 octonions
# n=4 sedenions
# etc.
#================================================
# We represent the element i_k as a vector [sign,0,0,...,1,...0],
# where sign=0 if the element is positive, sign=1 if the element is negative;
# we put 1 on (k+1)-st position.
# Then we encode this element by
# code(sign,i_k)=2*k-1+sign;
# Note that code is even for negative elements and odd for positive ones;
# code(1)=1 and code(-1)=2.
#================================================
# For example, the units of complex numbers are encoded as follows:
# 1 -1 i -i
# [0,1,0] [1,1,0] [0,0,1] [1,0,1]
# 2*1-1+0         2*1-1+1 2*2-1+0 2*2-1+1
# 1 2 3 4
#================================================
# For example, element with code=8 corresponds to -i_(8/2) = -i_4,
# element with code=17 corresponds to i_((17+1)/2) = i_9
#================================================
CDMultiply := function ( a, b, MT )
# multiplies two elements of a Cayley-Dickson loop,
# receives a multiplication table as input parameter;
# accepts input in encoded format

local i, pos_a, pos_b;

if (IsMatrix(MT)=false) then return "bad input"; fi;
pos_a:=0;
```

```
pos_b:=0;
if a=0 or b=0 then return 0; fi;
for i in [1..Length(MT)] do
if MT[i][1] = a then pos_a:=i; fi;
if MT[1][i] = b then pos_b:=i; fi;
od;
if ((pos_a=0) or (pos_b=0)) then return "bad input"; fi;
return MT[pos_a][pos_b];
end;
#===============================================
CDConjugate := function ( a )
# finds a conjugate of an element;
# accepts input in the encoded format

if (a<0 or IsInt(a)=false ) then return "a should be a natural number"; fi;
if a<3 then return a; fi; # do nothing with real units and zero
#(zero is not a unit, it is needed for consistensy in the multiplication formula)
if (a mod 2)=0 then a:=a-1; else a:=a+1; fi;
# if the element is negative (even), we conjugate it by subtracting 1;
# if the element is positive (odd), we conjugate it by adding 1;
return a;
end;
#===============================================
CDMultiplicationTableCreate := function ( n, MT_prev )
# internal routine that creates multiplication table of elements
of a Cayley-Dickson loop of order n
# MT_prev is a multiplication table of a Cayley-Dickson loop of order (n-1)

local units, i, j, MT, neg, units_prev, code;

units:=[];
neg:=0;
units_prev:=MT_prev[1];
for j in units_prev do
Append(units,[[j,0]]);
od;
for j in units_prev do
Append(units,[[0,j]]);
  od;
code:=0;
MT:=NullMat(2^(n+1),2^(n+1));
for i in [1..2^(n+1)] do
MT[i][1]:=units[i];
MT[1][i]:=units[i];
od;
for i in [2..2^(n+1)] do
for j in [2..2^(n+1)] do
MT[i][j]:=[CDMultiply(MT[i][1][1],MT[1][j][1],MT_prev)
-CDMultiply(CDConjugate(MT[1][j][2]),MT[i][1][2],MT_prev),
CDMultiply(MT[1][j][2],MT[i][1][1],MT_prev)
+CDMultiply(MT[i][1][2],CDConjugate(MT[1][j][1]),MT_prev)];
od;
od;
for i in [1..2^(n+1)] do
```

```
for j in [1..2^(n+1)] do
if MT[i][j][1]<0 then
neg:=1;
MT[i][j][1]:=AbsInt(MT[i][j][1]);
else neg:=0;
fi;
if MT[i][j][1]<>0
then code:=MT[i][j][1];
else code:=MT[i][j][2]+2^(n);
fi;
if neg=1 then
if (code mod 2)=0 then code:=code-1; else code:=code+1; fi;
fi;
MT[i][j]:=code;
od;
od;
return MT;
end;
#================================================
CayleyDicksonLoop:= function ( n )
# returns a Cayley-Dickson loop of order n

local i, CDMultiplicationTableList, RealMT;

if ((IsInt(n)=false) or (n<1)) then return "n should be a natural number"; fi;
CDMultiplicationTableList:=NullMat(1,n);
RealMT:=[[1,2],[2,1]];  # multiplication table of reals
CDMultiplicationTableList[1]:=CDMultiplicationTableCreate(1,RealMT );
if (n>1) then
for i in [2..n] do
CDMultiplicationTableList[i]:=
CDMultiplicationTableCreate(i,CDMultiplicationTableList[i-1]);
od;
fi;
return LoopByCayleyTable(CDMultiplicationTableList[n]);
end;
#================================================
```

Modified function *Discriminator(L)* calculates the associating triples invariant for a loop $L$ in addition to the invariants computed in the original function of the LOOPS package for GAP.

```
#================================================
#  Discriminator( L )
#
#  Returns the dicriminator of a loop <L>.
#  Discriminator must be cheap to calculate, yet it is supposed to
#  provide such invariants that result in a fine partition of <L>
#  preserved under isomorphisms.

InstallMethod( Discriminator, "for loop",
    [ IsLoop ],
function( L )
    local n, T, I, i, j, k, ebo, c, J, counter, A, P, B, FrequencySet;
```

```
    # making sure loop table is canonical
    if L = Parent( L ) then T := CayleyTable( L );
    else T := CanonicalCayleyTable( CayleyTable( L ) ); fi;
    n := Size( L );
    # Calculating invariants.
    if not IsPowerAssociative( L ) then
        ...
    else
        #power associative loop, hence refined discriminator
        # Element x asks: What is my order?
        I := List( L, x -> [Order(x), 0, 0, 0, 0, false, 0] );
        # Element x asks: How many times am I a square, third power, fourth power?
        for i in [1..n] do
            j := T[ i ][ i ];
            I[ j ][ 2 ] := I[ j ][ 2 ] + 1;
            j := T[ i ][ j ];
            I[ j ][ 3 ] := I[ j ][ 3 ] + 1;
            j := T[ i ][ j ];
            I[ j ][ 4 ] := I[ j ][ 4 ] + 1;
        od;
        # Element x asks: With how many elements of given order do I commute?
        ebo := List( [1..n], i -> []); # elements by order
        for i in [1..n] do Add( ebo[ I[ i ][ 1 ] ], i ); od;
        ebo := Filtered( ebo, i -> not IsEmpty( i ) );
        for i in [1..n] do
            c := [];
            for J in ebo do
                counter := 0;
                for j in J do if T[ i ][ j ] = T[ j ][ i ] then
                    counter := counter + 1;
                fi; od;
                Add( c, counter );
            od;
            I[i][5] := c;
        od;
        # Element x asks: Am I central?
        for i in [1..n] do
            I[ i ][ 6 ] := Elements( L )[ i ] in Center( L );
        od;
# Not in the LOOPS package
# Element x asks: with how many elements do I associate
# in the first position (x*(y*z) = (x*y)*z ?)
for i in [1..n] do
for j in [1..n] do for k in [1..n] do
if T[ i ][ T[ j ][ k ] ] = T[ T[ i ][ j ] ][ k ] then
I[ i ][ 7 ] := I[ i ][ 7 ] + 1;
fi;
od; od;
od;
# end of Not in the LOOPS package
    fi; # All invariants have been calculated at this point.

    FrequencySet := function (L)
```

```
    # Auxiliary function.
    # Given a list L, returns [ S, F ], where S = Set( L ),
    # and where F[ i ] is the number of occurences of Elements( S )[ i ] in L
        local S, F, x, i;
        S := Set( L );
        F := 0*[ 1..Size( S ) ];
        for x in L do
            i := Position( S, x );
            F[ i ] := F[ i ] + 1;
        od;
        return [S, F];
    end;

    # Setting up the first part of discriminator (invariants).
    A := FrequencySet( I );
    P := Sortex( A[ 2 ] ); #small invariant sets will be listed first
    A[ 1 ] := Permuted( A[ 1 ], P );

    # Setting up the second part of discriminator
    # (blocks of elements invariant under isomorphisms).
    B := List( A[ 1 ], i -> [] ); #for every invariant get a list of elements
    for i in [1..n] do
        Add( B[ Position( A[ 1 ], I[ i ] ) ],  Elements( L )[ i ] );
    od;

    # Returning the discriminator.
    return [ A, B ];
end);
#================================================
```