An Introduction to Quasigroups and Their Representations

Studies in Advanced Mathematics

Titles Included in the Series

John P. D'Angelo, Several Complex Variables and the Geometry of Real Hypersurfaces

Steven R. Bell, The Cauchy Transform, Potential Theory, and Conformal Mapping

John J. Benedetto, Harmonic Analysis and Applications

John J. Benedetto and Michael W. Frazier, Wavelets: Mathematics and Applications

Albert Boggess, CR Manifolds and the Tangential Cauchy–Riemann Complex

Keith Burns and Marian Gidea, Differential Geometry and Topology: With a View to Dynamical Systems

George Cain and Gunter H. Meyer, Separation of Variables for Partial Differential Equations: An Eigenfunction Approach

Goong Chen and Jianxin Zhou, Vibration and Damping in Distributed Systems
Vol. 1: Analysis, Estimation, Attenuation, and Design
Vol. 2: WKB and Wave Methods, Visualization, and Experimentation

Carl C. Cowen and Barbara D. MacCluer, Composition Operators on Spaces of Analytic Functions

Jewgeni H. Dshalalow, Real Analysis: An Introduction to the Theory of Real Functions and Integration

Dean G. Duffy, Advanced Engineering Mathematics with MATLAB®, 2nd Edition

Dean G. Duffy, Green's Functions with Applications

Lawrence C. Evans and Ronald F. Gariepy, Measure Theory and Fine Properties of Functions

Gerald B. Folland, A Course in Abstract Harmonic Analysis

José García-Cuerva, Eugenio Hernández, Fernando Soria, and José-Luis Torrea, Fourier Analysis and Partial Differential Equations

Peter B. Gilkey, Invariance Theory, the Heat Equation, and the Atiyah-Singer Index Theorem, 2nd Edition

Peter B. Gilkey, John V. Leahy, and Jeonghueong Park, Spectral Geometry, Riemannian Submersions, and the Gromov-Lawson Conjecture

Alfred Gray, Elsa Abbena, and Simon Salamon Modern Differential Geometry of Curves and Surfaces with Mathematica, Third Edition

Eugenio Hernández and Guido Weiss, A First Course on Wavelets

Kenneth B. Howell, Principles of Fourier Analysis

Steven G. Krantz, The Elements of Advanced Mathematics, Second Edition

Steven G. Krantz, Partial Differential Equations and Complex Analysis

Steven G. Krantz, Real Analysis and Foundations, Second Edition

Kenneth L. Kuttler, Modern Analysis

Michael Pedersen, Functional Analysis in Applied Mathematics and Engineering

Clark Robinson, Dynamical Systems: Stability, Symbolic Dynamics, and Chaos, 2nd Edition

John Ryan, Clifford Algebras in Analysis and Related Topics

John Scherk, Algebra: A Computational Introduction

Jonathan D. H. Smith, An Introductin to Quasigroups and Their Representations

Pavel Šolín, Karel Segeth, and Ivo Doležel, High-Order Finite Element Method

André Unterberger and Harald Upmeier, Pseudodifferential Analysis on Symmetric Cones

James S. Walker, Fast Fourier Transforms, 2nd Edition

James S. Walker, A Primer on Wavelets and Their Scientific Applications

Gilbert G. Walter and Xiaoping Shen, Wavelets and Other Orthogonal Systems, Second Edition

Nik Weaver, Mathematical Quantization

Kehe Zhu, An Introduction to Operator Algebras

An Introduction to Quasigroups and Their Representations

Jonathan D. H. Smith

Chapman & Hall/CRC
Taylor & Francis Group
Boca Raton London New York

Chapman & Hall/CRC is an imprint of the
Taylor & Francis Group, an informa business

Chapman & Hall/CRC
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 1-58488-537-8 (Hardcover)
International Standard Book Number-13: 978-1-58488-537-5 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Smith, Jonathan D. H. 1949-
An introduction to quasigroups and their representations / Jonathan D.H. Smith.
p. cm. -- (Studies in advance mathematics)
Includes bibliographical references and index.
ISBN 1-58488-537-8 (alk. paper)
1. Quasigroups. 2. Nonassociative algebras. 3. Representations of groups. I. Title.

QA181.5.S65 2006
512'.22--dc22 2006049290

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Preface

The theory of quasigroups ("nonassociative groups") is one of the oldest branches of algebra and combinatorics. In the guise of Latin squares, it dates back at least to Euler [54]. Nevertheless, throughout the twentieth century it was overshadowed by its subset, the theory of groups, to such an extent that *Mathematical Reviews* classified loops and quasigroups merely as "other generalizations of groups." Apart from the fashions of the day, the main reason for the predominance of group theory was the fact that abstract groups admit representations, either linearly by matrices and modules, or as symmetries in the form of permutation representations. The aim of the present book is to show how these representations for groups are fully capable of extension to general quasigroups, and to illustrate the added depth and richness that result from such an extension.

The linear theory for quasigroups separates two topics, character theory and module theory, that are usually conflated in the group case. Permutation representations take on two striking new aspects when extended to quasigroups. The first is probabilistic: permutation matrices of groups are replaced by Markov matrices for quasigroups. The second is the fact that quasigroup actions are naturally described as coalgebras rather than as algebras.

The book divides into three parts:

- The first three chapters cover elements of the theory of quasigroups and loops, including certain key examples and construction techniques, that are needed for a full appreciation of the representation theory.
- The bulk of the book is devoted to the three main branches of the representation theory itself: permutation representations, characters, and modules.
- Finally, three brief appendices summarize some essential topics from category theory, universal algebra, and coalgebras.

Chapter 1 provides a quick elementary introduction to quasigroups and loops, as well as some of the most important special classes such as semisymmetric quasigroups, Steiner triple systems, and Moufang loops. Chapter 2 discusses the group actions on the underlying set of a quasigroup that result from the quasigroup structure. These actions are the key tools of quasigroup theory. In particular, the action of the combinatorial multiplication group on a quasigroup yields the combinatorial characters, while the universal stabilizers discussed in Section 2.8 form the basis for much of quasigroup module theory.

Chapter 3 looks at the quasigroup analogues of abelian groups, namely central quasigroups and piques. It also touches briefly on a converse interpretation of "quasigroup representation theory," namely the representation of groups as multiplication groups of quasigroups.

Chapters 4 and 5 are devoted to the theory of permutation representations of quasigroups. With permutation representations of groups being regarded as the embodiment of symmetry, one may view permutation representations of quasigroups as the expression of a newer and more general kind of symmetry, probabilistic in nature, that may include certain forms of approximate symmetry. Chapter 4 describes this symmetry, and the quasigroup homogeneous spaces that underlie it. Homogeneous space concepts are also used to study issues related to the breakdown of Lagrange's Theorem in quasigroups. The slightly more advanced Chapter 5 provides the general definition of a quasigroup permutation action, as a sum of images of homogeneous spaces or as an element of a certain covariety of coalgebras. The isomorphism classes of the permutation representations of a quasigroup form a Burnside algebra, just as for groups, and a general form of Burnside's Lemma, linearly algebraic in nature, counts the number of orbits.

Chapters 6 through 9 treat the oldest branch of quasigroup representation theory, the combinatorial character theory. This theory extends the ordinary character theory of finite groups. In fact, selected material from the first two of these chapters might even be used as a quick introduction to that theory in a more general setting. In Chapter 6, the combinatorial characters of a finite quasigroup are obtained from the action of the combinatorial multiplication group on the quasigroup. The complex incidence matrices of the orbitals in this transitive action span a commutative algebra, and the characters emerge as normalized coefficients expressing the orthogonal idempotents of the algebra as linear combinations of the incidence matrices.

Chapter 7 develops those parts of quasigroup character theory that form natural generalizations of group character theory: induced characters, fusion, lifting characters from quotients, and the determination of the structure of a quasigroup from its character table. By contrast, the topics of Chapter 8 do not have direct counterparts in group character theory. The motivating question is the extent to which a combinatorial multiplication group action on a quasigroup may be recovered from character-theoretical data.

Chapter 9, on permutation characters, serves a twofold purpose. On the one hand, it uses properties of the permutation action of the multiplication group of a quasigroup to describe some of the algebra structure associated with a homogeneous space for that quasigroup. On the other hand, it also introduces the characters of a quasigroup that are associated with permutation actions of the quasigroup. These give a direct generalization of the permutation characters of a group.

The final chapters study quasigroup module theory. Since the composition of matrices or module endomorphisms is associative, module representations of quasigroups require a more sophisticated definition than for groups, using

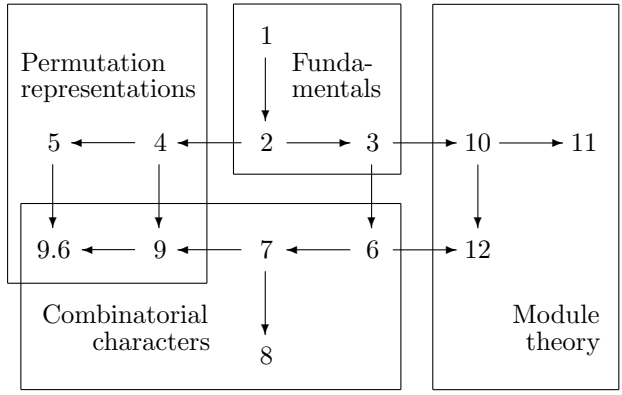
an algebraic analogue of the topological concept of a fiber bundle or the physical concept of a gauge theory (Sections 10.2 and 10.5). The fundamental theorems of Chapter 10 then show that categories of modules over a quasigroup are equivalent to categories of modules over certain rings, quotients of group algebras of universal stabilizers. In particular, there is a differential calculus for quasigroup words (Section 10.4).

Various applications of quasigroup module theory are given in Chapter 11. The topics discussed include the indexing of nonassociative powers (by their derivatives), the exponent of a quasigroup, Burnside's problem for quasigroups, construction of free commutative Moufang loops, and a quick synopsis of cohomology and extension theory for quasigroups.

Chapter 12 introduces analytical characters of a finite quasigroup, as certain almost-periodic functions. Although the finite-dimensional complex representations of a finite group are determined up to equivalence by its ordinary characters, the corresponding combinatorial characters of a finite quasigroup, as treated in Chapters 6 through 9, are inadequate for the task of classifying all the finite-dimensional modules over the complex numbers. This classification is achieved by the analytical characters.

Appendix A covers the main constructions of category theory used at various points throughout the text. Appendix B provides a quick introduction to universal algebraic concepts such as congruences, free algebras, and identities. Although these two appendices might conceivably serve as synopses for minicourses in their respective topics, readers are referred to [165] for more detail on categories and general algebraic methods. Appendix C summarizes the basic facts about coalgebras that are needed for the treatment of permutation representations in Chapter 5.

The structure of the book is summarized in the following chart.



Arrows show the approximate dependencies between the chapters or sections. In case of doubt, the index may be helpful in locating keywords or symbols.

Much of the work on this book was completed while I was on a Faculty Professional Development Assignment from Iowa State University during the academic year 2005–2006. The four-month period from October 2005 to February 2006 which I spent as a guest of the Faculty of Mathematics and Information Sciences at Warsaw University of Technology proved particularly fruitful. Many thanks are also due to Bob Stern and the staff of Taylor & Francis.

Contents

Chapter 1

QUASIGROUPS AND LOOPS

Quasigroups may be defined combinatorially or equationally. A (*combinatorial*) *quasigroup* $(Q, \cdot)$ is a set Q equipped with a binary *multiplication* operation

$$Q \times Q \to Q; (x, y) \mapsto xy \tag{1.1}$$

denoted by $\cdot$ or simple juxtaposition of the two arguments, in which specification of any two of x, y, z in the equation $x \cdot y = z$ determines the third uniquely. Note that group multiplications have this property, so that any group is a quasigroup. In particular, a quasigroup is said to be *abelian* if its multiplication is commutative and associative. However, quasigroup multiplications are not required to be associative. It is in this sense that quasigroups are considered to be "nonassociative groups."

Finite quasigroups are characterized in Section 1.1 as having bordered Latin squares for their multiplication tables. The more general and precise equational definition of Section 1.2 describes quasigroups as universal algebras with operations of multiplication, left and right division. Along with homomorphisms, quasigroups may also be related by homotopies. New quasigroups, known as conjugates, are obtained by regarding the divisions as basic multiplications (Section 1.3). For example, the nonassociative operation of subtraction yields a conjugate of an abelian group. The conjugates of a given quasigroup fit together to form its semisymmetrization, so that homotopies between quasigroups correspond to homomorphisms between their semisymmetrizations (Section 1.4). The type of a quasigroup may often be augmented by an idempotent element to give a so-called "pique" or pointed idempotent quasigroup (Section 1.5). If this idempotent element acts as an identity for the multiplication, then the pique becomes a loop.

Steiner triple systems are presented in Section 1.6 as an important equationally defined class of quasigroups. Section 1.7 provides a quick introduction to Moufang loops, more especially those obtained from Zorn's vector matrices and octonions. (One of the classical motivations for studying quasigroups and loops is the need for a deeper understanding of the octonions, as the last step in the sequence of algebras that starts with the reals and leads through the complex numbers and quaternions.) Section 1.8 examines the symmetry that holds between the various conjugates of a quasigroup. This symmetry is then applied to the proof of the normal form theorem for quasigroup words in the final Section 1.9.

1.1 Latin squares

A *Latin square*, such as that displayed in Figure 1.1, is an $n \times n$ square containing n copies of each of n symbols, arranged in such a way that no symbol is repeated in any row or column.

1	3	2	5	6	4
3	2	1	6	4	5
2	1	3	4	5	6
4	5	6	1	2	3
5	6	4	2	3	1
6	4	5	3	1	2

FIGURE 1.1: A Latin square.

Each Latin square may be bordered to yield the multiplication table of a quasigroup. For example, labeling the rows and columns of the Latin square of Figure 1.1 by $1, \ldots, 6$ in order, one obtains the multiplication table of a quasigroup Q with $3 \cdot 2 = 1$, etc., as displayed in Figure 1.2 below.

Q	1	2	3	4	5	6
1	1	3	2	5	6	4
2	3	2	1	6	4	5
3	2	1	3	4	5	6
4	4	5	6	1	2	3
5	5	6	4	2	3	1
6	6	4	5	3	1	2

FIGURE 1.2: A Latin square yields a multiplication table.

Conversely, the body of the multiplication table of a (finite) quasigroup Q yields a Latin square. Consider fixed elements x and z of Q. The existence of the solution y to the equation $x \cdot y = z$ means that the element z appears at least once in the row of the multiplication table labeled by x (namely in the column labeled y). The uniqueness of the solution y to the equation $x \cdot y = z$ means that the element z appears at most once in the row of the multiplication table labeled by x. In similar fashion, for fixed y and z in Q, the existence and uniqueness of the solution x to the equation $x \cdot y = z$ means that each element z appears exactly once in the column labeled y.

1.2 Equational quasigroups

From the algebraic point of view, the combinatorial definition of a quasigroup given in the introduction has some serious disadvantages. In particular, a homomorphic image of a combinatorial quasigroup need not be a quasigroup (Exercise 2). An (*equational*) *quasigroup* $(Q, \cdot, /, \backslash)$ is thus defined as a set Q equipped with three binary operations of multiplication, *right division* / and *left division* $\backslash$, satisfying the identities:

$$\begin{aligned} &\text{(IL)} \quad y\backslash(y \cdot x) = x\,; \\ &\text{(IR)} \quad x = (x \cdot y)/y\,; \\ &\text{(SL)} \quad y \cdot (y\backslash x) = x\,; \\ &\text{(SR)} \quad x = (x/y) \cdot y\,. \end{aligned}$$

Read x/y as "x divided by y" or "x over y." Read $x\backslash y$ as "x dividing y" or "x into y." To reduce the number of brackets required in quasigroup words, multiplications expressed implicitly by juxtaposition will be taken to bind more strongly than the divisions or explicitly expressed multiplications. With this convention, the left-hand side of (IL) reduces to $y\backslash yx$, while the associative law becomes $xy \cdot z = x \cdot yz$.

PROPOSITION 1.1
If $(Q, \cdot, /, \backslash)$ is an equational quasigroup, then $(Q, \cdot)$ is a combinatorial quasigroup.

PROOF It must be shown that knowledge of any two of x, y, z in

$$x \cdot y = z \tag{1.2}$$

specifies the third uniquely. Now the existence and uniqueness of z given x and y corresponds to the functionality of the multiplication (1.1). Suppose

that x and z are given. By (SL), $y = x\backslash z$ is one solution of Equation (1.2). On the other hand, if y' is a solution, then

$$y = x\backslash z = x\backslash(x \cdot y') = y'$$

by (IL), so the solution $x\backslash z$ is unique. The existence and uniqueness of x as a solution of (1.2) given y and z follows similarly. □

Conversely, suppose that $(Q, \cdot)$ is a combinatorial quasigroup. For given elements x and y of Q, define x/y as the unique solution of (SR), and $y\backslash x$ as the unique solution of (SL). This defines a right division $/ : Q^2 \to Q$ and left division $\backslash : Q^2 \to Q$ that make $(Q, \cdot, /, \backslash)$ an equational quasigroup. Thus it is usually not necessary to distinguish between the concepts of combinatorial and equational quasigroup: one refers simply to quasigroups.

The equational definition of quasigroups means that they form a variety (in the sense of "equationally defined class"), and are thus susceptible to study by the methods and concepts of universal algebra. (See Appendix B for a quick summary, or [165] for more detail). In particular, a subset P of a quasigroup Q is a *subquasigroup* of Q if it is closed under the three binary operations. Products of quasigroups become quasigroups under componentwise operations. An equivalence relation V on a quasigroup Q is a *congruence* if it is a subquasigroup of Q^2. A function $f : Q \to Q'$ from one quasigroup to another is a (*quasigroup*) *homomorphism* if it preserves all three quasigroup operations. For example, the natural projection

$$\mathrm{nat}\, V : Q \to Q^V; x \mapsto x^V := \{y \mid (x, y) \in V\}$$

of a quasigroup Q onto the quotient by a congruence relation V is a quasigroup homomorphism. A quasigroup Q is *simple* if its only congruence relations are the equality relation and the universal relation Q^2. Note that the class of all quasigroups forms the object class of a category **Q** whose morphisms are quasigroup homomorphisms.

More generally, a triple $(f_1, f_2, f_3) : Q \to Q'$ of maps from the underlying set Q of one quasigroup to the underlying set Q' of another is said to be a *homotopy* if

$$xf_1 \cdot yf_2 = (xy)f_3 \tag{1.3}$$

for all x, y in Q. In (1.3), one may regard juxtaposition as the multiplication in Q and $\cdot$ as the multiplication in Q'. The class of all quasigroups then forms the object class of a new category **Qtp** whose morphisms are quasigroup homotopies. The composite of homotopies $(f_1, f_2, f_3) : Q \to Q'$ and $(g_1, g_2, g_3) : Q' \to Q''$ is the homotopy $(f_1g_1, f_2g_2, f_3g_3) : Q \to Q''$. There is a forgetful functor

$$\Sigma : \mathbf{Q} \to \mathbf{Qtp} \tag{1.4}$$

preserving objects, and sending a quasigroup homomorphism $f : Q \to Q'$ to the homotopy $(f, f, f) : Q \to Q'$. A function $f : Q \to Q'$ connecting

the underlying sets of equational quasigroups $(Q, \cdot, /, \backslash)$ and $(Q' \cdot, /, \backslash)$ is a quasigroup homomorphism if it is a homomorphism $f : (Q, \cdot) \to (Q', \cdot)$ for the multiplications. Thus a homotopy (f_1, f_2, f_3) which has equal components $f_1 = f_2 = f_3$ is an element of the image of the morphism part of the forgetful functor (1.4).

If the f_i in (1.3) are bijections, then the triple (f_1, f_2, f_3) is said to be an *isotopy*, while the domain and codomain quasigroups are said to be *isotopic*. Thus isotopies are the isomorphisms (invertible morphisms) of the category **Qtp**. Note that isotopy provides an equivalence relation on any set of quasigroups. An isotopy $(g_1, g_2, g_3) : Q \to Q$ with equal domain and codomain Q is said to be *principal* if its third component g_3 is the identity map 1 or 1_Q on Q. Each isotopy $(f_1, f_2, f_3) : Q \to Q'$ factorizes as the product $(f_1, f_2, f_3) = (f_1 f_3^{-1}, f_2 f_3^{-1}, 1_Q)(f_3, f_3, f_3)$ of a principal isotopy and an isomorphism.

Given three permutations f_i of the underlying set Q of a quasigroup with multiplication denoted by juxtaposition, one may use (1.3) to define a new quasigroup multiplication $\cdot$ on Q, isotopic to the original multiplication. If the original multiplication is defined by a Latin square as discussed in Section 1.1, then f_1 corresponds to a permutation of row labels, f_2 a permutation of column labels, and f_3 a permutation of the symbols (elements of Q) entered in the Latin square.

1.3 Conjugates

A combinatorial quasigroup $(Q, \cdot)$ yields an equational quasigroup $(Q, \cdot, /, \backslash)$, which in turn yields combinatorial quasigroups $(Q, /)$ and $(Q, \backslash)$. For example, abelian groups form nonassociative quasigroups under their right division operation, namely subtraction. But Q or $(Q, \cdot)$ also yields the *opposite* quasigroup Q° or $(Q, \circ)$ with *opposite multiplication*

$$x \circ y = y \cdot x \tag{1.5}$$

for x, y in Q. There are corresponding *opposite divisions*

$$x // y = y / x \quad \text{and} \quad x \backslash\backslash y = y \backslash x \tag{1.6}$$

and combinatorial quasigroups $(Q, //), (Q, \backslash\backslash)$. Each quasigroup Q thus determines a full set of six potentially distinct combinatorial quasigroups, known as the *conjugates* of Q.

In specifying the equational quasigroups conjugate to a given quasigroup, it pays to be systematic. Recall that the (disjoint cycle representations of the) elements of the symmetric group S_3 on the set $\{1, 2, 3\}$ may be displayed as

the nodes of the Cayley diagram

$$\begin{array}{ccccc} (1) & \Longleftrightarrow & (23) & \longleftrightarrow & (123) \\ \updownarrow & & & & \Updownarrow \\ (12) & \Longleftrightarrow & (132) & \longleftrightarrow & (13) \end{array} \tag{1.7}$$

where the single arrows denote the action of right multiplication by the involution (12), and the double arrows denote the action of right multiplication by the involution (23). Trading typography for geometry, one might also imagine (1.7) displayed so that its nodes form a regular hexagon.

Now consider the equation $x_1 \cdot x_2 = x_3$ in a quasigroup $(Q, \cdot)$. Applying the various elements of S_3 from (1.7) to the suffices of the terms of this equation, one obtains the following display of the conjugate operations

$$\begin{array}{ccccc} \boxed{x_1 \cdot x_2 = x_3} & \Longleftrightarrow & \boxed{x_1 \backslash x_3 = x_2} & \longleftrightarrow & \boxed{x_2 // x_3 = x_1} \\ \updownarrow & & & & \Updownarrow \\ \boxed{x_2 \circ x_1 = x_3} & \Longleftrightarrow & \boxed{x_3 \backslash\backslash x_1 = x_2} & \longleftrightarrow & \boxed{x_3 / x_2 = x_1} \end{array} , \tag{1.8}$$

which then feature in turn as the multiplications of the conjugate equational quasigroups

$$\begin{array}{ccccc} (Q, \cdot, /, \backslash) & \Longleftrightarrow & (Q, \backslash, //, \cdot) & \longleftrightarrow & (Q, //, \backslash, \circ) \\ \updownarrow & & & & \Updownarrow \\ (Q, \circ, \backslash\backslash, //) & \Longleftrightarrow & (Q, \backslash\backslash, \circ, /) & \longleftrightarrow & (Q, /, \cdot, \backslash\backslash) \end{array} . \tag{1.9}$$

In (1.9), the multiplications cycle round in one sense

$$(\cdot, \backslash, //, /, \backslash\backslash, \circ),$$

while the right divisions and left divisions cycle round in the opposite sense:

$$(/, //, \backslash, \cdot, \circ, \backslash\backslash).$$

Finally, note that the identities (IR) in $(Q, \backslash)$ and (IL) in (Q,/) yield the respective identities

$$\begin{array}{l} \text{(DL) } y/(x\backslash y) = x\,, \\ \text{(DR) } x = (y/x)\backslash y \end{array}$$

in the basic quasigroup divisions.

1.4 Semisymmetry and homotopy

A quasigroup is said to be *semisymmetric* if it satisfies the identity

$$(yx)y = x\,.$$

The category of semisymmetric quasigroups and homomorphisms between them is denoted by **P**. Equivalent characterizations of semisymmetry are given by the following.

PROPOSITION 1.2
The following quasigroup identities are equivalent:

(a) $(yx)y = x$;

(b) $y(xy) = x$;

(c) $y\backslash x = xy$;

(d) $x/y = yx$.

In particular, each holds in **P**.

PROOF First note that (a) holds in **P**, by definition. Moreover, a quasigroup Q satisfies (a) if and only if its opposite Q° satisfies (b). Now if Q satisfies (a), one has $y(xy) = ((xy)x)(xy) = x$ there, so that (b) holds in Q. Thus if (b) holds in Q, then (a) holds in Q°, whence (b) holds in Q° and (a) holds in Q. Finally, the implications (a)⇔(d) and (b)⇔(c) are immediate. □

COROLLARY 1.1
Let $(Q, \cdot)$ *be a set with a binary multiplication satisfying* (a) *or* (b). *Defining a right division by* (d) *and a left division by* (c) *then yields a semisymmetric quasigroup* $(Q, \cdot, /, \backslash)$.

Regarding (1.8) as an action of the symmetric group S_3, one may restrict to the action of the cyclic subgroup C_3 generated by (123). There are two orbits of this action: $\{//, \backslash\backslash\,\cdot\}$ and $\{/, \backslash, \circ\}$. Proposition 1.2 says that a quasigroup Q is semisymmetric if and only if all three operations of each of these orbits agree on Q. It may thus seem that semisymmetric quasigroups are rather special. Nevertheless, each quasigroup Q or $(Q, \cdot, /, \backslash)$ defines a semisymmetric

quasigroup structure $Q\Delta$ on the direct cube Q^3 with multiplication as follows:

$$\begin{aligned} &(\quad x_1 \quad , \quad x_2 \quad , \quad x_3 \quad) \cdot \\ &(\quad y_1 \quad , \quad y_2 \quad , \quad y_3 \quad) = \\ &(x_2 // y_3, x_3 \backslash\backslash y_1, x_1 \cdot y_2) \, . \end{aligned} \tag{1.10}$$

Note that the operations used in the bottom line of (1.10) are the successive elements of the C_3-orbit $\{//, \backslash\backslash, \cdot\}$. To verify that $Q\Delta$ is indeed a semisymmetric quasigroup according to Corollary 1.1, note that

$$\begin{aligned} &(y_1, y_2, y_3) \cdot (x_2 // y_3, x_3 \backslash\backslash y_1, x_1 \cdot y_2) = \\ &\quad \big(y_2 // (x_1 \cdot y_2), y_3 \backslash\backslash (x_2 // y_3), y_1 \cdot (x_3 \backslash\backslash y_1)\big) = (x_1, x_2, x_3), \end{aligned}$$

the components of the latter equality holding respectively by (IR), (DR), and (SL).

Now consider a quasigroup homotopy $(f_1, f_2, f_3) : (Q, \cdot) \to (Q', \cdot)$. Define

$$(f_1, f_2, f_3)^\Delta : Q\Delta \to Q'\Delta; (x_1, x_2, x_3) \to (x_1 f_1, x_2 f_2, x_3 f_3). \tag{1.11}$$

This map is a quasigroup homomorphism. Indeed, for (x_1, x_2, x_3) and (y_1, y_2, y_3) in $Q\Delta$, one has

$$\begin{aligned} &(x_1 f_1, x_2 f_2, x_3 f_3) \cdot (y_1 f_1, y_2 f_2, y_3 f_3) \\ &\quad = (x_2 f_2 // y_3 f_3, x_3 f_3 \backslash\backslash y_1 f_1, x_1 f_1 \cdot y_2 f_2) \\ &\quad = \big((x_2 // y_3) f_1, (x_3 \backslash\backslash y_1) f_2, (x_1 \cdot y_2) f_3\big) \\ &\quad = \big((x_1, x_2, x_3) \cdot (y_1, y_2, y_3)\big)(f_1, f_2, f_3)^\Delta, \end{aligned}$$

the central equality holding by (1.3) and (1.8). Thus there is a functor

$$\Delta : \mathbf{Qtp} \to \mathbf{P}, \tag{1.12}$$

known as the *semisymmetrization functor*, with object part (1.10) and morphism part (1.11). This functor has a left adjoint, namely the restriction $\Sigma : \mathbf{P} \to \mathbf{Qtp}$ of the forgetful functor (1.4) [156, Th. 5.2]. The semisymmetrization functor reduces many questions about homotopies between general quasigroups to homomorphisms between semisymmetric quasigroups. In particular, two quasigroups are isotopic if and only if their semisymmetrizations are isomorphic semisymmetric quasigroups.

1.5 Loops and piques

A *loop* is a (nonempty) quasigroup Q with an *identity* element, an element e such that the equations $ex = x = xe$ hold for all x in Q. Loops form the nonempty members of the variety of quasigroups satisfying the identity

$$x\backslash x = y/y\,. \tag{1.13}$$

In a nonempty quasigroup, both sides of this identity evaluate to the identity element e of the loop, and then the equations $ex = x$, $xe = x$ follow from the respective quasigroup identities $(x/x)x = x$ and $x(x\backslash x) = x$. More strikingly, loops may be characterized as nonempty quasigroups endowed with a modicum of associativity:

PROPOSITION 1.3
A nonempty quasigroup Q is a loop if and only if it satisfies the "slightly associative identity"

$$x(y/y)\cdot z = x\cdot(y/y)z. \tag{1.14}$$

PROOF If Q is a loop with identity e, then $y/y = e$, and (1.14) follows. Conversely, suppose that (1.14) is satisfied. Setting $z = y$, one obtains $xy = x(y/y)\cdot y$ from (SR), so $x(y/y) = x$. Dividing from the left by x yields $y/y = x\backslash x$. □

Augmenting the type by adding a constant, loops may also be construed as algebras $(Q, \cdot, /, \backslash, e)$ such that $(Q, \cdot, /, \backslash)$ is a quasigroup and e is a nullary operation satisfying the identities $e\cdot x = x = x\cdot e$. Thus loops form a variety **Lp**.

It is sometimes useful to consider a more general variety $\mathbf{Q}_0$ of algebras $(Q, \cdot, /, \backslash, e)$ of the same type, in which $(Q, \cdot, /, \backslash)$ is a quasigroup, while e is only required to satisfy the identity $ee = e$. Such an algebra is called a *pique*, from an acronym for "pointed idempotent quasigroup." The semisymmetrization $Q\Delta$ of any pique $(Q, \cdot, e)$ may again be construed as a pique, with pointed idempotent (e, e, e). If $(A, +, 0)$ is an abelian group, then the subtraction operation yields a pique $(A, -, 0)$ with the zero element as the pointed idempotent. Note that $(1, -1, 1) : (A, +) \to (A, -)$ is a principal isotopy. While groups may have nonassociative pique isotopes, they cannot have nonassociative loop isotopes.

PROPOSITION 1.4
If a loop is isotopic to a group, then it is isomorphic to the group. In particular, isotopic groups are isomorphic.

PROOF It suffices to consider a principal isotopy

$$(f, g, 1_Q) : (Q, \circ, 1) \to (Q, \cdot, /, \backslash)$$

between a loop structure $(Q, \circ, 1)$ and a group structure $(Q, \cdot, /, \backslash)$ on a set Q, so that $x^f \cdot y^g = x \circ y$ for x, y in Q. Since $1^f \cdot y^g = 1 \circ y = y$, one has $y^g = 1^f \backslash y$. Similarly, $x^f = x/1^g$. Then

$$(1^f \cdot x \cdot 1^g) \circ (1^f \cdot y \cdot 1^g) = 1^f \cdot x \cdot y \cdot 1^g,$$

making $(Q, \cdot) \to (Q, \circ); q \mapsto 1^f \cdot q \cdot 1^g$ the required isomorphism. □

A quasigroup Q is said to be *idempotent* if it satisfies the identity

$$x \cdot x = x. \tag{1.15}$$

Write **Ip** for the category of idempotent quasigroups and homomorphisms. An idempotent quasigroup Q yields a loop Q' or $(Q', +, 0)$ on the disjoint union Q' of the set Q with a singleton $\{0\}$. The loop multiplication $+$ is specified by setting

$$x + y = \begin{cases} 0 & \text{if } x = y; \\ x \cdot y & \text{otherwise} \end{cases} \tag{1.16}$$

for elements x, y of Q.

PROPOSITION 1.5

Given an idempotent quasigroup Q, the specification (1.16)*, together with the loop identities $0 + x = x = x + 0$, defines a loop structure $(Q', +, 0)$ on the disjoint union Q' of Q and $\{0\}$.*

PROOF By hypothesis, each element of Q occurs exactly once in each row of the multiplication table of Q. Consider the augmentation of this table to the multiplication table of Q' by the addition of a new row and a new column, each labeled 0. According to (1.16), the unique occurrence of x in the diagonal position of the row labeled x in the multiplication table of Q is occupied by 0 in the multiplication table of Q', while the element x is moved there to the beginning of the row, the new column labeled by 0. The remaining elements are left unchanged. Thus each element of Q' appears exactly once in each row of the multiplication table of Q'. The behavior of columns is similar. □

The construction of Proposition 1.5 is illustrated by the example given in Figure 1.3.

Q	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

Q'	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	4	0	1	3
3	3	2	4	0	1
4	4	3	1	2	0

FIGURE 1.3: A unipotent loop from an idempotent quasigroup.

A quasigroup Q is said to be *covered* by a set $\{Q_k \mid k \in K\}$ of subquasigroups Q_k of Q if each element x of Q is contained in at least one element Q_k of the set. For example, an idempotent quasigroup Q is covered by its set

$$\big\{\langle x\rangle \;\big|\; x \in Q\big\} = \big\{\{x\} \;\big|\; x \in Q\big\} \tag{1.17}$$

of singleton subquasigroups. Now suppose that a loop $(L, +, 0)$ is covered by a set of 2-element subloops. Each such subloop is isomorphic to the cyclic group $\mathbb{Z}/2\mathbb{Z}$. Indeed, a loop $(L, +, 0)$ has such a cover if and only if it satisfies the *unipotent identity*

$$x + x = 0. \tag{1.18}$$

Define $\mathbf{L}_2$ to be the variety of unipotent loops. One may then invert the construction of Proposition 1.5. Let L^* denote the set of nonidentity elements of a unipotent loop L. Define a product $\cdot$ on L^* by

$$x \cdot y = \begin{cases} x & \text{if } x = y; \\ x + y & \text{otherwise} \end{cases} \tag{1.19}$$

for elements x, y of L^*. An argument similar to that of Proposition 1.5 shows that $(L^*, \cdot)$ is an idempotent quasigroup. Then $L^{*\prime}$ is isomorphic to L. Conversely, for an idempotent quasigroup Q with corresponding loop Q', the quasigroup Q'^* is isomorphic to Q.

1.6 Steiner triple systems I

A *Steiner triple system* $(S, \mathcal{B})$ is a finite set S together with a set $\mathcal{B}$ of 3-element subsets of S, with the property that each pair of distinct elements of S is contained in exactly one element of $\mathcal{B}$.

Example 1.1 Projective spaces over $\mathsf{GF}(2)$
If S is the projective space $\mathsf{PG}(d, 2)$ of dimension d over the 2-element field, then taking $\mathcal{B}$ to be the set of lines yields a Steiner triple system $(S, \mathcal{B})$ which will also be described as $\mathsf{PG}(d, 2)$. The points of S may be represented by homogeneous coordinates, which in turn may be interpreted as length $d+1$ binary expansions of numbers from 1 to $2^{d+1}-1$. In the 2-dimensional case, one obtains

$$\mathcal{B} = \{246, 145, 347, 123, 257, 167, 356\}$$

on writing each 3-element line $\{a, b, c\}$ in the abbreviated form abc. □

Example 1.2 Affine spaces over $\mathsf{GF}(3)$
If S is the affine space $\mathsf{AG}(d, 3)$ of dimension d over the 3-element field, then taking $\mathcal{B}$ to be the set of lines again yields a Steiner triple system $(S, \mathcal{B})$ which will also be described as $\mathsf{AG}(d, 3)$. The points of S may be represented by Cartesian coordinates, which in turn may be interpreted as length d ternary expansions of numbers from 0 to 3^d-1. In the 2-dimensional case, one obtains

$$\mathcal{B} = \{012, 036, 048, 057, 138, 147, 156, 237, 246, 258, 345, 678\}$$

on writing each 3-element line $\{a, b, c\}$ in the abbreviated form abc. □

A Steiner triple system $(S, \mathcal{B})$ yields a quasigroup $(S, \cdot)$ on defining $x \cdot y = z$ whenever $x = y = z$ or $\{x, y, z\} \in \mathcal{B}$. Such a quasigroup is idempotent, and possesses the property of *total symmetry* expressed by the identities

$$x \cdot y = x/y = x\backslash y. \tag{1.20}$$

A quasigroup is totally symmetric if and only if all its conjugates coincide. Note that total symmetry is stronger than semisymmetry as studied in Section 1.4.

In the other direction, each idempotent, totally symmetric quasigroup $(S, \cdot)$ yields a Steiner triple system on defining

$$\mathcal{B} = \big\{ \{x, y, x \cdot y\} \;\big|\; x \neq y \in S \big\}.$$

It is convenient to identify each Steiner triple system $(S, \mathcal{B})$ with the corresponding idempotent, totally symmetric quasigroup $(S, \cdot)$.

Algebraic constructions of quasigroups furnish useful models of Steiner triple systems. One may immediately realize $\mathsf{AG}(d,3)$ as the d-th direct power of the 3-element system $\mathsf{AG}(1,3)$ or $\mathsf{PG}(1,2)$. A slightly more sophisticated construction invokes the equivalence of Section 1.5 between idempotent quasigroups and unipotent loops. For example, a Steiner triple system of size 39 may be constructed as follows. Consider the system $Q_1 = \mathsf{PG}(1,2)$ of size 3 and its direct square $Q_2 = \mathsf{PG}(1,2)^2 = \mathsf{AG}(2,3)$ of size 9. These are both idempotent quasigroups. The corresponding loops Q_1' and Q_2' in the variety $\mathbf{L}_2$ have respective sizes 4 and 10, so their product $Q_1' \times Q_2'$ there has size 40. The equivalent idempotent quasigroup $(Q_1' \times Q_2')^*$ is totally symmetric, and identifies with the desired Steiner triple system of size 39.

1.7 Moufang loops and octonions

Let F be a field. A *Zorn vector-matrix* over F is a 2×2 matrix

$$z = \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \tag{1.21}$$

in which α and β are scalars from F, while $\mathbf{a}$ and $\mathbf{b}$ are 3-dimensional row vectors over F. A *Zorn scalar* is a vector-matrix of the form

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$$

for an element α of the field F. In particular, the *Zorn identity matrix* is the vector-matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The *trace* of the Zorn vector-matrix (1.21) is the field element

$$\mathrm{Tr}(z) = \alpha + \beta. \tag{1.22}$$

The *Zorn conjugate* of the Zorn vector-matrix (1.21) is the Zorn vector-matrix

$$z' = \begin{bmatrix} \beta & -\mathbf{a} \\ -\mathbf{b} & \alpha \end{bmatrix}. \tag{1.23}$$

The *norm* or *Zorn determinant* of the Zorn vector-matrix (1.21) is the field element

$$\mathrm{N}(z) = \begin{vmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{vmatrix} = \alpha\beta - \mathbf{a} \cdot \mathbf{b} \tag{1.24}$$

defined using the usual scalar product

$$\mathbf{a} \cdot \mathbf{b} = [a_1\ a_2\ a_3] \cdot [b_1\ b_2\ b_3] = a_1b_1 + a_2b_2 + a_3b_3$$

of row vectors.

DEFINITION 1.1 *The* Zorn vector-matrix algebra $\mathsf{Zorn}(\mathsf{F})$ *over the field* F *is the* 8*-dimensional* F*-vector space of all Zorn vector-matrices over* F*. The vector space operations are defined componentwise, while the product of two Zorn vector-matrices is given as*

$$\begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \cdot \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix} = \begin{bmatrix} \alpha\gamma + \mathbf{a} \cdot \mathbf{d} & \alpha\mathbf{c} + \delta\mathbf{a} - \mathbf{b} \times \mathbf{d} \\ \gamma\mathbf{b} + \beta\mathbf{d} + \mathbf{a} \times \mathbf{c} & \mathbf{b} \cdot \mathbf{c} + \beta\delta \end{bmatrix} \tag{1.25}$$

using the usual vector or cross product

$$[a_1\ a_2\ a_3] \times [b_1\ b_2\ b_3] = \begin{bmatrix} \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} & \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} & \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \end{bmatrix}$$

of row vectors. The field F *is identified with the subalgebra of Zorn scalars; indeed*

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \cdot \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} = \begin{bmatrix} \lambda\alpha & \lambda\mathbf{a} \\ \lambda\mathbf{b} & \lambda\beta \end{bmatrix} = \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \cdot \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \tag{1.26}$$

for λ *in* F*.*

PROPOSITION 1.6
Each Zorn vector matrix z *satisfies the quadratic equation*

$$x^2 - \mathrm{Tr}(z)x + \mathrm{N}(z) = 0 \tag{1.27}$$

together with its Zorn conjugate.

PROOF The satisfaction of (1.27) follows from

$$z + z' = \mathrm{Tr}(z) \tag{1.28}$$

and

$$z \cdot z' = \mathrm{N}(z). \tag{1.29}$$

(Note the identification of scalars with the corresponding Zorn scalar matrices.) □

The Zorn vector-matrix algebra $\mathsf{Zorn}(\mathsf{F})$ may be directly verified to satisfy the (*third*) *Moufang identity*

$$zx \cdot yz = (z \cdot xy)z \tag{1.30}$$

(Exercise 18). A loop satisfying (1.30) is said to be a *Moufang loop*. A loop is said to be *diassociative* if each subloop generated by two elements

is associative. The most important classical result about Moufang loops is Moufang's Theorem, stating that Moufang loops are diassociative [21, VII.4].

The norm in the Zorn vector-matrix algebra $\mathsf{Zorn}(\mathsf{F})$ is *multiplicative*, in the sense that

$$\mathrm{N}(x)\mathrm{N}(y) = \mathrm{N}(xy) \tag{1.31}$$

for x, y in $\mathsf{Zorn}(\mathsf{F})$. (Compare Exercise 16.) For each element t of F, let $\mathrm{M}_t(\mathsf{F})$ be the set of Zorn vector-matrices over F whose norm is t.

PROPOSITION 1.7

Under the multiplication (1.25)*, the set* $\mathrm{M}_1(\mathsf{F})$ *of Zorn vector-matrices of norm* 1 *forms a Moufang loop* $(\mathrm{M}_1(\mathsf{F}), \cdot, I)$.

PROOF The multiplicativity (1.31) of the norm shows that $\mathrm{M}_1(\mathsf{F})$ is closed under multiplication. Consider the bilinear form

$$\langle z \,|\, t \rangle = \mathrm{N}(z + t) - \mathrm{N}(z) - \mathrm{N}(t) \tag{1.32}$$

given by the norm on the vector-matrix algebra, namely

$$\left\langle \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \,\middle|\, \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix} \right\rangle = \alpha\delta + \beta\gamma - \mathbf{a}\cdot\mathbf{d} - \mathbf{b}\cdot\mathbf{c}\,. \tag{1.33}$$

From (1.33) it is apparent that the bilinear form is nondegenerate. Now multiplication on the left or right by an element x of norm one preserves the nondegenerate form. For example,

$$\begin{aligned} \langle zx \,|\, tx \rangle &= \mathrm{N}\big((z+t)x\big) - \mathrm{N}(zx) - \mathrm{N}(tx) \\ &= \mathrm{N}(z+t)\mathrm{N}(x) - \mathrm{N}(z)\mathrm{N}(x) - \mathrm{N}(t)\mathrm{N}(x) \\ &= \mathrm{N}(z+t) - \mathrm{N}(z) - \mathrm{N}(t) = \langle z \,|\, t \rangle\,. \end{aligned}$$

Thus the right and left multiplications by x are representable by orthogonal matrices. This implies that the multiplications are invertible, making $\mathrm{M}_1(\mathsf{F})$ a loop. □

For a prime power q, let $\mathrm{M}_1(q)$ denote the loop $\mathrm{M}_1(\mathsf{F})$ over the finite field F of order q. The group $\{\pm 1\}$ of scalars acts by multiplication on $\mathrm{M}_1(q)$, so that the orbits are the classes of a loop congruence on $\mathrm{M}_1(q)$. Let $\mathrm{M}(q)$ denote the corresponding quotient. Paige showed that the Moufang loops $\mathrm{M}(q)$ are simple [123]. Using work of Doro [46], and the classification of finite simple groups, Liebeck [104] showed that up to isomorphism, the $\mathrm{M}(q)$ are the only nonassociative finite simple Moufang loops.

Over a field F, define the 3-dimensional unit vectors

$$\mathbf{u}_1 = [1\ 0\ 0], \quad \mathbf{u}_2 = [0\ 1\ 0], \quad \mathbf{u}_3 = [0\ 0\ 1].$$

In the complex Zorn vector-matrix algebra $\mathsf{Zorn}(\mathbb{C})$, consider the elements $e_0 = 1$,

$$e_4 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, e_j = \begin{bmatrix} 0 & -\mathbf{u}_j \\ \mathbf{u}_j & 0 \end{bmatrix}, \text{ and } e_{4+j} = \begin{bmatrix} 0 & i\mathbf{u}_j \\ i\mathbf{u}_j & 0 \end{bmatrix}$$

for $1 \leq j \leq 3$. Note that $e_j^2 = -1$ for $1 \leq j \leq 7$. Then the algebra $\mathbb{R}$ of real numbers forms the real span of the subset $\{e_0\}$ of $\mathsf{Zorn}(\mathbb{C})$. The algebra $\mathbb{C}$ of complex numbers forms the real span of the subset $\{e_0, e_1\}$ of $\mathsf{Zorn}(\mathbb{C})$. The algebra $\mathbb{H}$ of quaternions forms the real span of the subset $\{e_0, e_1, e_2, e_3\}$ of $\mathsf{Zorn}(\mathbb{C})$: indeed $e_1e_2 = e_3 = -e_2e_1$, etc. (Compare [165, Ch. II, Ex.2.4S].) Now

$$e_j e_k \in \{\pm e_{j*k}\} \tag{1.34}$$

for $1 \leq j, k \leq 7$, the product $*$ being taken in the projective geometry $\mathsf{PG}(2,2)$ of Section 1.6. [In fact, (1.34) holds for $0 \leq j, k \leq 7$ if the product $*$ is taken in the unipotent loop $\mathsf{PG}(2,2)'$ of the projective geometry $\mathsf{PG}(2,2)$.] Then the real span of the subset

$$\{e_0, \ldots, e_7\} \tag{1.35}$$

of $\mathsf{Zorn}(\mathbb{C})$ forms an 8-dimensional real algebra $\mathbb{K}$, the *Cayley numbers* or *octonions*. The norms of octonions are real. The argument of the proof of Proposition 1.7 shows that the set S^7 of nonzero octonions of norm 1 forms a Moufang loop under multiplication. (Geometrically, this set is a 7-sphere.) It follows that the set $\mathbb{K}^*$ of nonzero octonions also forms a Moufang loop, while the full set of octonions forms a real normed division algebra.

1.8 Triality

The quasigroup conjugates introduced in Section 1.3 display a high degree of symmetry. This symmetry is known as *triality*. It is very helpful for dealing with the equational structure of quasigroups, as in the Normal Form Theorem 1.2 in Section 1.9 below. In order to exploit the symmetry, postfix notation is most appropriate. The quasigroup product $x \cdot y$ is written in the form $xy\mu$. A repeated product such as $xy \cdot (xz \cdot y)$ is then written as $xy\mu\, xz\mu\, y\mu\, \mu$. These repeated products are parsed using the rule that each multiplication μ multiplies the two arguments or completed products to its immediate left. Thus $xy\mu\, xz\mu\, y\mu\, \mu$ unravels as

$$\begin{aligned} xy\mu\, xz\mu\, y\mu\, \mu &= (xy\mu) \cdot (xz\mu\, y\mu) \\ &= xy \cdot (xz\mu \cdot y) \\ &= xy \cdot (xz \cdot y)\,. \end{aligned}$$

Writing σ and τ for the respective generators (12) and (23) of S_3, the Cayley diagram (1.7) of S_3 becomes

$$\begin{array}{ccccc} 1 & \Longleftrightarrow & \tau & \longleftrightarrow & \tau\sigma \\ \updownarrow & & & & \Updownarrow \\ \sigma & \Longleftrightarrow & \sigma\tau & \longleftrightarrow & \sigma\tau\sigma \end{array} .$$

Note that the third transposition (13) or $\sigma\tau\sigma$ may also be written as $\tau\sigma\tau$. The six conjugate operations are correspondingly displayed in Figure 1.4 as the successive images μ^g of the multiplication μ under a regular right action by the elements g of S_3.

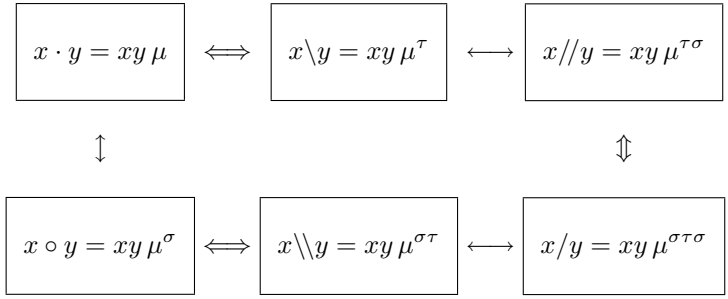


FIGURE 1.4: Triality symmetry of the quasigroup operations.

It is interesting to note that the opposite of each operation μ^g is given by $\mu^{\sigma g}$. In other words, passage to the opposite operation corresponds to left multiplication by the transposition σ. The pairs of opposite operations lie in the three respective columns of Figure 1.4.

Left multiplication by τ also has a simple interpretation. Let M be the set of binary operations on a quasigroup. Formally, this set may be considered as the free algebra on two generators x, y in the variety $\mathbf{Q}$ of quasigroups (compare Appendix B). Define a multiplication $*$ on M by

$$xy(\alpha * \beta) = x\,xy\alpha\,\beta\,. \tag{1.36}$$

Define the binary operation ϵ as the right projection $xy\epsilon = y$.

PROPOSITION 1.8

The set M of binary quasigroup operations forms a monoid $(M, *, \epsilon)$ under the multiplication (1.36)*, with identity element ϵ.*

PROOF First note that

$$xy(\alpha * \epsilon) = x\, xy\alpha\, \epsilon = xy\alpha$$

and

$$xy(\epsilon * \alpha) = x\, xy\epsilon\, \alpha = xy\alpha$$

for α in M, so that ϵ is an identity element. Now consider α, β, γ in M. Then

$$\begin{aligned} xy\big((\alpha * \beta) * \gamma\big) &= x\, xy(\alpha * \beta)\, \gamma \\ &= x(xxy\alpha\beta)\gamma \\ &= xxxy\alpha\beta\gamma \\ &= xx(xy\alpha)\beta\gamma \\ &= x\, xy\alpha(\beta * \gamma) = xy\big(\alpha * (\beta * \gamma)\big)\,, \end{aligned}$$

verifying the associativity of the multiplication (1.36). □

The significance of the left multiplication by τ then follows.

THEOREM 1.1
For each element g of S_3, the binary operation μ^g is an invertible element of the monoid M, with inverse $\mu^{\tau g}$. Thus the quasigroup operations generate a subgroup of M.

PROOF The identity (IL), namely $x\backslash(x \cdot y) = y$, becomes $x\, xy\mu\, \mu^\tau = y$ or $\mu * \mu^\tau = \epsilon$. Similarly (SL), namely $x \cdot (x\backslash y) = y$, becomes $x\, xy\mu^\tau\, \mu = x$ or $\mu^\tau * \mu = \epsilon$. Thus μ and μ^τ are mutual inverses.

The identity (IR), namely $(y \cdot x)/x = y$, may be written as $x//(x \circ y) = y$. This becomes $x\, xy\mu^\sigma\, \mu^{\tau\sigma} = y$ or $\mu^\tau * \mu^{\tau\sigma} = \epsilon$. Similarly (SR), namely $(y/x) \cdot x = y$, may be written as $x \circ (x//y) = y$. This becomes $x\, xy\mu^{\tau\sigma}\, \mu^\sigma = y$ or $\mu^{\tau\sigma} * \mu^\tau = \epsilon$. Thus μ^σ and $\mu^{\tau\sigma}$ are mutual inverses.

The identity (DR), namely $(x/y)\backslash x = y$, may be written as $x\backslash\backslash(x/y) = y$. This becomes $x\, xy\mu^{\tau\sigma\tau}\, \mu^{\sigma\tau} = y$ or $\mu^{\tau\sigma\tau} * \mu^{\sigma\tau} = \epsilon$. Finally (DL), namely $x/(y\backslash x) = y$, may be written as $x/(x\backslash\backslash y) = y$. This becomes $x\, xy\mu^{\sigma\tau}\, \mu^{\tau\sigma\tau} = y$ or $\mu^{\sigma\tau} * \mu^{\tau\sigma\tau} = \epsilon$. Thus $\mu^{\sigma\tau}$ and $\mu^{\tau\sigma\tau}$ are mutual inverses. □

COROLLARY 1.2
A quasigroup may be defined as an algebra Q equipped with a binary operation μ^g for each element g of the group S_3, such that the hypercommutative law

$$xy\, \mu^g = yx\, \mu^{\sigma g}$$

and the hypercancellation law

$$x\, xy\mu^g\, \mu^{\tau g} = y$$

are satisfied for each element g of S_3.

Now let H be a subgroup of S_3. A quasigroup is said to be *H-symmetric* if it satisfies the identity

$$xy\,\mu^g = xy\,\mu^{gh} \tag{1.37}$$

for each g in S_3 and h in H. Semisymmetry is $\langle\sigma\tau\rangle$-symmetry. and total symmetry becomes S_3-symmetry in the current sense. Commutativity is just $\langle\sigma\rangle$-symmetry. The remaining nontrivial cases are covered by the following proposition, whose proof is relegated to Exercise 27.

PROPOSITION 1.9
Let Q be a quasigroup.

(a) *The following are equivalent:*

(i) *Q is $\langle\tau\rangle$-symmetric;*

(ii) *$(Q, /)$ is commutative;*

(iii) *$(Q, \cdot)$ satisfies the* left symmetric identity

$$x \cdot (x \cdot y) = y\,. \tag{1.38}$$

(b) *The following are equivalent:*

(i) *Q is $\langle\sigma\tau\sigma\rangle$-symmetric;*

(ii) *$(Q, \backslash)$ is commutative;*

(iii) *$(Q, \cdot)$ satisfies the* right symmetric identity

$$(y \cdot x) \cdot x = y\,. \tag{1.39}$$

Together, (1.38) and (1.39) are known as *symmetric identities*.

1.9 Normal forms

A quasigroup Q determines a ternary relation T or

$$T(Q) = \{(x_1, x_2, x_3) \in Q^3 \mid x_1 \cdot x_2 = x_3\}\,.$$

known as the (*ternary*) *multiplication table* of Q. The multiplication table has the property that for any two elements (x_i, x_2, x_3), (x'_1, x'_2, x'_3) of T,

$$\big|\{1 \le i \le 3 \mid x_i = x'_i\}\big| \ne 2\,.$$

This property is called the *Latin square property* of the table T. It is equivalent to the combinatorial property (1.1) defining quasigroup multiplications. Now let X be a set. A *partial Latin square* on X is a ternary relation U on X that has the Latin square property. Formally, one may consider a partial Latin square as such a pair (X, U). A quasigroup Q is said to *extend* a partial Latin square (X, U) if X is a subset of Q and U is a subset of $T(Q)$. Such an extension Q is said to be *free* if the embedding of X in any extension Q' extends to a unique quasigroup homomorphism from Q to Q'. The goal of this section is to show that each partial Latin square (X, U) possesses a free extension $Q_{(X,U)}$, and to give an explicit description of the extension.

Let (X, U) be a partial Latin square. In order to describe the extension $Q_{(X,U)}$, it is most convenient to construe quasigroups in the form given by Corollary 1.2, as algebras with the set

$$\mu^{S_3} = \{\mu^g \mid g \in S_3\} \tag{1.40}$$

of binary operations, satisfying the hypercommutative and hypercancellation laws. Consider the free monoid $(X + \mu^{S_3})^*$, the set of words with letters taken from the disjoint union $X + \mu^{S_3}$ of X with the set (1.40). The set (1.40) — or more precisely its image in the disjoint union — acts as a set of binary operations on $(X + \mu^{S_3})^*$, with

$$\mu^g : (w, w') \mapsto ww'\mu^g$$

for w, w' in $(X + \mu^{S_3})^*$ and g in S_3. Let W_X or W be the subalgebra of

$$\left((X + \mu^{S_3})^*, \mu^{S_3}\right)$$

generated by X. An equivalence relation V will be defined on the set W of words, such that the set W^V of equivalence classes will carry the structure of the free extension $Q_{(X,U)}$. Each equivalence class will be represented by a unique word, of minimal length amongst all the words in the class. This representative is the *normal form* of the words in the class.

Given a word w in W, its normal form is obtained by an iterative process known as *rewriting*. The steps in the process are known as *rewritng rules*. First, each instance of $uv\mu^g$ in w with u, v in W may be replaced by $vu\mu^{\sigma g}$, to obtain a new word w', of the same length as w. Two words are said to be *σ-equivalent* if they are related by a (possibly empty) sequence of such replacements. Note that if a word w contains r letters from μ^{S_3}, then it has 2^r σ-equivalent forms (Exercise 31). A word w from W is said to be *primary* if it does not include the letters μ^σ, $\mu^{\sigma\tau}$, $\mu^{\tau\sigma}$ (the opposites of the respective basic quasigroup operations $\cdot$, $\backslash$, $/$). Each σ-equivalence class has a unique primary representative. The normal form is chosen as the primary representative of its σ-equivalence class.

The remaining rewriting rules are of two kinds, each reducing the length of words. They are known as *reduction rules*. The first of these reduction

rules implements hypercancellation. Thus if some σ-equivalent of w contains an instance of $u\,uv\mu^g\,\mu^{\tau g}$ with u, v in W, the subword $u\,uv\mu^g\,\mu^{\tau g}$ may be replaced by v to yield an equivalent but shorter word w'. A rewriting step of this kind is denoted by $w \to w'$, or more explicitly by

$$w \xrightarrow{g} w'\,. \tag{1.41}$$

The second reduction rule depends on an element $x = (x_1, x_2, x_3)$ of the partial Latin square U. Note that such a triple represents an equation

$$x_{1g}x_{2g}\mu^g = x_{3g}$$

for each element g of S_3. Now if a σ-equivalent of the word w involves $x_{1g}x_{2g}\mu^g$ as a subword, this subword may be replaced by x_{3g} to yield an equivalent but shorter word w'. A rewriting step of this kind is denoted by $w \to w'$, or more explicitly by

$$w \xrightarrow{x_g} w'\,. \tag{1.42}$$

The equivalence relation V is defined as the smallest equivalence relation on W that contains the set of pairs (w, w') for which either w and w' are σ-equivalent, or for which one of (1.41) or (1.42) holds. Note that V is a congruence of the algebra (W, μ^{S_3}).

A given word w of W initiates a maximal chain

$$w \to w_1 \to w_2 \to \cdots \to \overline{w} \tag{1.43}$$

of reductions of types (1.41) or (1.42), with implicit σ-equivalences at the tail of each arrow. The final node $\overline{w}$, representing the normal form of w, is taken to be in primary form. Note that w and $\overline{w}$ are related by V. The following theorem shows that there is a unique normal form $\overline{w}$ terminating a reduction chain that starts with the given word w.

THEOREM 1.2 (***Normal Form Theorem***)
Let w be a word in W. If w has two maximal reduction chains of type (1.43)*, namely*

$$w \to w_1 \to w_2 \to \cdots \to \overline{w}_k \tag{1.44}$$

and

$$w \to w'_1 \to w'_2 \to \cdots \to \overline{w}'_l\,, \tag{1.45}$$

then $\overline{w}_k = \overline{w}'_l$, so that w reduces to a unique normal form $\overline{w}$.

PROOF The proof proceeds by induction on the length of the word w in the alphabet $X + \mu^{S_3}$. If the length is 1, then w is just an element x of the set X. Now assume that the normal forms are unique for all words shorter than w. If w cannot be reduced further, then the normal form $\overline{w}$ is just the primary

representative of the σ-equivalence class of w. If w_1 and w_1' are σ-equivalent, then $\overline{w} = \overline{w_1} = \overline{w_1'}$ by the induction hypothesis, since w_1 is shorter than w. For example, if $w = u\,u\,ut\mu^g\,\mu^{\tau g}\,\mu^g$ for words t, u in W, then $w \to w_1$ may take the form

$$w = u\,u\,(ut\mu^g)\,\mu^{\tau g}\,\mu^g \xrightarrow{\tau g} ut\mu^g\,,$$

with $w \to w_1'$ as

$$w = u\,(u\,ut\mu^g\,\mu^{\tau g})\,\mu^g \xrightarrow{g} ut\mu^g\,.$$

Otherwise, w_1 and w_1' are σ-inequivalent, and the reduction chains (1.44), (1.45) begin as

$$\begin{array}{ccc} & \nearrow & w_1 \\ w & & \\ & \searrow & w_1' \end{array} \tag{1.46}$$

with diverging paths. It will be shown that one of the following occurs:

Triangle: There is a chain of reductions from one of w_1, w_1' to the other, without loss of generality from w_1' to w_1:

$$w_1' \to \cdots \to w_1\,.$$

In this case $\overline{w} = \overline{w_1}$.

Diamond: There is a word w_0 in W that lies on reduction chains

$$w_1 \to \cdots \to w_0$$

from w_1 and

$$w_1' \to \cdots \to w_0$$

from w_1'. In this case $\overline{w} = \overline{w_0}$.

Suppose that $w = uv\mu^g$ for words u, v in W. A reduction $w \to w_1$ is said to be *internal* if it is of the form $uv\mu^g \to u_1v\mu^g$ for a reduction $u \to u_1$ of u, or else of the form $uv\mu^g \to uv_1\mu^g$ for a reduction $v \to v_1$ of v. There are two possible cases for (1.46): **internal** and **external**.

Internal case: Here the initial reductions $w \to w_1$ and $w \to w_1'$ are both internal. If (1.46) takes the form

$$\begin{array}{ccc} & \nearrow & u_1v\mu^g \\ w = uv\mu^g & & \\ & \searrow & u_1'v\mu^g \end{array}$$

with reduction chains $u \to u_1 \to \dots$ and $u \to u_1' \to \dots$ for u, then the diamond pattern occurs with $w_0 = \overline{u}v\,\mu^g$. Similarly, if (1.46) takes the form

$$\begin{array}{ccc} & & uv_1\mu^g \\ & \nearrow & \\ w = uv\mu^g & & \\ & \searrow & \\ & & uv_1'\mu^g \end{array}$$

with reduction chains $v \to v_1 \to \dots$ and $v \to v_1' \to \dots$ for v, the diamond pattern occurs with $w_0 = u\overline{v}\,\mu^g$. Finally, if (1.46) takes the form

$$\begin{array}{ccc} & & u_1v\mu^g \\ & \nearrow & \\ w = uv\mu^g & & \\ & \searrow & \\ & & uv_1\mu^g \end{array} \quad ,$$

then the diamond pattern again occurs, this time as

$$\begin{array}{ccccc} & & u_1v\mu^g & & \\ & \nearrow & & \searrow & \\ w = uv\mu^g & & & & u_1v_1\mu^g\,. \\ & \searrow & & \nearrow & \\ & & uv_1\mu^g & & \end{array}$$

External case: Here, at least one of the initial reductions $w \to w_1$ and $w \to w_1'$ is not internal. If (1.46) takes the form

$$\begin{array}{ccc} & & t \\ & g \nearrow & \\ w = u\,ut\mu^g\,\mu^{\tau g} & & \\ & \searrow & \\ & & u_1\,ut\mu^g\,\mu^{\tau g} \end{array}$$

for some word t in W, then the triangle pattern occurs, as

$$\begin{array}{ccc} & & t \\ & g \nearrow & \uparrow g \\ w = u\,ut\mu^g\,\mu^{\tau g} & & u_1\,u_1t\mu^g\,\mu^{\tau g} \\ & \searrow & \uparrow \\ & & u_1\,ut\mu^g\,\mu^{\tau g} \end{array}$$

Similarly, if (1.46) takes the form

$$\begin{array}{ccc} & & t \\ & g \nearrow & \\ w = u\,ut\mu^g\,\mu^{\tau g} & & \\ & \searrow & \\ & & u\,u_1 t\mu^g\,\mu^{\tau g} \end{array}$$

then the triangle pattern occurs again, as

$$\begin{array}{ccc} & & t \\ & g \nearrow & \uparrow g \\ w = u\,ut\mu^g\,\mu^{\tau g} & & u_1\,u_1 t\mu^g\,\mu^{\tau g} \\ & \searrow & \uparrow \\ & & u\,u_1 t\mu^g\,\mu^{\tau g} \end{array}$$

If (1.46) takes the form

$$\begin{array}{ccc} & & t \\ & g \nearrow & \\ w = u\,ut\mu^g\,\mu^{\tau g} & & \\ & \searrow & \\ & & u\,ut_1\mu^g\,\mu^{\tau g} \end{array}$$

with a reduction $t \to t_1$ for t, then the diamond pattern occurs as

$$\begin{array}{ccccc} & & t & & \\ & g \nearrow & & \searrow & \\ w = u\,ut\mu^g\,\mu^{\tau g} & & & & t_1\,. \\ & \searrow & & \nearrow g & \\ & & u\,ut_1\mu^g\,\mu^{\tau g} & & \end{array}$$

If (1.46) takes the form

$$\begin{array}{ccc} & & s \\ & g \nearrow & \\ st\mu^{\tau\sigma g}\,st\mu^{\tau\sigma g}\,s\mu^g\,\mu^{\tau g} & & \\ \| & & \\ st\mu^{\tau\sigma g}\,s\,st\mu^{\tau\sigma g}\,\mu^{\sigma g}\,\mu^{\tau g} & & \\ & \tau\sigma g \searrow & \\ & & st\mu^{\tau\sigma g}\,t\mu^{\tau g} \end{array}$$

for words s, t in W, then the triangle pattern occurs, as

$$\begin{array}{ccc} & & s \\ & g \nearrow & \\ st\mu^{\tau\sigma g}\, st\mu^{\tau\sigma g}\, s\mu^{g}\, \mu^{\tau g} & & \uparrow\ \sigma\tau\sigma g \\ \| & & \\ st\mu^{\tau\sigma g}\, s\, st\mu^{\tau\sigma g}\, \mu^{\sigma g}\, \mu^{\tau g} & & t\, ts\mu^{\sigma\tau\sigma g}\, \mu^{\sigma\tau g} \\ & \tau\sigma g \searrow & \| \\ & & st\mu^{\tau\sigma g}\, t\mu^{\tau g} \end{array}$$

— note the use of the σ-equivalences denoted by $\|$. Finally, suppose that $x = (x_1, x_2, x_3)$ is an element of the partial Latin square U. If (1.46) takes the form

$$\begin{array}{ccc} & & x_{2g} \\ & g \nearrow & \\ w = x_{1g}\, x_{1g}x_{2g}\mu^{g}\, \mu^{\tau g} & & \\ & x_g \searrow & \\ & & x_{1g}x_{3g}\mu^{\tau g} \end{array}$$

then the triangle pattern occurs, as

$$\begin{array}{ccc} & & x_{2g} \\ & g \nearrow & \uparrow x_{\tau g} \\ w = x_{1g}\, x_{1g}x_{2g}\mu^{g}\, \mu^{\tau g} & & x_{1\tau g}x_{2\tau g}\mu^{\tau g} \\ & x_g \searrow & \| \\ & & x_{1g}x_{3g}\mu^{\tau g} \end{array}$$

(with $\|$ as true equality this time). □

COROLLARY 1.3

Two words u and v of W are related by V if and only if the normal forms $\overline{u}$ and $\overline{v}$ coincide.

PROOF The "if" statement is immediate, since $(u, \overline{u})$ and $(\overline{v}, v)$ both lie in the transitive relation V. Conversely, suppose that u and v are related by V. Then there is a chain

$$u = w_0 \sim w_1 \sim \cdots \sim w_{n-1} \sim w_n = v \tag{1.47}$$

of some finite length n such that successive elements w_i, w_{i+1} of W (for $0 \leq i < n$) are either σ-equivalent, or else related by a reduction $w_i \to w_{i+1}$

or $w_{i+1} \to w_i$. The desired equality of the normal forms will be proved by induction on n. If $n = 1$, then the equality is immediate if u and v are σ-equivalent. Otherwise, suppose without loss of generality that there is a reduction $u \to v$. Suppose that u and v reduce to their normal forms by respective chains

$$u \to u_1 \to \cdots \to \overline{u} \tag{1.48}$$

and

$$v \to v_1 \to \cdots \to \overline{v}$$

Applying the Normal Form Theorem 1.2 to the reduction chains (1.48) and

$$u \to v \to v_1 \to \cdots \to \overline{v}$$

for u then shows that $\overline{u} = \overline{v}$.

Now suppose that the desired equality holds for all pairs u', v' of words connected by chains of length less than n. Consider the chain (1.47). Then $\overline{u} = \overline{w_1}$ and $\overline{w_1} = \overline{v}$ by induction, so $\overline{u} = \overline{v}$ as required. □

The free extension $Q_{(X,U)}$ of (X, U) is now obtained abstractly as the quotient (W_X^V, μ^{S_3}). More concretely, it is realized as the quasigroup

$$\overline{W} = \{\overline{w} \mid w \in W\}$$

of normal forms, with

$$\overline{u}\,\overline{v}\,\mu^g = \overline{\overline{u}\,\overline{v}\,\mu^g}$$

for u, v in W and g in S_3. In particular, the free quasigroup generated by a set X is the free extension $Q_{(X,\varnothing)}$ of the empty partial Latin square $(X, \varnothing)$ on X.

1.10 Exercises

1. Show that the integers are generated up to isomorphism by any nonzero element of the quasigroup $\mathbb{Z}$ under subtraction, whereas no integer generates (an isomorphic copy of) $\mathbb{Z}$ under the associative operation of addition. (In other words, the quasigroup structure of subtraction on the integers is more fundamental, while the addition operation is merely a proper reduct of this structure.)

2. Let P be the set of polynomials $p(X)$ with real coefficients. Given two such polynomials $p(X)$, $q(X)$, define

$$p(X) * q(X) = p(X) + q'(X)\,,$$

the sum of $p(X)$ and the derivative of $q(X)$. Let Q be the set of polynomial sequences $\big(p_0(X), p_1(X), \dots\big)$ such that $p_n(X) = p'_{n+1}(X)$ for $n = 0, 1, \dots$. Define the componentwise product

$$\begin{aligned}\big(p_0(X), p_1(X), \dots\big) * \big(q_0(X), q_1(X), \dots\big)\\ = \big(p_0(X) * q_0(X), p_1(X) * q_1(X), \dots\big)\end{aligned}$$

on Q. Finally, define $f : Q \to P; \big(p_0(X), p_1(X), \dots\big) \mapsto p_0(X)$.

(a) Show that $(Q, *)$ is a combinatorial quasigroup.

(b) Show that $f : (Q, *) \to (P, *)$ is a surjective homomorphism.

(c) Conclude that a homomorphic image of a combinatorial quasigroup need not be a combinatorial quasigroup.

3. Show that a nonempty quasigroup $(Q, \cdot, /, \backslash)$ is a group if and only if it satisfies the identity $x\backslash yz = (x\backslash y)z$.

4. A quasigroup Q is said to be *entropic* if the operation (1.1) is a homomorphism from $Q \times Q$ to Q. Show that Q is entropic if and only if it satisfies the identity

$$xy \cdot zt = xz \cdot yt\,. \tag{1.49}$$

(The name "entropic" means "inner turning," and refers to the switching of the variables y and z between the two sides of (1.49) [53, p.444]. Many other names have been used in the literature, such as "abelian" [119], "surcommutative" [166], "transposition property" [133] and "medial" [168]. Of these, only the latter has retained some currency, although Soublin [166] used it to mean something different.)

5. (a) Show that up to isomorphism, there are just two quasigroups of order 3 that are not commutative.

(b) Show that the two nonisomorphic quasigroups of (a) are obtained as respective conjugates of a group of order 3.

6. The semisymmetrization (1.10) uses the operations from the C_3-orbit $\{//, \backslash\backslash, \cdot\}$ in (1.8). Is it possible to build a semisymmetrization using the operations from the second C_3-orbit $\{/, \backslash, \circ\}$?

7. If the quasigroup $(Q, \cdot, /, \backslash)$ is a group, show that

$$x \cdot y = x/((z/z)/y)\,.$$

8. Show that a nonempty quasigroup is a group if and only if it satisfies the identity

$$(x/y)/(y/z) = x/z\,.$$

9. (a) Prove that a finite, idempotent and commutative quasigroup has odd order.

   (b) Conclude that a finite, unipotent and commutative loop has even order.

10. Show that the quasigroup identities (1.15) of idempotence and (1.20) of total symmetry are equivalent to idempotence (1.15), commutativity, and the right symmetric identity (1.39).

11. For which positive integers n do the constructions of Section 1.6 furnish a Steiner triple system of size n?

12. Exhibit a totally symmetric quasigroup that is neither a loop nor a Steiner triple system.

13. Let e be an element of a totally symmetric quasigroup $(Q, \cdot)$. Show that $x + y = e \cdot xy$ defines a loop $F_e(Q, \cdot) = (Q, +, e)$.

14. [99] Show that a quasigroup Q is a union of three proper nonempty subquasigroups whose common intersection is empty if and only if the idempotent 3-element quasigroup is a quotient of Q.

15. Let $(Q, \cdot, 1)$ be a group in which each nonidentity element has order 3. Define a new multiplication on Q by

$$x \circ y = y^2 x y^2 \, .$$

    Show that $(Q, \circ, 1)$ is a commutative Moufang loop.

16. Give a direct verification of the multiplicativity (1.31) of the norm in a Zorn vector-matrix algebra.

17. Show that the Moufang loop $\mathrm{M}_1(2)$ has 120 elements.

18. Show that the Zorn vector-matrix algebra $\mathsf{Zorn}(\mathsf{F})$ satisfies the third Moufang identity (1.30) as well as the *first* or *left Moufang identity*

$$(zy \cdot z)x = z(y \cdot zx) \tag{1.50}$$

    and the *second* or *right Moufang identity*

$$x(z \cdot yz) = (xz \cdot y)z \, . \tag{1.51}$$

19. (a) Show that the 8-element set

$$\{\pm e_0, \pm e_1, \pm e_2, \pm e_3\}$$

    of signed elements from (1.35) forms a group, the *quaternion group*.

(b) Show that the 16-element set

$$\{\pm e_0, \pm e_1, \ldots, \pm e_7\}$$

of signed elements from (1.35) forms a Moufang loop, the *octonion loop*.

20. Show that a 4-vector $(t, \mathbf{r})$ in Minkowski spacetime (with the speed of light normalized to $c = 1$) may be identified with the element

$$\begin{bmatrix} t & -\mathbf{r} \\ \mathbf{r} & -t \end{bmatrix}$$

of the real Zorn vector-matrix algebra $\mathsf{Zorn}(\mathbb{R})$, so that the norm becomes the Lorentz metric.

21. Pick units with the dielectric constant and permeability normalized to 1. Defining the differential operator matrix

$$D = \begin{bmatrix} -\frac{\partial}{\partial t} & \nabla \\ \nabla & -\frac{\partial}{\partial t} \end{bmatrix}, \tag{1.52}$$

the field matrix

$$F = \begin{bmatrix} 0 & -\mathbf{E} + \mathbf{B} \\ \mathbf{E} + \mathbf{B} & 0 \end{bmatrix},$$

and the 4-current

$$j = \begin{bmatrix} \rho & -\mathbf{j} \\ \mathbf{j} & -\rho \end{bmatrix},$$

show that Maxwell's equations may be written as the single equation

$$DF = J$$

in the real Zorn vector-matrix algebra $\mathsf{Zorn}(\mathbb{R})$.

22. For D as in (1.52) and for

$$\overline{D} = \begin{bmatrix} -\frac{\partial}{\partial t} & -\nabla \\ -\nabla & -\frac{\partial}{\partial t} \end{bmatrix},$$

show that $D\overline{D} = \Delta \cdot I$ with the Laplacian

$$\Delta = \frac{\partial^2}{\partial t^2} - \nabla^2$$

in the real Zorn vector-matrix algebra $\mathsf{Zorn}(\mathbb{R})$.

23. Defining the electromagnetic potential matrix

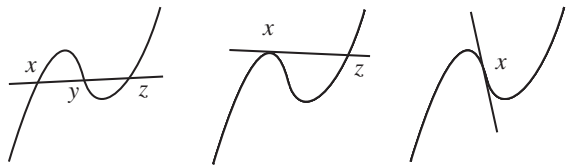
$$P = \begin{bmatrix} \varphi & -\mathbf{A} \\ \mathbf{A} & -\varphi \end{bmatrix},$$

with $F = \overline{D}P$, obtain the *wave equation*

$$\Delta P = J$$

in the real Zorn vector-matrix algebra $\mathsf{Zorn}(\mathbb{R})$. (Hint: apply the diassociativity of Moufang loops.)

24. (a) Manin [111] defines a quasigroup $(Q, \cdot)$ to be *Abelian* if it is totally symmetric, and if for each element e of Q, the loop $F_e(Q, \cdot) = (Q, +, e)$ in Exercise 13 is an abelian group. Let V be an irreducible cubic curve in the complex projective plane $\mathsf{PG}(2, \mathbb{C})$. Let Q be the set of simple points of V. Specify the ternary multiplication table of a quasigroup structure $(Q, \cdot)$ on Q to consist of collinear triples (x, y, z). If two of x, y, z coincide, then the line on which they lie is tangent to V. All three coincide if and only if x is a flex of V. Show that $(Q, \cdot)$ is an Abelian quasigroup [62, Lemma 17.3].



$x \cdot y = z$ $\qquad$ $x \cdot x = z$ $\qquad$ $x \cdot x = x$

(b) [111] A quasigroup $(Q, \cdot)$ is said to be a *CH-quasigroup* or *cubic hypersurface quasigroup* if each set of at most three elements of Q generates an Abelian subquasigroup. Show that a CH-quasigroup is totally symmetric.

(c) [111] Suppose that e is an element of a CH-quasigroup $(Q, \cdot)$. Show that the loop $F_e(Q, \cdot)$ in Exercise 13 is a commutative Moufang loop with identity element e.

(d) [111] If e and f are elements of a CH-quasigroup $(Q, \cdot)$, show that the Moufang loops $F_e(Q, \cdot)$ and $F_f(Q, \cdot)$ are isomorphic.

25. Consider the monoid M in Proposition 1.8. Let Q be a quasigroup. Show that M acts on Q^2 by $(x, y)\alpha = (x, xy\,\alpha)$ for α in M.

26. Let Ω be a set equipped with bijections

$$\sigma : \Omega \to \Omega; \omega \mapsto \sigma\omega \tag{1.53}$$

and

$$\tau : \Omega \to \Omega; \omega \mapsto \tau\omega\,. \tag{1.54}$$

For example, if Ω is a group with elements σ and τ, then $\sigma\omega$ in (1.53) and $\tau\omega$ in (1.54) may just be products in the group Ω. Then a pair (Q, Ω) consisting of a set Q and the set Ω is a *hyperquasigroup* if there is a map

$$Q^2 \times \Omega \to Q : (x, y, \omega) \mapsto xy\,\underline{\omega}$$

such that the hypercommutative law

$$xy\,\underline{\omega} = yx\,\underline{\sigma\omega}$$

and the hypercancellation law

$$x(xy\,\underline{\omega})\,\underline{\tau\omega} = y$$

are satisfied for x, y in Q and ω in Ω. For each ω in Ω, consider the binary operation

$$\underline{\omega} : Q^2 \to Q; (x, y) \to xy\,\underline{\omega}\,.$$

(a) Show that each quasigroup Q forms a hyperquasigroup (Q, S_3) with $\sigma = (12)$ and $\tau = (23)$.

(b) Let Q be a vector space over a field F. Let $\Omega = F \setminus \{0, 1\}$, with

$$\sigma : \Omega \to \Omega; \omega \mapsto 1 - \omega$$

and

$$\tau : \Omega \to \Omega; \omega \mapsto \omega^{-1}\,.$$

For each x, y in Q and ω in Ω, define $xy\,\underline{\omega} = x(1-\omega) + y\omega$. Show that (Q, Ω) is a hyperquasigroup.

(c) If (Q, Ω) is a hyperquasigroup, show that $(Q, \underline{\omega}\,)$ is a combinatorial quasigroup for each ω in Ω.

(d) If (Q, Ω) is a hyperquasigroup, show that $(Q, \underline{\sigma\omega}\,, \underline{\sigma\tau\omega}\,, \underline{\tau\sigma\omega}\,)$ is an equational quasigroup for each ω in Ω.

27. (a) Suppose that (1.37) is satisfied for all h in H and for one element g of S_3. Show that (1.37) is then satisfied for all g in S_3 and all h in H.

(b) Prove the equivalences claimed in Proposition 1.9.

28. Let Q be a quasigroup. Show that the ternary multiplication table $T(Q)$ is the set of idempotent elements of the semisymmetrization $Q\Delta$.

29. Let X be a set of finite size n. If U is a partial Latin square on X, show that $|U| \leq n^2$.

30. Let Q and Q' be free extensions of a partial Latin square (X, U). Show that there is an isomorphism $\theta : Q \to Q'$ restricting to the identity on the subset X of Q and Q'.

31. Let X be a set, and let w be a word in the subalgebra W_X of

$$\left((X + \mu^{S_3})^*, \mu^{S_3}\right)$$

generated by X. Suppose that w includes r letters from μ^{S_3}.

(a) If $r = 0$, show that the σ-equivalence class of w is a singleton.

(b) If $w = uv\mu^g$ for u, v in W_X and g in S_3, suppose that the respective sizes of the σ-equivalence classes of u and v are m and n. Show that the σ-equivalence class of w has $2mn$ elements.

(c) Use induction to show that the σ-equivalence class of w has 2^r elements.

32. For each subgroup H of S_3, define a partial Latin square (X, U) to be *H-symmetric* if

$$(x_1, x_2, x_3) \in U \;\Rightarrow\; (x_{1h}, x_{2h}, x_{3h}) \in U$$

for all h in H.

(a) Show that a quasigroup Q is H-symmetric (as a quasigroup) if and only if its ternary multiplication table $T(Q)$ is H-symmetric (as a partial Latin square).

(b) Derive a Normal Form Theorem for H-symmetric quasigroups by suitable identification of the operations μ^g used in the proof of Theorem 1.2.

33. Define a partial Latin square (X, U) on a set X to be *idempotent* if

$$(x, x, x) \in U$$

for all x in X. For each subgroup H of S_3, derive a Normal Form Theorem for the class of idempotent H-symmetric quasigroups. If a word w from W contains an instance of $uu\mu^g$ for a word u from W, the subword $uu\mu^g$ may be replaced by u. Obtain a new reduction rule $w \to w'$, or more explicitly

$$w \xrightarrow{I_g} w' .$$

Then for the instances

$$\begin{array}{ccc} & u & \\ & I_g \nearrow & \\ w = uu\mu^g & & \\ & \searrow & \\ & u_1 u\mu^g & \end{array} \qquad \text{and} \qquad \begin{array}{ccc} & u & \\ & I_g \nearrow & \\ w = uu\mu^g & & \\ & \searrow & \\ & uu_1\mu^g & \end{array}$$

of (1.46) in the external cases of the proof of the Normal Form Theorem, show that the respective diamond patterns

$$\begin{array}{ccccc} & & & u & \\ & & I_g \nearrow & & \searrow \\ w = uu\mu^g & & & & u_1 \\ & & \searrow & & \uparrow I_g \\ & & & u_1u\mu^g & \to u_1u_1\mu^g \end{array}$$

and

$$\begin{array}{ccccc} & & & u & \\ & & I_g \nearrow & & \searrow \\ w = uu\mu^g & & & & u_1 \\ & & \searrow & & \uparrow I_g \\ & & & uu_1\mu^g & \to u_1u_1\mu^g \end{array}$$

are obtained.

1.11 Notes

Section 1.2

The equational definition of quasigroups is due to T. Evans [55].

Section 1.3

The conjugates of a quasigroup are also known as "derived quasigroups" [86] or "parastrophes" [125, p. 43] [137].

Section 1.4

Semisymmetric quasigroups have also been described as "3-cyclic." They were studied by Osborn [122], Sade [138, 139, 140, 141], Mendelsohn [114, 115], Grätzer and Padmanabhan [66], Mitschke and Werner [117], and DiPaola and Nemeth [42]. Their use for reducing homotopies to homomorphisms first appeared in [156], inspired by work of Gvaramiya and Plotkin that interpreted homotopies as homomorphisms of heterogeneous algebras [72]. The classical approach to studying properties of a quasigroup invariant under isotopy was geometrical, through the concept of a 3-net, as presented by Exercise 10 in Chapter 2 and Exercise 6 in Chapter 3 below [3, p. 74], [13, Ch. XI], [125, Ch. II], [165, Th. I.4.5].

Section 1.5

The construction of a unipotent loop from an idempotent quasigroup goes back to Bruck [19]. For related constructions and further discussion, see [28, Ex. II.7.5].

Section 1.6

Readers unfamiliar with elementary geometric concepts are referred to [62]. The discussion of the "nine point configuration" (the $\mathsf{AG}(2,3)$ of Example 1.2) in [62, §13.2] helps elucidate why Steiner's name is attached to the triple systems. Note that Fig. 17.3 in [62] only shows 10 of the 12 blocks.

Section 1.7

Zorn's vector-matrix algebra was presented in [179]. For more details on the octonions, see [33] and [50]. For a discussion of some physical applications beyond those given in Exercises 20 through 23, see [45].

Section 1.8

It is convenient to call the right action of S_3 on the quasigroup operations (and their opposites) the *semantic action*, describing the left action as the *syntactic action*. The syntactic action is less well known than the semantic action. A general result of Movsisyan [118] implies that the quasigroup operations form a subgroup of the monoid M, but does not address the specific description of the inverses given by Theorem 1.1 in terms of the syntactic action.

The symmetric identities (with a parity depending on the conventions used for mappings) appear in Loos' axiomatization of symmetric spaces [107]. Compare the description of reflections in [134, §4.1].

A more restricted version of the triality symmetry is observed in Moufang loops — see Exercise 21 in Chapter 2, and [33, Ch. 7, 8].

Section 1.9

In its original version, the Normal Form Theorem 1.2 is due to T. Evans [56]. Evans used the language of equational quasigroups (which he had just introduced in [55]). The only symmetry of this theory is the duality between left and right (compare Exercise 8 in Chapter 2). As a result, Evans' proof involved consideration of 15 external cases, as opposed to the 5 that are needed when the full triality symmetry is used.

Evans' Normal Form Theorem was remarkable for being the first example of a so-called *convergent* rewriting system. Later, Knuth and Bendix gave a convergent rewriting system for groups [101]. For more details, see [38].

Chapter 2

MULTIPLICATION GROUPS

This chapter introduces some of the permutation groups on the underlying set of a quasigroup that result from the quasigroup structure. These groups are key tools of quasigroup theory. The most accessible are the combinatorial multiplication groups of Section 2.1, the faithful permutation groups generated by the right and left multiplications. As discussed in Section 2.2, the combinatorial multiplication group construction yields a functorial assignment only to surjective quasigroup homomorphisms. The diagonal action of the combinatorial multiplication group on the direct square of a quasigroup yields the quasigroup congruences as the invariant equivalence relations (Section 2.3). (This diagonal action is the cornerstone of the combinatorial character theory in Chapters 6 and 7.) Section 2.4 considers point stabilizers in the combinatorial multiplication group, and the extent to which they generalize the inner automorphism groups of groups. Section 2.5 examines transversals to the point stabilizers. The concept of a loop transversal, essentially going back to Baer, shows how loops arise as a generalization of quotient groups when one relaxes the requirement of normality on a subgroup of a group. Section 2.6 discusses an application of the loop transversal concept to algebraic coding theory. It provides a nice illustration of the way that quasigroup-theoretical concepts may yield new insights even within the context of abelian groups. In Section 2.7, the universal multiplication group $\mathrm{U}(Q;\mathbf{V})$ of a quasigroup Q in a given variety $\mathbf{V}$ of quasigroups, possibly in the variety $\mathbf{Q}$ of all quasigroups, is introduced as a completely functorial multiplication group construction. The universal multiplication group of Q acts on Q via its quotient, the usual or combinatorial multiplication group of Q that is defined in Section 2.1. The corresponding stabilizers are examined in Section 2.8, ready for their application to the module theory of Chapter 10.

2.1 Combinatorial multiplication groups

Let q be an element of a set $(Q,*)$ equipped with a binary multiplication. The *right multiplication* $R_Q(q)$ or $R_*(q)$ is defined as the map

$$R(q) : Q \to Q; x \mapsto x * q\,. \tag{2.1}$$

The *left multiplication* $L_Q(q)$ or $L_*(q)$ is defined as the map

$$L(q) : Q \to Q; x \mapsto q * x\,. \tag{2.2}$$

If $(Q, *)$ is a quasigroup, then the right and left multiplications are elements of the group $Q!$ of bijections from the set Q to itself. For example, the identity (IR) says that each $R(q)$ injects, while (SL) gives the surjectivity of $L(q)$. The (*combinatorial*) *right multiplication group* of Q is the subgroup $\mathrm{RMlt}\, Q$ of $Q!$ generated by

$$\{R(q) \mid q \in Q\}. \tag{2.3}$$

The (*combinatorial*) *left multiplication group* of Q is the subgroup $\mathrm{LMlt}\, Q$ of $Q!$ generated by

$$\{L(q) \mid q \in Q\}. \tag{2.4}$$

The (*combinatorial*) *multiplication group* of Q is the subgroup G or $\mathrm{Mlt}\, Q$ of $Q!$ generated by

$$\{R(q), L(q) \mid q \in Q\}. \tag{2.5}$$

By (SL) and (SR) respectively, the right and left multiplication groups act transitively on Q; in particular $\mathrm{Mlt}\, Q$ acts transitively on Q. This action has a useful graphical representation: the *Cayley graph* $\mathrm{Cay}\, Q$ of a quasigroup Q is defined to be a labeled directed graph with vertex set Q. For each ordered pair (x, y) of vertices, there are two directed edges, namely

$$R(x \searrow y) := \langle x, R(x\backslash y), y\rangle \quad \text{or} \quad x \xrightarrow{\quad R(x\backslash y) \quad} y \quad \text{or} \quad x \xrightarrow{R} y \tag{2.6}$$

and

$$L(y \swarrow x) := \langle x, L(y/x), y\rangle \quad \text{or} \quad y \xleftarrow{\quad L(y/x) \quad} x \quad \text{or} \quad y \xleftarrow{L} x\,. \tag{2.7}$$

For a fixed quasigroup Q, the edge $R(x \searrow y)$ of (2.6) is called the *right-labeled edge* from x to y, while the edge $L(y \swarrow x)$ of (2.7) is called the *left-labeled edge* from x to y. The *label* of $R(x \searrow y)$ is defined to be $R(x\backslash y)$, while the label of $L(y \swarrow x)$ is defined to be $L(y/x)$.

Example 2.1

Let Q be a group. Cayley's Theorem may be formulated as saying that there are group isomorphisms

$$R : Q \to \mathrm{RMlt}\, Q; q \mapsto R(q)$$

and

$$L : Q \to \mathrm{LMlt}\, Q; q \mapsto L(q^{-1}).$$

Moreover, there is an exact sequence

$$1 \longrightarrow Z(Q) \xrightarrow{\Delta} Q \times Q \xrightarrow{T} \mathrm{Mlt}\, Q \longrightarrow 1$$

of groups with $\Delta : z \mapsto (z, z)$ and $T : (x, y) \mapsto L(x)^{-1}R(y)$. The associative law makes T a group homomorphism. The sequence is exact at $\mathrm{Mlt}\, Q$ since $T(1, x) = R(x)$ and $T(x^{-1}, 1) = L(x)$ for x in Q. If $T(x, y) = L(x)^{-1}R(y) = 1_G$, then $1_Q = 1_Q T(x, y) = 1_Q L(x)^{-1}R(y) = x^{-1}y$, so that $y = x$, and then for any q in Q one has $q = qT(x, x) = x^{-1}qx$. Thus x lies in the center $Z(Q)$ of Q, and the sequence is exact at $Q \times Q$. □

Example 2.2
For a positive integer n, let Q be the cyclic group $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n, considered as a quasigroup under subtraction. Then the set (2.5) is already a subgroup of $Q!$, isomorphic to the dihedral group D_n. In fact this is the simplest specification of the dihedral group D_n, as the multiplication group of the quasigroup of integers modulo n under subtraction. It requires no geometry, split extensions, or presentation by generators and relations. □

For a subquasigroup P of a quasigroup Q, the *relative left multiplication group* of P in Q is the subgroup $\mathrm{LMlt}_Q(P)$ of $\mathrm{Mlt}\, Q$ generated by

$$L_Q(P) = \{L(p) : Q \to Q \mid p \in P\}. \tag{2.8}$$

The *relative right multiplication group* $\mathrm{RMlt}_Q(P)$ is defined similarly. The *relative multiplication group* $\mathrm{Mlt}_Q(P)$ of P in Q is the smallest subgroup of $Q!$ containing the relative left and right multiplication groups of P in Q. Restriction yields a group epimorphism

$$\mathrm{Mlt}_Q(P) \to \mathrm{Mlt}\, P \tag{2.9}$$

from the relative multiplication group of P in Q to the combinatorial multiplication group of P. Note that the combinatorial multiplication groups of P are the respective relative multiplication groups of P in itself.

If Q is a group and P is nonempty, then the set of orbits of $\mathrm{LMlt}_Q P$ on Q is the set

$$P\backslash Q = \{Px \mid x \in Q\} \tag{2.10}$$

of cosets of P. The set of orbits of $\mathrm{Mlt}_Q P$ on Q is the set of double cosets of P in Q.

2.2 Surjections

For a quasigroup $(Q, \cdot, /, \backslash)$, the typical element of the combinatorial multiplication group $\mathrm{Mlt}\, Q$ will be denoted by $E_1(q_1)^{\varepsilon_1} \ldots E_n(q_n)^{\varepsilon_n}$, where $n \in \mathbb{N}$, $\varepsilon_i = \pm 1$, $E_i = R_Q$ or L_Q, and $q_i \in Q$. By convention an element of $\mathrm{Mlt}\, Q$ in this form with $n = 0$ is taken to be the identity element. The generic

element $E_1(q_1)^{\varepsilon_1} \dots E_n(q_n)^{\varepsilon_n}$ will also be denoted by E_Q or $E_Q(q_1, \dots, q_n)$. For q in Q and E_Q in $\operatorname{Mlt} Q$, there is then a quasigroup word w_E such that $qE_Q(q_1, \dots, q_n) = w_E(q, q_1, \dots, q_n)$ or $qq_1 \dots q_n w_E$. The words w_E are defined inductively by $w_1(q) = q$,

$$\begin{aligned}
w_{ER(q_{n+1})}(q, q_1, \dots, q_n, q_{n+1}) &= w_E(q, q_1, \dots, q_n) \cdot q_{n+1}, \\
w_{ER(q_{n+1})^{-1}}(q, q_1, \dots, q_n, q_{n+1}) &= w_E(q, q_1, \dots, q_n)/q_{n+1}, \\
w_{EL(q_{n+1})}(q, q_1, \dots, q_n, q_{n+1}) &= q_{n+1} \cdot w_E(q, q_1, \dots, q_n), \\
w_{EL(q_{n+1})^{-1}}(q, q_1, \dots, q_n, q_{n+1}) &= q_{n+1} \backslash w_E(q, q_1, \dots, q_n).
\end{aligned}$$

If V is a congruence on Q, the natural projection $\operatorname{nat} V$ induces an epimorphism

$$\begin{aligned}
\operatorname{Mlt} \operatorname{nat} V : \operatorname{Mlt} Q &\to \operatorname{Mlt} Q^V; \\
E_Q(q_1, \dots, q_n) &\mapsto E_{Q^V}(q_1^V, \dots, q_n^V).
\end{aligned} \tag{2.11}$$

This epimorphism is well-defined. Indeed, suppose that $E_Q(p_1, \dots, p_m)$ and $F_Q(q_1, \dots, q_n)$ are elements of $\operatorname{Mlt} Q$. Then for each q in Q, one has

$$\begin{aligned}
E_Q(p_1, \dots, p_m) &= F_Q(q_1, \dots, q_n) \\
\Rightarrow qE_Q(p_1, \dots, p_m) &= qF_Q(q_1, \dots, q_n) \\
\Rightarrow w_E(q, p_1, \dots, p_m) &= w_F(q, q_1, \dots, q_n) \\
\Rightarrow w_E(q^V, p_1^V, \dots, p_m^V) &= w_F(q^V, q_1^V, \dots, q_n^V) \\
\Rightarrow E_{Q^V}(p_1^V, \dots, p_m^V) &= F_{Q^V}(q_1^V, \dots, q_n^V).
\end{aligned}$$

Generalizing (2.11) slightly, one obtains a *combinatorial multiplication group functor* Mlt from the category of surjective quasigroup homomorphisms to the category of group epimorphisms, taking a morphism $f : P \to Q$ to

$$\operatorname{Mlt} f : \operatorname{Mlt} P \to \operatorname{Mlt} Q; E_P(p_1, \dots, p_m) \mapsto E_Q(p_1 f, \dots, p_m f). \tag{2.12}$$

Unfortunately, for quasigroup homomorphisms $f : P \to Q$ that are not surjective, the attempt to make Mlt a functor by extending (2.12) fails. Taking $P = \{1\}$ and f the injection $f : 1 \mapsto 1$ of P in the projective space $Q = \mathsf{PG}(1, 2) = \{1, 2, 3\}$, note that $R_P(1)$ is the identity element (indeed the only element) of $\operatorname{Mlt} P$, whereas $R_Q(1f) = R_Q(1) = (23)$ in the symmetric group S_3.

2.3 The diagonal action

Let Q be a quasigroup with combinatorial multiplication group G. Then G has a *diagonal action*

$$G \to (Q \times Q)!; g \mapsto \big((x_1, x_2) \mapsto (x_1 g, x_2 g)\big) \tag{2.13}$$

on $Q \times Q$. The following proposition shows that the congruences on a quasigroup Q are precisely the congruences of the G-set Q.

PROPOSITION 2.1
An equivalence relation V on the quasigroup Q is a congruence on Q if and only if the subset V of $Q \times Q$ is invariant under the diagonal action of G on $Q \times Q$.

PROOF If V is invariant, it must be shown to be a subquasigroup of $Q \times Q$. Suppose $x\,V\,y$ and $z\,V\,t$. Then

$$(xz, yz) \in VR(z) \subseteq V \text{ and } (yz, yt) \in VL(y) \subseteq V,$$

whence $(xz, yt) \in V$ by the transitivity of V. Thus V is closed under multiplication. It follows that V contains

$$((y,x)((z,t)L(y)^{-1}))L(x)^{-1} = (zL(x)^{-1}, tL(y)^{-1}) = (x\backslash z, y\backslash t),$$

i.e. V is closed under left division. Closure under right division follows by symmetry. Thus V is a subquasigroup of $Q \times Q$.

Conversely, suppose V is a congruence on Q. For q in Q and (x, y) in V, one has

$$(x,y)R(q) = (xR(q), yR(q)) = (xq, yq) = (x,y)(q,q) \in V\,.$$

and similarly $(x,y)R(q)^{-1} = (x,y)/(q,q) \in V$, $(x,y)L(q) = (q,q)(x,y) \in V$, $(x,y)L(q)^{-1} = (q,q)\backslash(x,y) \in V$. Thus V is an invariant subset of the G-set $Q \times Q$. ∎

Recall that the action of a group H on a set X is said to be *primitive* if it is transitive, and the only H-congruences on X are the trivial congruence $\widehat{X}$ and the improper congruence X^2.

COROLLARY 2.1
A quasigroup Q is simple if and only if the combinatorial multiplication group G acts primitively on Q.

More generally, each congruence V on a quasigroup Q determines a normal subgroup of $\mathrm{Mlt}\,Q$, namely

$$V^\sharp = \{g \in \mathrm{Mlt}\,Q \mid \forall q \in Q,\ (q, qg) \in V\}. \tag{2.14}$$

Indeed, for each h in $\mathrm{Mlt}\,Q$, and for each g in $V^\sharp$, one has

$$\forall q \in Q,\ (qh^{-1}, qh^{-1}g) \in V = Vh^{-1}$$

by Proposition 2.1. Thus $\forall q \in Q$, $(q, qh^{-1}gh) \in V$, so that $h^{-1}gh \in V^\sharp$. The normal subgroup $V^\sharp$ is the set of elements of $\mathrm{Mlt}\, Q$ whose orbits on Q lie entirely within V-classes. It may also be interpreted as the group kernel of the homomorphism (2.11).

Working in the other direction, consider a normal subgroup N of $\mathrm{Mlt}\, Q$. For elements x and y of Q, note that $xN = yN$ implies $xgN = xNg = yNg = ygN$ for each g of $\mathrm{Mlt}\, Q$. Thus the kernel $N^\flat$ of the projection $x \mapsto xN$ from Q to the set Q/N of orbits of N on Q is a congruence on Q by Proposition 2.1. In other words, the orbit set Q/N carries a quasigroup structure with $xN \cdot yN = (xy)N$ for x, y in Q. Finally, it is worth remarking that $N \mapsto N^{\flat\sharp}$ is a closure operator on the set of normal subgroups of the combinatorial multiplication group $\mathrm{Mlt}\, Q$ of the quasigroup Q.

2.4 Inner multiplication groups of piques

For an element e of a (nonempty) quasigroup Q with combinatorial multiplication group G, let G_e denote the stabilizer $\{g \in G \mid eg = e\}$ of e in G. Note that for each element g of G, the stabilizer G_{eg} is the conjugate $G_e^g = g^{-1}G_e g$ of G_e by g. Since the permutation group G is transitive, the stabilizers of elements of Q are all conjugate to each other. If Q is a group with identity element e, then

$$G_e = \{T(x, x) \mid x \in Q\} \tag{2.15}$$

in the notation of Example 2.1. Thus G_e in this case is the inner automorphism group $\mathrm{Inn}\, Q$ of Q. If Q is a pique with pointed idempotent e, the stabilizer G_e of the pointed idempotent is called the *inner multiplication group* (or *inner mapping group*) $\mathrm{Inn}\, Q$ of Q. As the following example shows, $\mathrm{Inn}\, Q$ need not consist entirely of automorphisms of Q, even if e is the identity element of a loop Q.

Example 2.3

Consider the loop $(Q', +, 0)$ of Figure 1.3. It has $R(1) = (01)(243)$, $R(2) = (02)(134)$, and $R(3) = (03)(142)$, whence $R(1)R(2)R(3) = (24) \in \mathrm{Inn}\, Q$. Then $1(24) + 2(24) = 1 + 4 = 2 \neq 3 = 3(24) = (1 + 2)(24)$, so that (24) is not an automorphism of Q. □

If the inner multiplication group $\mathrm{Inn}\, Q$ of a loop Q does consist entirely of automorphisms, then Q is described as an A-*loop*. Despite the phenomenon of Example 2.3, it is often convenient to think of the stabilizer G_e of an element e of a quasigroup Q as a generalization of the concept of the inner automorphism group of a group.

For a pique $(Q, \cdot, /, \backslash, e)$ with pointed idempotent e, it is conventional to set $R = R(e)$ and $L = L(e)$. Note that R and L lie in $\operatorname{Inn} Q$. The *cloop* or *corresponding loop* of the pique Q is the loop $B(Q)$ or $(Q, +, -, \leftthreetimes, e)$ with

$$\begin{cases} x + y = x^{R^{-1}} \cdot y^{L^{-1}}; \\ x - y = (x/y^{L^{-1}})^R; \\ x \leftthreetimes y = (x^{R^{-1}} \backslash y)^L. \end{cases} \tag{2.16}$$

Inverting (2.16), the pique Q is recovered from its cloop $B(Q)$ by

$$\begin{cases} x \cdot y = x^R + y^L; \\ x/y = (x - y^L)^{R^{-1}}; \\ x \backslash y = (x^R \leftthreetimes y)^{L^{-1}}. \end{cases} \tag{2.17}$$

The first equations of (2.16) and (2.17) exhibit principal isotopies between the pique and its cloop. For an element x of Q, (2.17) yields

$$\begin{cases} L(x) = LL_+(xR); \\ R(y) = RR_+(yL), \end{cases} \tag{2.18}$$

while (2.16) yields

$$\begin{cases} L_+(x) = L^{-1}L(xR^{-1}); \\ R_+(y) = R^{-1}R(yL^{-1}). \end{cases} \tag{2.19}$$

Thus the multiplication group of the cloop is a subgroup of the multiplication group of the pique. Indeed

$$\operatorname{Mlt} Q = \big\langle \operatorname{Mlt} B(Q), R, L \big\rangle. \tag{2.20}$$

by (2.18).

2.5 Loop transversals and right quasigroups

Let e be an element of a (nonempty) quasigroup Q with combinatorial multiplication group G. The main aim of this section is to introduce certain transversals to the stabilizer G_e of e in G. Recall that a (*right*) *transversal* T to a subgroup H of a group G is a full set of unique representatives for the set $\{Hx \mid x \in G\}$ of right cosets of H. In other words, there are surjections $\delta : G \to H$ and $\varepsilon : G \to T$ such that

$$G \to H \times T; g \mapsto (g^\delta, g^\epsilon) \tag{2.21}$$

is a two-sided inverse to the product map

$$H \times T \to G; (h,t) \mapsto ht. \tag{2.22}$$

In particular,

$$g = g^{\delta} g^{\varepsilon} \tag{2.23}$$

for each element g of G. The transversal T is said to be *normalized* if $1^{\varepsilon} = 1$.

On each transversal T, a binary multiplication $*$ and right division $\|$ are defined by

$$t * u = (tu)^{\varepsilon} \text{ and } t\|u = (tu^{-1})^{\varepsilon}. \tag{2.24}$$

Now a *right quasigroup* Q is defined to be an algebra $(Q, \cdot, /)$ with a binary multiplication $\cdot$ and right division $/$ such that the identities (IR) and (SR) are satisfied. A right quasigroup Q is said to be a *right loop* $(Q, \cdot, /, e)$ if it contains a two-sided identity element e. The structures of *left quasigroup* $(Q, \cdot, \backslash)$ and *left loop* $(Q, \cdot, \backslash, e)$ are defined dually.

PROPOSITION 2.2

Let T be a transversal to a subgroup H of a group G. Then $(T, *, \|)$ is a right quasigroup. Moreover, if T is normalized, then $(T, *, \|, 1)$ is a right loop.

PROOF For elements t and u of T, the equation (IR) written in the form $(t * u)\|u = t$ follows from

$$H((t * u)\|u) = H(t * u)u^{-1} \ni (tu)u^{-1} = t \in Ht$$

and the disjointness of distinct cosets of a subgroup of a group. In similar fashion, (SR) in the form $(t\|u) * u = t$ follows from

$$H((t\|u) * u) = H(t\|u)u \ni (tu^{-1})u = t \in Ht\,.$$

Finally, if T is normalized, one has the containments $H(1 * t) \ni 1t = t \in Ht$ and $H(t * 1) \ni t1 = t \in Ht$ showing that T forms a right loop. □

To within isomorphism, each right loop is obtained by the construction of Proposition 2.2. To obtain a suitable group G, note that for any right quasigroup Q, one may define right multiplications as in Section 2.1. The identities (IR) and (SR) again confirm that these right multiplications biject. Define the *right multiplication group* as in Section 2.1. This is a group G of permutations on Q. For left quasigroups, an analogous *left multiplication group* is defined.

PROPOSITION 2.3

Let $(Q, \cdot, /, e)$ be a right loop. Then there is a transversal T to a subgroup H of a group G such that $(Q, \cdot, /, e)$ is isomorphic to $(T, *, \|, 1)$.

PROOF The right multiplication group G of Q acts transitively, since the orbit of e covers Q. Let H be the stabilizer of e in G. Then $T = \{R(x) \mid x \in Q\}$ is a normalized transversal to H in G. Finally, $R : Q \to T$ is the desired isomorphism. Note that $R(x) = R(y) \Rightarrow x = eR(x) = eR(y) = y$. □

DEFINITION 2.1 *A normalized transversal T to a subgroup H of a group G is said to be a* loop transversal *if the right loop $(T, *, \|, 1)$ of Proposition 2.2 is a (two-sided) loop, or in other words, if for each ordered pair (t, u) of elements of T, the equation*

$$t * x = u \tag{2.25}$$

has a unique solution x in T.

PROPOSITION 2.4
Let T be a normalized transversal to a normal subgroup N of a group G. Then:

(a) *the transversal T is a loop transversal, and*

(b) *the loop $(T, *, 1)$ is isomorphic to the quotient group G/N.*

PROOF The set bijection $T \to G/N; t \mapsto Nt$ becomes a right loop isomorphism, since for t, u in T, one has $N(t * u) = Ntu = NtNu$. □

PROPOSITION 2.5
Let T be a normalized transversal to a subgroup H of a group G. Then T is a loop transversal if and only if it is a transversal to each conjugate H^g of H in G.

PROOF Suppose first that T is a loop transversal. Note that

$$H^g = g^{-1}Hg = (g^\delta g^\varepsilon)^{-1} H g^\delta g^\varepsilon = H^{g\varepsilon}.$$

Then for x in T and a in G,

$$\begin{aligned} a \in H^g x &\Leftrightarrow a \in H^{g\varepsilon} x \Leftrightarrow g^\varepsilon \cdot a \in H g^\varepsilon \cdot x \\ &\Leftrightarrow (g^\varepsilon \cdot a)\varepsilon = (g^\varepsilon \cdot x)\varepsilon \Leftrightarrow g^\varepsilon * x = (g^\varepsilon \cdot a)\varepsilon. \end{aligned}$$

Since $(T, *, 1)$ is a loop, there is a unique solution x to the latter equation. Thus x exists as a unique solution to the first containment, making T a transversal to the conjugate subgroup H^g.

Conversely, suppose that T is a transversal to each conjugate of H in G. For each ordered pair (t, u) of elements of T, it must be shown that (2.25) has

a unique solution x. But

$$t * x = u \Leftrightarrow (tx)\varepsilon = u \Leftrightarrow Hu = H(tx)^{\varepsilon} = Htx$$
$$\Leftrightarrow u \in Htx \Leftrightarrow t^{-1}u \in H^t x.$$

Since T is a transversal to H^t, there is a unique x in T for which $t^{-1}u \in H^t x$, and thus for which $t * x = u$. □

Given a quasigroup Q with multiplication group G, define a mapping

$$\rho : Q \times Q \to G; (x, y) \mapsto R(x\backslash x)^{-1} R(x\backslash y). \tag{2.26}$$

PROPOSITION 2.6
The mapping $\rho : Q \times Q \to G$ has the following properties:

(P1) *For each x in Q, $\rho(x, x) = 1$;*

(P2) *For x, y in Q, $x\rho(x, y) = y$;*

(P3) *For x, y in Q, $x = y \Leftrightarrow \rho(x, y) = 1$;*

(P4) *The derived quasigroup operation*

$$P : Q^3 \to Q; (x, y, z) \mapsto x\rho(y, z) \tag{2.27}$$

satisfies the identities

$$(x, x, z)P = z \quad \text{and} \quad (x, y, y)P = x\,; \tag{2.28}$$

(P5) *For each e in Q, the set*

$$T = \{\rho(e, x) \mid x \in Q\} \tag{2.29}$$

is a normalized loop transversal to the stabilizer G_e of e in G;

(P6) *For each e in Q, $N_G(G_e) = \bigcup\{G_e\rho(e, x) \mid xG_e = \{x\}\}$;*

(P7) *For e, x in Q, one has $xG_e = \{x\} \Leftrightarrow \rho(e, x) \in Z(G)$.*

PROOF Most of these properties follow directly. For (P5), first note that

$$\varepsilon : G \to T; g \mapsto \rho(e, eg)$$

establishes T as a normalized transversal to G_e in G. Then for x, y in Q, one has

$$\begin{aligned}\rho(e, x) * \rho(e, y) &= (\rho(e, x)\rho(e, y))^{\varepsilon} \\ &= \rho(e, e\rho(e, x)\rho(e, y)) \\ &= \rho(e, x\rho(e, y)) = \rho(e, (x, e, y)P).\end{aligned}$$

Thus $\rho(e,x) \mapsto x$ gives a right loop isomorphism from $(T,*)$ to Q equipped with the multiplication

$$x +_e y = (x,e,y)P = xR(e\backslash e)^{-1} \cdot yL(e)^{-1}. \tag{2.30}$$

By (2.30), it is apparent that $(R(e\backslash e)^{-1}, L(e)^{-1}, 1_Q)$ is a principal isotopy from $(Q,+_e)$ to $(Q,\cdot)$. Thus the isomorphic right loops $(Q,+_e)$ and $(T,*)$ are actually loops, and T becomes a loop transversal.

For (P6), let $\{\rho(e,x) \mid x \in S\}$ be the subtransversal of T to G_e in $N_G(G_e)$. Then

$$x \in S \Leftrightarrow e\rho(e,x)G_e = \{e\rho(e,x)\} \Leftrightarrow xG_e = \{x\}.$$

For (P7), suppose that $\rho(e,x)$ lies in $Z(G)$. Let g stabilize e. Then

$$xg = e\rho(e,x)g = eg\rho(e,x) = x.$$

Conversely, suppose $xG_e = \{x\}$. Let $y \in Q$ and $g \in G$. Now

$$eL(e)^{-1}L(y/(e\backslash e))g = yg = eL(e)^{-1}L((yg)/(e\backslash e)),$$

implying that $xL(e)^{-1}L(y/(e\backslash e))g = xL(e)^{-1}L((yg)/(e\backslash e))$. In other terms, $yR(e\backslash e)^{-1}R(e\backslash x)g = ygR(e\backslash e)^{-1}R(e\backslash x)$. Thus $y\rho(e,x)g = yg\rho(e,x)$, whence $\rho(e,x) \in Z(G)$. □

COROLLARY 2.2

Let $(Q,\cdot)$ be a quasigroup with an element e. Then $(Q,\cdot)$ is isotopic to a loop $(Q,+_e,e)$ with identity element e, and with multiplication given by (2.30).

COROLLARY 2.3

Let $(Q,\cdot,e)$ be a pique with pointed idempotent element e. Then the loop $(Q,+_e,e)$ is the cloop of $(Q,\cdot,e)$.

PROOF If e is idempotent, then (2.30) reduces to

$$x +_e y = (x,e,y)P = xR(e)^{-1} \cdot yL(e)^{-1},$$

coinciding with the first equation of (2.16). □

COROLLARY 2.4

In the multiplication group G of a quasigroup Q with element e, one has $N_G(G_e) = G_e \cdot Z(G)$.

PROOF The properties P(6) and P(7) yield

$$G_e \cdot Z(G) \leq N_G(G_e) = \bigcup\{G_e\rho(e,x) \mid xG_e = \{x\}\} \leq G_e \cdot Z(G).$$

□

2.6 Loop transversal codes

The concept of a loop transversal offers a quick and elementary introduction to the subject of algebraic coding theory. Algebraic coding theory addresses certain aspects of the problem of transmitting information through channels that are subject to interference. The effect of the interference is to corrupt the signals being transmitted. Nevertheless, algebraic coding theory offers methods of encoding the original information into a signal for transmission, in such a way that the original information may be recovered from a corrupt received signal, or at least so that a signal may be recognized as being corrupt. The information transmission may be taking place through space, sending a message from one physical location to another. On the other hand, it may also be taking place through time, recording a message (data) in a memory, and then reading it back later.

The usual scheme of algebraic coding theory may be summarized as follows. A finite set A is given, known as the *alphabet*. The elements of the alphabet A are often described as the *letters* of the alphabet A. Typically, one uses the *binary alphabet* $\{0,1\}$ consisting of the two binary digits $0,1$ or integers modulo 2. The information to be transmitted is assembled from words of fixed length k, i.e. concatenations of k (not necessarily distinct) letters of the alphabet. This set of words to be encoded is described as the *uniform code* A^k. The information channel carries words from the uniform code A^n, for some $n \geq k$. The integer n is known as the *length* of the channel. A subset C of A^n is chosen. This subset C is known as the *code* (or a *block code* to avoid confusion with the concept of a uniform code). The *encoding* is an embedding $A^k \to A^n$ with image C, restricting to a bijection $\eta : A^k \to C$. Thus $|C| = |A|^k$. The integer k is known as the *dimension* of the code. If a word c from the code C is transmitted through the channel without corruption, then it is received as the same word c. The original encoded word from A^k may then be recovered as $c\eta^{-1}$. However, the emitted codeword c may have been subject to interference in the channel, being received as a corrupted word x in A^n. A *decoding* map

$$\delta : A^n \to C \tag{2.31}$$

assigns a codeword x^δ to the received word x. Provided that the received word x was not corrupted excessively from the emitted codeword c, one should expect that $x^\delta = c$. In particular, one should have $c^\delta = c$ for c in C.

Example 2.4 Repetition codes

Let $A = \{0,1\}$ and $k = 1$. Consider a channel length of 3. Define $0\eta = 000$ and $1\eta = 111$. Thus $C = \{000, 111\}$. Define the decoding (2.31) by $\delta^{-1}\{000\} = \{000, 001, 010, 100\}$ and $\delta^{-1}\{111\} = \{111, 110, 101, 011\}$ ("majority vote"). Provided that at most one letter of the emitted codeword gets

corrupted in the channel, the decoder is able to recover the codeword. One may extend this scheme to channels of greater odd length. □

For further analysis, it is convenient to put an abelian group structure $(A, +, 0)$ on the alphabet A. Usually, for $|A| = l$, one takes A to be the cyclic group $(\mathbb{Z}/l\mathbb{Z}, +, 0)$ of residues modulo l. The channel A^n is the n-th direct power of A, with componentwise operations. Thus the channel A^n becomes the abelian group $(A^n, +, 0)$, or more pedantically $(A^n, +, 00\ldots0)$. This abelian group structure may be used to describe the interference taking place in the channel. If an emitted codeword c is received as the corrupted word x, one says that the *error* $x - c$ was added to c during passage through the channel. The decoder $\delta : x \mapsto c$ is then said to *correct* the error $x - c$. To measure the seriousness of the error, one may define the *Hamming weight* $|x|$ of a channel word x in A^n to be the number of nonzero letters in x. The *Hamming distance* between two words x, y is then $|x - y|$. Note that the triangle inequality

$$|x + y| \leq |x| + |y| \tag{2.32}$$

is satisfied. Indeed, $|x + y| > |x| + |y|$ is impossible, since $x + y$ can only have a nonzero letter in a certain slot if at least one of x and y has a nonzero letter in that slot. Moreover, $|x| = 0 \Leftrightarrow x = 0$.

The decoding may be analyzed using the abelian group structure. An *error map*

$$\varepsilon : A^n \to A^n \tag{2.33}$$

determines that a received word x was the result of an error x^ε. Thus

$$x = x^\delta + x^\varepsilon \tag{2.34}$$

for each x in A^n. The key idea behind loop transversal codes is the observation that (2.34) may just be an instance of (2.23). Thus the code C is defined to be *linear* if it is a subgroup of the channel A^n. Since A^n is abelian, such a subgroup C is normal. As in Proposition 2.4, any normalized right transversal T to C in A^n is then a loop transversal. Taking the error map ε as in (2.21), one obtains the loop transversal T as the set of errors corrected by the code. Note that the loop $(T, *, 0)$ defined by (2.24) is an abelian group, since the map

$$T \to A^n/C; t \mapsto C + t$$

of Proposition 2.4 is a right loop isomorphism of T with the abelian group A^n/C. Nevertheless, it is often convenient to continue to refer to the operation $*$ as a loop multiplication, in order to distinguish it from the abelian group operation $+$ on A^n.

Example 2.5

Consider the length 3 binary repetition code C of Example 2.4. Interpret A as $\mathbb{Z}/2\mathbb{Z}$. Then C becomes linear, and the normalized right transversal

$T = \{000, 001, 010, 100\}$ is the set of errors corrected by C. The abelian group multiplication $*$ on T given by (2.24) has the table

$*$	000	001	010	100
000	000	001	010	100
001	001	000	100	010
010	010	100	000	001
100	100	010	001	000

Note that the table may be summarized by the specification that the map

$$s : (T, *) \to (A^2, +); 001 \mapsto 01, 010 \mapsto 10, 100 \mapsto 11$$

is an abelian group homomorphism. □

If one knows a linear code C in a channel A^n, one may determine a loop transversal T to C by selecting representatives of the various cosets of C. Typically, one picks *coset leaders* — representatives having minimal Hamming weight within their cosets. On the other hand, one of the major problems of algebraic coding theory is to determine a suitable code C to begin with, for a given channel A^n. If the loop $(T, *, 0)$ is known, then the code C may be obtained from T by the so-called *Principle of Local Duality*. To formulate this principle, it is convenient to establish some notation. For elements $t_1, t_2, \ldots$ of T, define $\sum_{i=1}^{m} t_i$ inductively by $\sum_{i=1}^{0} t_i = 0$ and $\sum_{i=1}^{m} t_i = t_m + \sum_{i=1}^{m-1} t_i$. Define $\prod_{i=1}^{m} t_i$ inductively by $\prod_{i=1}^{0} t_i = 0$ and $\prod_{i=1}^{m} t_i = t_m * \prod_{i=1}^{m-1} t_i$. In compound expressions involving loop operations $*$, $\|$ and abelian group operations $+, -$, the loop operations will bind more strongly than the group operations. For example, $t + u - t * u = t + u - (t * u)$.

PROPOSITION 2.7 (Principle of Local Duality)
Let T be a loop transversal to a linear code C in a channel A^n, over a finite abelian group alphabet A. Suppose that T is a set of generators for A^n. Then $C = \{\sum_{i=1}^{m} t_i - \prod_{i=1}^{m} t_i \,\big|\, t_1, \ldots, t_m \in T\}$.

PROOF Recall that $t^{\varepsilon} = t$ for t in T. Induction on m using (2.24) then shows that $(\sum_{i=1}^{m} t_i)\varepsilon = \prod_{i=1}^{m} t_i$ for $t_1, \ldots, t_m$ in T. Since T generates A^n and A is finite, each channel word x may be written in the form $x = \sum_{i=1}^{m} t_i$ for some multisubset $\langle t_1, \ldots, t_m \rangle$ of T. Then

$$\begin{aligned} C &= \{x^{\delta} \,\big|\, x \in A^n\} \\ &= \{x - x^{\varepsilon} \,\big|\, x \in A^n\} \\ &= \left\{ \sum_{i=1}^{m} t_i - \prod_{i=1}^{m} t_i \,\middle|\, t_1, \ldots, t_m \in T \right\}. \end{aligned}$$

□

The full force of the Principle of Local Duality comes into play when it is not even known in advance that there is some code C to which a loop $(T, *, 0)$ in A^n is transversal. For simplicity, the case $A = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ will be discussed here. Given a channel A^n, one normally has a list of the errors one would like to correct (e.g., the most common errors), and this list usually includes the n-element set B of errors of Hamming weight 1. Let T be a 2^{n-k}-element set of errors to be corrected, with $T \supseteq \{0\} \cup B$. Suppose that T carries a loop structure $(T, *, 0)$ given by an isomorphism

$$s : (T, *, 0) \to (A^{n-k}, +, 0) \tag{2.35}$$

(e.g., as in Example 2.5). Let $t_1, \ldots, t_m$ be elements of T. By the closure of $(T, *)$, the loop product $\prod_{i=1}^m t_i$ always lies in T. On the other hand, the sum $\sum_{i=1}^m t_i$ may only lie in T for certain choices of $t_1, \ldots, t_m$. The isomorphism (2.35) is said to be a *partial homomorphism* $s : (T, +) \to (A^{n-k}, +)$ if $(\sum_{i=1}^m t_i)s = \sum_{i=1}^m t_i^s$ whenever $\sum_{i=1}^m t_i \in T$. Of course, this means that $\sum_{i=1}^m t_i = \prod_{i=1}^m t_i$ in such cases, since the two sides of the equation have the same image under the isomorphism (2.35).

THEOREM 2.1

Let T be a 2^{n-k}-element subset of the length n binary channel A^n, such that T contains 0 and the n-element set B of errors of Hamming weight 1. Suppose that T carries a loop structure $(T, *, 0)$ given by an isomorphism (2.35) *such that $s : (T, +) \to (A^{n-k}, +)$ is a partial homomorphism. Then there is a linear code C of dimension k in A^n to which $(T, *, 0)$ is a loop transversal. Moreover, T is precisely the set of errors corrected by C.*

PROOF Note that each element x of A^n has a unique expression $x = \sum\{b_i \mid i \in X\}$ for a subset X of B. Define the *syndrome*

$$s : A^n \to A^{n-k}; \sum_{i \in X} b_i \mapsto \sum_{i \in X} b_i^s. \tag{2.36}$$

Since (2.35) is a partial homomorphism, it is the restriction of the syndrome to T. Now for x, y in A^n, with $x = \sum_{i \in X} b_i$ and $y = \sum_{i \in Y} b_i$, one has

$$x^s + y^s = \sum_{i \in X} b_i^s + \sum_{i \in Y} b_i^s = \sum\{b_i^s \mid i \in (X \cup Y) - (X \cap Y)\} = (x + y)s.$$

Thus the syndrome is an abelian group homomorphism. Let $C = \operatorname{Ker} s$ be its group kernel $s^{-1}\{0\}$. Note that $|C| = |A|^k$. For $x = \sum_{i \in X} b_i$ in A, define $x^\delta = \sum_{i \in X} b_i - \prod_{i \in X} b_i$ and $x^\varepsilon = \prod_{i \in X} b_i$. Then $x^\delta \in C$ and $x^\varepsilon \in T$, with $x = x^\delta + x^\varepsilon$. Thus $A^n = C + T$. But $|A^n| = |C|.|T|$, so T is a loop transversal to C in A^n. Moreover, $\delta : A^n \to C; x \mapsto x^\delta$ and $\varepsilon : A^n \to T; x \mapsto x^\varepsilon$ surject, indeed $\varepsilon|_T = 1_T$, so T is precisely the set of errors corrected by C. □

Example 2.6 (A code for hexadecimal digits.)

For the alphabet $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, consider the set $(\mathbb{Z}/2\mathbb{Z})^4 = \{0 = 0000, 1 = 0001, 2 = 0010, \ldots, 9 = 1001, A = 1010, B = 1011, \ldots, F = 1111\}$ of hexadecimal digits. This set is to be encoded for transmission through a binary channel of length 7 in such a way that errors of single Hamming weight may be corrected. Let b_i, for $1 \leq i \leq 7$, denote the binary word of length 7 and Hamming weight 1 with its unique nonzero letter in the i-th slot. Thus $b_1 = 1000000, \ldots, b_3 = 0010000$, etc. Set $B = \{b_i \mid 1 \leq i \leq 7\}$ and $T = \{0000000\} \cup B$. Define $s : T \to (\mathbb{Z}/2\mathbb{Z})^3 = (\mathbb{Z}/2\mathbb{Z})^{7-4}$ as a partial homomorphism by sending b_i to the binary representation of i, e.g. $b_3^s = 011$. This sets up an isomorphism (2.35), e.g. $b_1 * b_3 = (b_1^s + b_3^s)s^{-1} = (001 + 011)s^{-1} = 010s^{-1} = b_2$. By Theorem 2.1, the loop transversal $(T, *, 1)$ then determines a code C of dimension 4. The 2^4 hexadecimal digits may be encoded by bijection with C. The elements of C may be determined by the Principle of Local Duality. For example, $b_1 + b_3 - b_1 * b_3 = 1000000 + 0010000 - 0100000 = 1110000 \in C$. □

2.7 Universal multiplication groups

In Section 2.2, the construction of the combinatorial multiplication group of a quasigroup Q led to the combinatorial multiplication group functor Mlt from the category of surjective quasigroup homomorphisms to the category of groups. The functor Mlt did not extend, however, to a functor defined on general quasigroup homomorphisms. Now let $\mathbf{V}$ denote a variety of quasigroups, i.e. the class of all quasigroups satisfying a given set of identities. Examples are given by the variety $\mathbf{Q}$ of all quasigroups, and the variety $\mathbf{STS}$ of Steiner triple systems, quasigroups satisfying the identities (1.15) and (1.20). Such a variety may also be considered as a category, with the class of quasigroups from the variety as the class of objects, and with all quasigroup homomorphisms between members of the variety admitted as morphisms. The aim of this section is to exhibit a multiplication group construction which does provide a functor from the full category $\mathbf{V}$ to the category $\mathbf{Gp}$ of groups.

Let Q be a quasigroup in the given variety $\mathbf{V}$ of quasigroups. The category $\mathbf{V}$ is bicomplete, and thus possesses all limits and colimits [165, Ch. IV, Th. 2.2.3]. In particular, coproducts exist there. Let $Q[X]$ be the coproduct of Q with the free quasigroup in $\mathbf{V}$ on the singleton set $\{X\}$. This $\mathbf{V}$-quasigroup contains X, and comes equipped with a homomorphism $\iota : Q \to Q[X]$. It is specified to within isomorphism by the universality property that for each homomorphism $f : Q \to P$ to a quasigroup P in $\mathbf{V}$, and for each element p of P, there is a unique homomorphism $f_p : Q[X] \to P$ such that $f_p : X \mapsto p$ and $\iota f_p = f$.

LEMMA 2.1
The homomorphism $\iota : Q \to Q[X]$ injects.

PROOF If Q is empty, the result is immediate. If Q is nonempty, take $f = 1_Q : Q \to Q$, and pick some element q of Q to be the image of X under f_q. Then $\iota f_q = 1_Q$, so that f_q retracts ι. □

On the strength of Lemma 2.1, one identifies Q with its image in the coproduct under the insertion. The element X may be considered as an indeterminate, and the properties of the quasigroup $Q[X]$ in the variety $\mathbf{V}$ are analogous to those of the polynomial ring $S[X]$ over a commutative ring S in the variety of commutative rings.

DEFINITION 2.2 *Let Q be a member of a variety $\mathbf{V}$ of quasigroups. Then the* universal multiplication group $\widetilde{G}$ *or* $\mathrm{U}(Q;\mathbf{V})$ *of Q in $\mathbf{V}$ is the relative multiplication group of Q in $Q[X]$.*

It is convenient to set $R_{Q[X]}(q) = \widetilde{R}(q)$ and $L_{Q[X]}(q) = \widetilde{L}(q)$ for each element q of Q (although often the tildes are omitted). Note that (2.9) provides a group epimorphism

$$\widetilde{G} \to G \quad \text{or} \quad \mathrm{U}(Q;\mathbf{V}) \to \mathrm{Mlt}\, Q \tag{2.37}$$

between the universal and the combinatorial multiplication groups of Q. In this way $\widetilde{G}$ acts as a group of permutations on Q. The universal multiplication group construction is functorial.

PROPOSITION 2.8
For a $\mathbf{V}$-morphism $f : Q \to Q'$, there is a group homomorphism

$$\mathrm{U}(f;\mathbf{V}) : \mathrm{U}(Q;\mathbf{V}) \to \mathrm{U}(Q';\mathbf{V}) \tag{2.38}$$

extending the assignments $\widetilde{R}(q) \mapsto \widetilde{R}(qf)$ and $\widetilde{L}(q) \mapsto \widetilde{L}(qf)$ for q in Q. Then (2.38) *becomes the morphism part of a functor* $\mathrm{U}(\ \ ;\mathbf{V})$ *from $\mathbf{V}$ to the category* **Gp** *of groups.*

PROOF In the notation of Section 2.2, the map (2.38) is a group homomorphism well-defined by

$$\mathrm{U}(f;\mathbf{V}) : E_{\widetilde{Q}}(p_1, \ldots, p_m) \mapsto E_{\widetilde{Q'}}(p_1 f, \ldots, p_m f).$$

Indeed,

$$\begin{aligned}
&E_{\widetilde{Q}}(p_1,\dots,p_m) = F_{\widetilde{Q}}(q_1,\dots,q_n)\\
&\quad\Rightarrow w_E(X,p_1,\dots,p_m) = w_F(X,q_1,\dots,q_n)\\
&\quad\Rightarrow \forall y\in\widetilde{Q'},\ w_E(X,p_1,\dots,p_m)f_y = w_F(X,q_1,\dots,q_n)f_y\\
&\quad\Rightarrow \forall y\in\widetilde{Q'},\ w_E(y,p_1f,\dots,p_mf) = w_F(y,q_1f,\dots,q_nf)\\
&\quad\Rightarrow \forall y\in\widetilde{Q'},\ yE_{\widetilde{Q}}(p_1f,\dots,p_mf) = yF_{\widetilde{Q}}(q_1f,\dots,q_nf)\\
&\quad\Rightarrow E_{\widetilde{Q'}}(p_1f,\dots,p_mf) = F_{\widetilde{Q'}}(q_1f,\dots,q_nf).
\end{aligned}$$

For a further $\mathbf{V}$-morphism $g : Q' \to Q''$, one has

$$\mathrm{U}(fg;\mathbf{V}) = \mathrm{U}(f;\mathbf{V})\mathrm{U}(g;\mathbf{V}).$$

Thus $\mathrm{U}(\ \ ;\mathbf{V})$ is a functor from $\mathbf{V}$ to the category $\mathbf{Gp}$ of groups. □

COROLLARY 2.5

Let Q be a subquasigroup of a quasigroup Q' in a variety $\mathbf{V}$. Let $\widetilde{G}$ be the universal multiplication group of Q in $\mathbf{V}$. Then there is a group epimorphism

$$\widetilde{G} \to \mathrm{Mlt}_{Q'}Q;\ \widetilde{R}(q) \mapsto R_{Q'}(q),\ \widetilde{L}(q) \mapsto L_{Q'}(q) \tag{2.39}$$

from the universal multiplication group $\widetilde{G}$ to the relative multiplication group of Q in Q'.

PROOF By Proposition 2.8, the insertion $Q \hookrightarrow Q'$ induces a group homomorphism $j : \mathrm{U}(Q;\mathbf{V}) \to \mathrm{U}(Q';\mathbf{V})$. The epimorphism (2.39) is then obtained by corestricting the composite of j with the projection (2.37) for Q'. □

Example 2.7

Let $\mathbf{A}$ be the variety of abelian quasigroups. The free $\mathbf{A}$-quasigroup on the singleton $\{X\}$ is the infinite cyclic group $\mathbb{Z}X$. For a nonempty member A of $\mathbf{A}$, i.e. for an abelian group A, the quasigroup $\widetilde{A}$ is just $A \oplus \mathbb{Z}X$. Then $A \to \mathrm{U}(A;\mathbf{A}); a \mapsto \widetilde{R}(a)$ is an isomorphism of groups. Also $\mathrm{U}(\varnothing;\mathbf{A}) = \{1\}$. □

Let $\mathbf{G}$ be the variety of associative quasigroups. Thus $\mathbf{G}$ includes the empty quasigroup that is not an object of $\mathbf{Gp}$. The following result identifies the universal multiplication groups in $\mathbf{G}$ as "diagonal groups" in the sense of [24, p. 8]. It is instructive to contrast Proposition 2.9 with Example 2.1.

PROPOSITION 2.9

For nonempty Q in $\mathbf{G}$, i.e. for a group Q, the universal multiplication group $\mathrm{U}(Q;\mathbf{G})$ of Q in the variety of associative quasigroups is the direct product $\widetilde{L}(Q) \times \widetilde{R}(Q)$ of two copies of Q.

PROOF The free **G**-quasigroup on the singleton $\{X\}$ is the infinite cyclic group $\mathbb{Z}X$. Then $\widetilde{Q}$ is the free product of Q with $\mathbb{Z}X$. As in Example 2.1, define

$$\widetilde{T} : Q \times Q \to \mathrm{U}(Q;\mathbf{G}); (g,h) \mapsto \widetilde{L}(g)^{-1}\widetilde{R}(h). \tag{2.40}$$

This is clearly a surjective homomorphism. Suppose $\widetilde{T}(g,h) = 1$. Then for all y in $\widetilde{Q}$, one has $g^{-1}yh = y$. Taking $y = g$ yields $h = g$. Taking $y = X$ then yields $g^{-1}Xg = X \in \mathbb{Z}X \cap g^{-1}\mathbb{Z}Xg$. By the known structure of free products of groups [98, Cor. 4.1.5 and Lemma 4.1], it follows that $g \in Q \cap \mathbb{Z}X = \{1\}$. Thus $\widetilde{T}$ is also injective, and hence an isomorphism. □

The main result of this section is the demonstration that the universal multiplication group $\widetilde{G}$ of a quasigroup Q in the variety of all quasigroups is free. Let $T(Q)$ be the ternary multiplication table of Q. It may be regarded as a partial Latin square on the disjoint union $Q + \{X\}$ of Q with the singleton $\{X\}$. The coproduct $Q[X]$ is then obtained as the free extension $Q_{(Q+\{X\},T(Q))}$ of this partial Latin square $\big(Q + \{X\}, T(Q)\big)$. The actions of the right and left multiplications by elements of Q on the generic element X may be written as

$$X\widetilde{L}(q) = qX\mu\,, \qquad X\widetilde{R}(q) = qX\mu^{\sigma}\,,$$

$$X\widetilde{L}(q)^{-1} = qX\mu^{\tau}\,, \qquad X\widetilde{R}(q)^{-1} = qX\mu^{\tau\sigma}$$

in the notation of Section 1.8. In the notation of Section 2.2, the universal multiplication group elements $\widetilde{R}(q_i)^{\pm 1}$ or $\widetilde{L}(q_i)^{\pm 1}$, for an element q_i of Q, are written generically as $\widetilde{E}_i(q_i)^{\varepsilon_i}$. The action of this universal multiplication group element on X now becomes $X\widetilde{E}_i(q_i)^{\varepsilon_i} = q_i X \mu^{g_i}$ for an element g_i of the complex product $\langle\tau\rangle\langle\sigma\rangle$ in the symmetric group S_3.

THEOREM 2.2

For the variety **Q** *of all quasigroups, and for a quasigroup Q, the universal multiplication group $\widetilde{G} = \mathrm{U}(Q;\mathbf{Q})$ is the free group on the disjoint union $\widetilde{L}(Q) + \widetilde{R}(Q)$ of two copies of Q.*

PROOF Suppose that the identity element of $\widetilde{G}$ is represented by a non-trivial reduced group word $\widetilde{E}(q_1)^{\varepsilon_1} \ldots, \widetilde{E}(q_r)^{\varepsilon_r}$ over the set $\widetilde{L}(Q) + \widetilde{R}(Q)$ of generating letters. Then the element $X\widetilde{E}(q_1)^{\varepsilon_1} \ldots, \widetilde{E}(q_r)^{\varepsilon_r}$ of $Q_{\left(Q+\{X\},T(Q)\right)}$ has the form

$$q_r \ldots q_1 X \mu^{g_1} \ldots \mu^{g_r} \tag{2.41}$$

with q_i in Q and g_i in $\langle\tau\rangle\langle\sigma\rangle$. This form is already reduced, since the group word $\widetilde{E}(q_1)^{\varepsilon_1} \ldots, \widetilde{E}(q_r)^{\varepsilon_r}$ is reduced. On the other hand, for this group word to represent the identity element of $\widetilde{G}$, the form (2.41) should reduce to X. □

2.8 Universal stabilizers

Let Q be a quasigroup in a variety $\mathbf{V}$ of quasigroups. For elements e, q, r of Q, define elements

$$\widetilde{T}_e(q) = \widetilde{R}(e\backslash q)\widetilde{L}(q/e)^{-1}, \tag{2.42}$$

$$\widetilde{R}_e(q,r) = \widetilde{R}(e\backslash q)\widetilde{R}(r)\widetilde{R}(e\backslash qr)^{-1}, \tag{2.43}$$

$$\widetilde{L}_e(q,r) = \widetilde{L}(q/e)\widetilde{L}(r)\widetilde{L}(rq/e)^{-1} \tag{2.44}$$

of the universal multiplication group $\widetilde{G}$ of Q in $\mathbf{V}$. It is helpful to associate these elements with circuits based at the vertex e in the Cayley graph $\mathrm{Cay}\,\widetilde{Q}$. For example, $\widetilde{T}_e(q)$ corresponds to the circuit starting out from e forwards along the edge $R(e \searrow q)$ to q, and then backwards along the edge $L(q \swarrow e)$. The element $\widetilde{R}_e(q,r)$ corresponds to the circuit which again starts out from e forwards along the edge $R(e \searrow q)$ to q, then continues forwards along the edge $R(q \searrow qr)$ to qr, finally returning to e backwards along the edge $R(e \searrow qr)$. It is thus clear that for a fixed element e of Q, the elements (2.42) through (2.44) all lie in the *universal stabilizer* of e in Q in $\mathbf{V}$, the stabilizer $\widetilde{G}_e$ of e in the permutation group $\widetilde{G}$ on Q. In fact, the full set

$$\{\widetilde{T}_e(q), \widetilde{R}_e(q,r), \widetilde{L}_e(q,r) \mid \ q,r \in \ Q\} \tag{2.45}$$

of elements (2.42) through (2.44) serves to generate $\widetilde{G}_e$, as seen immediately from the following theorem.

THEOREM 2.3

Let e be an element of a quasigroup Q. Let $\widetilde{G}$ be the universal multiplication group of Q in the variety $\mathbf{Q}$ of all quasigroups. Then the universal stabilizer $\widetilde{G}_e$ is the free group on (2.45)*. In particular, if Q has finite order n, then the rank of $\widetilde{G}_e$ is $2n^2 - n + 1$.*

PROOF Apply the explicit form of Schreier's Theorem, e.g., as in [143, Prop. I.16]. The notation of that reference will be used. By Theorem 2.2, the disjoint union $\widetilde{L}(Q) + \widetilde{R}(Q)$ is a free basis S for $\widetilde{G}$. A transversal to $\widetilde{G}_e$ in $\widetilde{G}$, closed under initial subwords, is given by

$$T = \{1\} \cup \{\widetilde{R}(e\backslash\ q) \mid e \neq q \in Q\}.$$

Then $W = \{(t,s) \in \ T \times \ S \mid ts \notin T\}$

$$= \{(1, \widetilde{R}(e\backslash\ e)), (1, \widetilde{L}(q)) \mid q \in Q\}$$
$$\cup \{(\widetilde{R}(e\backslash\ q), \widetilde{R}(r)), (\widetilde{R}(e\backslash\ q), \widetilde{L}(r)) \mid e \neq q \in Q,\ r \in Q\}.$$

The free basis $R = \{h_{t,s} \mid (t,s) \in W\}$ of $\widetilde{G}_e$ consists of $h_{1,\widetilde{R}(e\setminus\ e)} = \widetilde{R}(e\setminus\ e)$, $h_{1,\widetilde{L}(q/e)} = \widetilde{T}_e(q)^{-1}$ for q in Q, $h_{\widetilde{R}(e\setminus\ q),\widetilde{R}(r)} = \widetilde{R}_e(q,r)$ for $q \neq e$, and $h_{\widetilde{R}(e\setminus\ q),\widetilde{L}(r)} = \widetilde{T}_e(q)\widetilde{L}_e(q,r)\widetilde{T}_e(qr)^{-1}$ for $q \neq e$. Since (2.45) is obtained from R by a Nielsen transformation [98, §3.2], that set is also a free basis for $\widetilde{G}_e$. Now $\widetilde{G}_e$ is of index $|Q|$ in $\widetilde{G}$. If Q has finite order n, the Schreier Index Formula [143, Cor. I.5] gives the rank of $\widetilde{G}_e$, i.e., the cardinality of (2.45), as $2n^2 - n + 1$. □

COROLLARY 2.6

Let e be an element of a quasigroup Q. Then the stabiliser G_e of e in the combinatorial multiplication group G of Q is generated by

$$\{T_e(q), R_e(q,r), L_e(q,r) \mid q, r \in Q\}\,.$$

PROOF Apply the homomorphism (2.37) to the generation of $\widetilde{G}_e$ by (2.45). □

2.9 Exercises

1. Let Q be a nonempty quasigroup. Show that Q is a group if and only if the map
$$R : Q \to \mathrm{Mlt}\, Q; q \mapsto R(q)$$
is a quasigroup homomorphism.

2. A quasigroup Q is said to be *right distributive* if for each element q of Q, the right multiplication (2.1) is an endomorphism of Q. Similarly, Q is said to be *left distributive* if the left multiplications (2.2) are all endomorphisms. Finally, Q is said to be *distributive* if it is both right and left distributive.

   (a) Show that Q is right distributive if and only if it satisfies the identity
   $$xy \cdot z = xz \cdot yz\,.$$
   (b) Determine the corresponding identity characterizing left distributivity.
   (c) Is there a single quasigroup identity characterizing distributivity?

3. Show that an idempotent, entropic quasigroup is distributive.

4. Show that each conjugate of a distributive quasigroup is distributive.

5. [12] Let e be a fixed element of a distributive quasigroup $(Q, \cdot)$. Show that $x + y = (x/e) \cdot (e \backslash y)$ defines a commutative Moufang loop $(Q, +, e)$.

6. (a) If $(Q, \cdot)$ is a right quasigroup, show that the opposite multiplication (1.5) yields a left quasigroup $(Q, \circ)$.

   (b) If $(Q, \cdot, /)$ is a right quasigroup, show that $(Q, /, \cdot)$ is also a right quasigroup.

7. Show that a set Q, equipped with a binary multiplication, forms a left quasigroup if and only if for all x, y in Q, there is a unique element z of Q such that $y = xz$.

8. Show that the quasigroup identities (IL)–(SR) may be displayed in the mirror-symmetric form

$$\begin{array}{l|l} \mathsf{v}\backslash(\mathsf{v}\cdot\mathsf{w}) = \mathsf{w} & \mathsf{w} = (\mathsf{w}\cdot\mathsf{v})/\mathsf{v} \\ \mathsf{v}\cdot(\mathsf{v}\backslash\mathsf{w}) = \mathsf{w} & \mathsf{w} = (\mathsf{w}/\mathsf{v})\cdot\mathsf{v} \end{array}$$

   so that the two identities on the left of the mirror characterize left quasigroups $(Q, \cdot, \backslash)$, while their images on the right of the mirror characterize right quasigroups $(Q, \cdot, /)$.

9. Two binary operations m_1, m_2 on a set Q are said to be *orthogonal* if the map

$$Q \times Q \to Q \times Q; (x, y) \mapsto (xym_1, xym_2)$$

   bijects.

   (a) Show that $(Q, \cdot)$ is a left quasigroup if and only if the left projection

$$\pi_1 : Q \times Q \to Q; (x, y) \mapsto x \tag{2.46}$$

   and the multiplication

$$\mu : Q \times Q \to Q; (x, y) \mapsto x \cdot y \tag{2.47}$$

   are orthogonal.

   (b) If Q is a left quasigroup, determine the inverse of the bijection $(\pi_1, \mu) : Q \times Q \to Q \times Q$.

   (c) Formulate and prove a comparable characterization of right quasigroups using the right projection

$$\pi_2 : Q \times Q \to Q; (x, y) \mapsto y\,. \tag{2.48}$$

   (d) [86] Combine (a) and (c) to obtain a characterization of quasigroups.

10. Let Q be a quasigroup. Continue the notation of Exercise 9. For an element q of Q, define the 1-*line* labeled q to be the inverse image

$$\pi_1^{-1}(\{q\}) = \{(q, y) \in Q \times Q \mid y \in Q\}$$

of the singleton $\{q\}$ under the left projection (2.46). Similarly, define the 2-*line* labeled q to be the inverse image

$$\pi_2^{-1}(\{q\}) = \{(x, q) \in Q \times Q \mid x \in Q\}$$

of the singleton $\{q\}$ under the right projection (2.48), and define the 3-*line* labeled q to be the inverse image

$$\mu^{-1}(\{q\}) = \{(x, y) \in Q \times Q \mid x \cdot y = q\}$$

of the singleton $\{q\}$ under the multiplication (2.47). Define

$$\left\{\pi_1^{-1}(\{x\}) \,\middle|\, x \in Q\right\},$$

$$\left\{\pi_2^{-1}(\{x\}) \,\middle|\, x \in Q\right\},$$

$$\left\{\mu^{-1}(\{x\}) \,\middle|\, x \in Q\right\}$$

as the respective (*unlabeled*) *bundles* of 1-, 2-, and 3-lines. Similarly, define

$$\left\{\pi_1^{-1}(\{x\}) \,\middle|\, x \in Q\right\} \to Q; \pi_1^{-1}(\{q\}) \mapsto q,$$

$$\left\{\pi_2^{-1}(\{x\}) \,\middle|\, x \in Q\right\} \to Q; \pi_2^{-1}(\{q\}) \mapsto q,$$

$$\left\{\mu^{-1}(\{x\}) \,\middle|\, x \in Q\right\} \to Q; \mu^{-1}(\{q\}) \mapsto q$$

as the respective *labeled bundles* of 1-, 2-, and 3-lines. Finally, define the set $Q \times Q$ equipped with the bundles of 1-, 2-, and 3-lines as the (*unlabeled*) 3-*net* of Q, and the set $Q \times Q$ equipped with the labeled bundles of 1-, 2-, and 3-lines as the *labeled* 3-*net* of Q.

(a) Show that the quasigroup Q is determined by its labeled 3-net.

(b) Show that Q is determined up to isotopy by its unlabeled 3-net.

11. Let $(Q, \cdot, /)$ be a right loop. Show that the derived operation

$$(x, y, z)P = (x/y) \cdot z$$

satisfies the identities (2.28).

12. Let Q be a set. For elements x, y of Q, define $x \cdot y = x$.

    (a) Show that $(Q, \cdot, \cdot)$ is a right quasigroup.

    (b) Show that Proposition 2.3 does not extend from right loops to right quasigroups.

13. [47] Let e and f be elements of a quasigroup Q with multiplication group G. Show that for all x in Q, the multiplication group element

$$R(e\backslash x)L(f)^{-1}L(e)R(f\backslash x)^{-1}$$

    lies in both the stabilizers G_e and G_f.

14. Give an alternative proof of Theorem 2.3 as follows: taking H to be the (free) subgroup of $\widetilde{G}$ generated by (2.45), prove by induction on the length of a typical nontrivial word w in $\widetilde{G}$ that there is an expression $w = h\widetilde{R}(e\backslash\, q)$ with h in H and q in Q. It then follows that $H = \widetilde{G}_e$.

15. Let Q be a quasigroup with an element e. Show that the universal multiplication group $\widetilde{G}$ is free on

$$\left\{\rho(e,q), R(e\backslash e), T_e(e), T_e(q) \,\middle|\, q \in Q \smallsetminus \{e\}\right\}. \tag{2.49}$$

    (The free generating set (2.49) for $\widetilde{G}$ breaks up nicely into the set

$$\left\{\rho(e,q) \,\middle|\, q \in Q \smallsetminus \{e\}\right\}$$

    of nontrivial elements of a loop transversal to $\widetilde{G}_e$ in $\widetilde{G}$ and the set

$$\{T_e(q) \mid q \in Q\}$$

    of elements of the universal stabilizer $\widetilde{G}_e$. For an application of this generating set, see Theorem 12.2.)

16. Let G be a group generated by a conjugacy class Q of involutions. For each x, y in Q, suppose that the product xy has odd order.

    (a) Show that $x \cdot y = yxy$ defines a right distributive quasigroup $(Q, \cdot)$.

    (b) Show that $\mathrm{RMlt}(Q, \cdot)$ is isomorphic to $G/Z(G)$.

17. (a) For each positive dimension n, use polar decomposition to show that the set P_n of $n \times n$ positive definite symmetric real matrices forms a loop transversal to the orthogonal group O_n in the general linear group $\mathrm{GL}_n(\mathbb{R})$ of invertible real matrices.

    (b) Demonstrate that for $n > 1$, the loop P_n is not associative.

(c) Obtain similar results for the set of $n \times n$ positive definite Hermitian complex matrices as a loop transversal to the unitary group U_n in the general linear group $\mathrm{GL}_n(\mathbb{C})$ of invertible complex matrices.

18. In special relativity, show that the set of boosts forms a loop transversal to the group of spatial rotations in the Lorentz group.

19. Determine a basis for the 4-dimensional vector space C of Example 2.6.

20. Consider the binary alphabet A as the two-element field $\mathbb{Z}/2\mathbb{Z}$. Thus a binary channel A^n of length n carries the product ring structure, with componentwise addition and multiplication. A linear code C in the channel A^n is said to be *doubly even* if 4 divides the Hamming weight $|c|$ of each codeword c in C. A mapping $\phi : C^2 \to A$ is then said to be a *factor set* if:

(i) $\phi(c, c) = |c|/4 + 2\mathbb{Z}$,

(ii) $\phi(c, d) + \phi(d, c) = |c \cdot d|/2 + 2\mathbb{Z}$, and

(iii) $\phi(b, c) + \phi(b, c + d) + \phi(c, d) + \phi(b + c, d) = |b \cdot c \cdot d| + 2\mathbb{Z}$

for all codewords b, c, d in C. If $\phi : C^2 \to A$ is indeed a factor set, show that

$$(\alpha, c)(\beta, d) = (\alpha + \beta + \phi(c, d), c + d) \tag{2.50}$$

defines a Moufang loop operation on $A \times C$. (Griess [67] showed that each doubly even code admits a factor set, yielding a *code loop* (2.50).)

21. In the multiplication group of a Moufang loop, set $P(x) = L(x)^{-1}R(x)^{-1}$. Derive the *triality relations*

$$\begin{aligned} P(xyx) &= P(x)P(y)P(x)\,, \\ R(xyx) &= R(x)R(y)R(x)\,, \\ L(xyx) &= L(x)L(y)L(x) \end{aligned}$$

and

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

22. Let u be an element of an entropic quasigroup $(Q, \cdot, /, \backslash)$. Define elements $u_1, u_2, \ldots$ of Q inductively by $u_1 = u$ and $u_{n+1} = u_n \cdot u_n$ for $n > 0$. Show that the right quasigroup reduct $(Q, //, \backslash)$ of Q, together with the set $\{u_n \mid n \in \mathbb{Z}^+\}$ of elements of Q, forms a Conway algebra in the sense of knot theory [133].

23. In the context of Theorem 1.1, let N be the subgroup of the monoid M generated by the subset $\{\mu, \mu^\sigma\}$. Show that the group N is isomorphic to the relative multiplication group of the subquasigroup generated by x in the free quasigroup M on $\{x, y\}$.

24. In the context of Theorem 1.1, let F be the subgroup of the monoid M generated by the subset $\{\mu^g \mid g \in S_3\}$. Show that F is a free group of rank 3.

25. [55] Show that the combinatorial multiplication group of a free quasigroup is free.

2.10 Notes

Section 2.3

The closure operator $N \mapsto N^{\flat\sharp}$ was originally studied by A.A. Albert [2] for the case of loops.

Section 2.5

In [56], right and left quasigroups were described respectively as "right" and "left groupoids."

The characterization of loop transversals given in Proposition 2.5 is due to R. Baer [5]. Use of a derived operation with the properties (2.28) goes back to Mal'tsev [110].

Section 2.6

Loop transversal codes were first introduced in the R.C. Bose memorial volume [154]. Using a simple greedy algorithm to construct the loop transversal, one obtains uniform series of good linear codes, many of them optimal, that have previously required a range of ad hoc techniques from Galois theory, combinatorics and elsewhere for their construction [81] [82]. Loop transversal codes are readily designed for the correction of errors having specific statistics, such as burst errors [30].

Section 2.8

For the identity element e of a loop Q, Corollary 2.6 was proved by Bruck [21, Lemma IV.1.2], using a method like that of Exercise 14.

Chapter 3

CENTRAL QUASIGROUPS

Central quasigroups are the quasigroup analogues of abelian groups. For a quasigroup Q, the *diagonal* quasigroup is defined as

$$\widehat{Q} = \{(x, x) \mid x \in Q\}. \tag{3.1}$$

Now a group Q is abelian if and only if the diagonal is a normal subgroup of Q^2. Certainly, if Q is abelian, then so is Q^2, whence each subgroup of Q^2 is normal. Conversely, suppose that $\widehat{Q} \lhd Q^2$. Then for all $x, y \in Q$, one has

$$(x, y)^{-1}(x, x)(x, y) = (x, y^{-1}xy) \in \widehat{Q},$$

so that $x = y^{-1}xy$. Thus Q is abelian. A subquasigroup N of a quasigroup P is said to be a *normal* subquasigroup, written as $N \lhd P$, if there is a congruence W on P having N as a congruence class.[1] Note that the congruence W is specified uniquely by the fact that for any $e \in N, x \in P$, the map $\rho(e, x) : N \to x^W$ of (2.26) provides a bijection between N and the congruence class x^W of the element x of P. One may then use the usual division notation P/N to denote the unambiguously specified quotient quasigroup P^W.[2] By analogy with the group case, a quasigroup Q is defined to be *central*, or in the class $\mathfrak{Z}$, if the diagonal is a normal subquasigroup of Q^2. One also says that the universal congruence Q^2 on Q is central. More generally, a congruence V on a quasigroup Q is defined to be *central* if $\widehat{Q} \lhd V$.

Following a brief discussion of general quasigroup congruences in Section 3.1, Section 3.2 examines the central congruences of a quasigroup, in the slightly broader context of centrality that will be useful for the treatment of quasigroup modules in Chapter 10. Now abelian groups are the nilpotent groups of class 1. Section 3.3 uses central congruences to give a definition of nilpotence for quasigroups that specializes appropriately to groups. Central quasigroups then become the nilpotent quasigroups of class 1. Section 3.4 discusses the relation of central isotopy, which is weaker than isomorphism, but stronger than general isotopy. In many ways, the relation of central isotopy between quasigroups is more important than the relation of isomorphism. Theorem 3.4

[1] The empty quasigroup is a normal subquasigroup of itself, but not of any bigger quasigroup.
[2] Note that $\varnothing/\varnothing$ is empty, as required for the integrity of the First Isomorphism Theorem [165, IV Th.1.2.7].

gives a typical example, showing the role of central isotopy in noncancellation phenomena under the direct product. Theorem 3.8 is another example. Here, central isotopy classes of central quasigroups are shown to correspond exactly to isomorphism classes of central piques. The key Section 3.6, describing the structure of central quasigroups, is thus preceded by Section 3.5 dealing with central piques. Section 3.7 uses centrality to classify quasigroups of prime order. The main Theorem 3.10 may be summarized as saying that for prime order, either a quasigroup is central, or else its multiplication group is almost simple — sandwiched between a simple group and its automorphism group, the simple group being alternating, linear, or one of the Mathieu groups M_{11} or M_{23}. Section 3.8 examines the stability congruence of a quasigroup. For loops, the stability and center congruences coincide, but they may separate for general quasigroups. There is a corresponding concept of stable nilpotence. Nilpotence of the multiplication group implies stable nilpotence of a finite quasigroup. Conversely, stably nilpotent quasigroups have solvable multiplication groups. Chapter 3 concludes with a brief discussion of some so-called "no-go theorems," showing that certain groups or group actions cannot be represented as multiplication groups of quasigroups.

3.1 Quasigroup congruences

In general, a congruence relation V on an algebra A is a subalgebra of A^2 that is an equivalence relation (Appendix B). For a quasigroup Q, the properties (2.28) of the derived operation (2.27) imply that reflexivity of a subquasigroup V of Q^2 already yields V as a congruence on Q.

PROPOSITION 3.1

Let V be a subquasigroup of the direct square Q^2 of a quasigroup Q. Then if V contains the diagonal $\widehat{Q}$, it is a congruence on Q.

PROOF The symmetry and transitivity of V must be established. Suppose $(x, y), (y, z) \in V$. Then

$$\begin{aligned} &(x, x) \in V && \text{by reflexivity,} \\ &(x, y) \in V && \text{is given, and} \\ &(y, y) \in V && \text{by reflexivity} \\ \Rightarrow\ &((x, x, y)P, (x, y, y)P) \in V, \end{aligned}$$

since the subalgebra V of Q^2 is closed under the derived operation P. By (2.28), it follows that $(y, x) \in V$, so that V is symmetric. Similarly,

$$\begin{array}{ll} (x,y) \in V & \text{is given,} \\ (y,y) \in V & \text{by reflexivity, and} \\ (y,z) \in V & \text{given} \\ \Rightarrow ((x,y,y)P, (y,y,z)P) \in V. & \end{array}$$

Thus $(x,z) \in V$, so that V is transitive. ∎

The *join* of two congruences V, V' on an algebra A is the smallest congruence containing both of them. The *relation product* $V \circ V'$ of two binary relations V, V' on a set N is the relation

$$V \circ V' = \{(x,z) \in N^2 \mid \exists\, y \in N \,.\, x\ V\ y\ V' z\}. \tag{3.2}$$

on the set N.

COROLLARY 3.1
Let V and V' be congruences on a quasigroup Q. Then their join is their relation product $V \circ V'$.

PROOF The relation product $V \circ V'$ is a reflexive subquasigroup of Q^2, itself containing V and V', and contained in each congruence containing V and V'. ∎

PROPOSITION 3.2
A quasigroup Q is isomorphic to the direct product $P \times P'$ of two quasigroups P, P' if and only if there are congruences V, V' on Q such that

$$V \circ V' = Q^2,\ V \cap V' = \widehat{Q},\ Q^V \cong P,\ Q^{V'} \cong P'.$$

PROOF On $Q = P \times P'$, define

$$(a,a')V(b,b') \Leftrightarrow a = b \ \text{ and } \ (a,a')V'(b,b') \Leftrightarrow a' = b'. \tag{3.3}$$

Then $V \circ V' = Q^2$, since $(a,a')V(a,b')V'(b,b')$. Also $V \cap V' = \widehat{Q}$. Moreover, the First Isomorphism Theorem applied to the projections $Q \to P; (a,a') \mapsto a$ and $Q \to P'; (a,a') \mapsto a'$ yields well-defined isomorphisms $Q^V \cong P$ and $Q^{V'} \cong P'$.

Conversely, suppose that a quasigroup Q carrying two congruences V, V' satisfying $V \circ V' = Q^2,\ V \cap V' = \widehat{Q}$ is equipped with a pair of isomorphisms $f : Q^V \to P,\ f' : Q^{V'} \to P'$. Define

$$F : Q \to P \times P'; x \mapsto (x^V f, x^{V'} f'),$$

clearly a quasigroup homomorphism. Then $xF = yF \Rightarrow x(V \cap V')y$, so F injects. Now consider $(a,c) \in P \times P'$. Suppose $af^{-1} = x^V$ and $cf'^{-1} = z^{V'}$. Now

$$(x,z) \in Q^2 = V \circ V' \Rightarrow \exists y \in Q.\ x\ V\ y\ V'\ z.$$

Then

$$yF = (y^V f, y^{V'} f') = (x^V f, z^{V'} f') = (a, c),$$

so that F surjects. □

3.2 Centrality

DEFINITION 3.1 *Let U and V be congruences on a quasigroup Q. Then U is said to* centralize *V by a* centering congruence *W if and only if W is a congruence on the quasigroup V such that the following conditions are satisfied:*

(C0) $(x, y)W(x', y') \Rightarrow (x, x') \in U$;

(C1) *For all (x, y) in V, the map*

$$\pi : (x, y)^W \to x^U; (x', y') \mapsto x' \tag{3.4}$$

bijects;

(C2) W respects the equivalence *of V in the following sense:*

(RR) $(x, y) \in U \Rightarrow (x, x)W(y, y)$;

(RS) $(x_1, x_2)W(y_1, y_2) \Rightarrow (x_2, x_1)W(y_2, y_1)$;

(RT) $(x_1, x_2)W(y_1, y_2),\ (x_2, x_3)W(y_2, y_3) \Rightarrow (x_1, x_3)W(y_1, y_3)$.

The three conditions comprising (C2) *are known as* respect for the reflexivity, symmetry, *and* transitivity *of V, respectively.*

Example 3.1
Consider the congruences V, V' defined by (3.3) on the direct product $P \times P'$ of two quasigroups. Define

$$W = \{(((x_1, x_1'), (x_1, x_2')), ((x_2, x_1'), (x_2, x_2'))) \mid x_i \in P,\ x_i' \in P'\}.$$

Then V' centralizes V with W as a centering congruence. □

PROPOSITION 3.3
Let V be a congruence on a quasigroup Q. Then V is central if and only if it is centralized by $U = Q^2$ via a centering congruence W.

PROOF Let V be centered by W. If Q is empty, then so are V and $\widehat{Q}$, with $\widehat{Q} \lhd V$, so that V is central. Otherwise, consider an element e of Q. Now $\widehat{Q} \leq (e,e)^W$ by (RR), while $(e,e)^W \subseteq \widehat{Q}$ by (C1). Thus $\widehat{Q} = (e,e)^W$, so that V is central.

Conversely, suppose that V is central, $\widehat{Q}$ being an equivalence class of a congruence W on V. It will be shown that W is a centering congruence by which Q^2 centralizes V. The result is immediate if Q is empty, so assume $Q \neq \varnothing$. The proof uses the properties (2.28) of the derived operation P of (2.27), and the fact that the congruence W on V is a subalgebra of V^2 under the operation P. Certainly (RR) holds, since $\widehat{Q}$ is a W-class.

(RS): Suppose $(x_1,x_2)W(y_1,y_2)$. Then

$$\begin{array}{ll} (x_1,x_1)W(y_1,y_1) & \text{by (RR)}, \\ (x_1,x_2)W(y_1,y_2) & \text{is given}, \\ (x_2,x_2)W(y_2,y_2) & \text{by (RR)} \end{array}$$

$$\Rightarrow ((x_1,x_1,x_2)P,(x_1,x_2,x_2)P)W((y_1,y_1,y_2)P,(y_1,y_2,y_2)P).$$

By (2.28), it follows that $(x_2,x_1)W(y_2,y_1)$, as required for (RS).

(RT): Suppose further that $(x_2,x_3)W(y_2,y_3)$. Then

$$\begin{array}{ll} (x_1,x_2)W(y_1,y_2) & \text{is given}, \\ (x_2,x_2)W(y_2,y_2) & \text{by (RR)}, \\ (x_2,x_3)W(y_2,y_3) & \text{is given} \end{array}$$

$$\Rightarrow ((x_1,x_2,x_2)P,(x_2,x_2,x_3)P)W((y_1,y_2,y_2)P,(y_2,y_2,y_3)P).$$

By (2.28), it follows that $(x_1,x_3)W(y_1,y_3)$, as required for (RT). This completes the verification of (C2). Note that (C0) is trivial.

(C1): Suppose $(x,y) \in W$, and $x' \in Q$. Then

$$\begin{array}{ll} (x,y)W(x,y) & (W \text{ reflexive}), \\ (x,x)W(x,x) & (W \text{ reflexive}), \\ (x,x)W(x',x') & \text{by (RR)} \end{array}$$

$$\Rightarrow ((x,x,x)P,(y,x,x)P)W((x,x,x')P,(y,x,x')P).$$

By (2.28), it follows that $(x,y)W(x',(y,x,x')P)$, so that (3.4) surjects. Now suppose $(x',y')W(x',y'')$. Then

$$\begin{array}{ll} (x',y')W(x',y'') & \text{is given}, \\ (x',x')W(x',x') & (W \text{ reflexive}), \\ (y',x')W(y',x') & (W \text{ reflexive}) \end{array}$$

$$\Rightarrow ((x',x',y')P,(y',x',x')P)W((x',x',y')P,(y'',x',x')P).$$

By (2.28), it follows that $(y', y')W(y', y'')$. Thus (y', y'') lies in the class $\widehat{Q}$ of W, so that $y' = y''$ and (3.4) injects. This completes the proof of (C1). □

PROPOSITION 3.4

Let U and V be congruences on a quasigroup Q. Suppose that U centralizes V by a centering congruence W. Then W is uniquely specified by

$$\forall\ yVxUx'\,,\ \forall\ y' \in Q\,,\ (x,y)W(x',y') \ \Leftrightarrow\ y' = (x',x,y)P \tag{3.5}$$

in terms of the derived operation P of (2.27)*. Further,*

$$\forall\ xVyUy'\,,\ \forall\ x' \in Q\,,\ (x,y)W(x',y') \ \Leftrightarrow\ x' = (x,y,y')P. \tag{3.6}$$

PROOF The statements (3.5) and (3.6) are vacuously true if Q is empty. Otherwise, consider $yVxUx'$. Then

$$\begin{array}{ll} (x,x)W(x',x') & \text{by (RR)},\\ (x,x)W(x,x) & (W \text{ reflexive}),\\ (x,y)W(x,y) & (W \text{ reflexive}) \end{array}$$

$$\Rightarrow ((x,x,x)P,(x',x,x)P)W((x',x,x)P,(x',x,y)P).$$

By (2.28), it follows that $(x,x')W(x',(x',x,y)P)$, proving the backward implication of (3.5). For the forward implication of (3.5), suppose $(x,y)W(x',y')$. Then $(x',y')W(x',(x',x,y)P)$, so that $y' = (x',x,y)P$ by property (C1) of W. The last statement (3.6) is proved similarly. □

In view of Proposition 3.4, it is sometimes convenient to write

$$(U|V) \quad \text{or} \quad (U'|V) \tag{3.7}$$

for the unique centering congruence by which a congruence U centralizes a congruence V, U' being a congruence containing U that still centralizes V.

COROLLARY 3.2

For an element (x,y) of a central congruence V on a quasigroup Q, and for each z in Q,

$$z = ((z,x,y)P,y,x)P. \tag{3.8}$$

PROOF Let V be centered by W. By (3.5) one has that

$$(x,y)W(z,(z,x,y)P) \text{ and } (y,x)W((z,x,y)P,((z,x,y)P,y,x)P).$$

Now (RT) implies $(x,x)W(z,((z,x,y)P,y,x)P)$, so (3.8) holds by (C1). □

REMARK 3.1 Note that (3.8) in the context of Corollary 3.2 amounts to

$$\rho(x,y)\rho(y,x) = 1. \tag{3.9}$$

In a group Q, the equation (3.9) always holds, even when x and y are not related by a central congruence. But in the quasigroup of Figure 1.2, one has $\rho(3,4)\rho(4,3) = (23)(56)$. □

An important application of Proposition 3.3 is to show that the join of two central congruences is central.

THEOREM 3.1
If V_1, V_2 are central congruences on a quasigroup Q, then so is $V = V_1 \circ V_2$.

PROOF Suppose that V_i is centered by W_i for $i = 1, 2$. Define a relation W on V by

$$(x,z)W(x',z') \Leftrightarrow \exists y, y' \in Q.\ (x,y)W_1(x',y') \text{ and } (y,z)W_2(y',z').$$

The relation W is certainly reflexive, and is readily seen to be a subquasigroup of V^2. By Proposition 3.1, W is a congruence on V. Now given $x, y \in Q$, respect for reflexivity yields $(x,x)W_i(y,y)$, $i = 1, 2$, so that $(x,x)W(y,y)$ and $\widehat{Q} \subseteq (x,x)^W$.

Conversely, suppose $(x,x)W(x',z')$, say

$$(x,y)W_1(x',y') \tag{3.10}$$

and

$$(y,x)W_2(y',z'). \tag{3.11}$$

By (3.5), the latter equation implies $z' = (y',y,x)P$. Since W_1 respects symmetry, (3.10) implies $(y,x)W_1(y',x')$, from which the equation $x' = (y',y,x)P$ follows by (3.5). Thus $x' = z'$, whence $\widehat{Q} = (x,x)^W$, and V is central. □

COROLLARY 3.3
A quasigroup Q has a unique maximal central congruence.

PROOF The set of central congruences on Q is partially ordered by inclusion. Zorn's Lemma yields the existence of maximal central congruences. By Theorem 3.1, there is then a unique maximal central congruence. □

DEFINITION 3.2 *Let Q be a quasigroup. Then the unique maximal central congruence on Q, whose existence is guaranteed by Corollary 3.3, is*

called the center congruence ζ *or* $\zeta(Q)$ *of* Q. *The* center *of a pique* Q *with pointed idempotent* e *is defined to be the subpique* $Z(Q) = e^{\zeta}$.

Corollary 3.8 below shows that the center (3.31) of a loop Q with identity element e (as defined by Albert and Bruck [20]) coincides with its pique center as specified by Definition 3.2. In particular, if e is the identity element of a group Q, then e^{ζ} is the usual center $Z(Q)$ of Q in the group sense.

3.3 Nilpotence

Given a function $f : X \to Y$, define

$$f^{\mathsf{II}} : X^2 \to Y^2; (x_1, x_2) \mapsto (x_1 f, x_2 f) \tag{3.12}$$

and

$$f^{\mathsf{IV}} : X^4 \to Y^4; ((x_1, x_2), (x_3, x_4)) \mapsto ((x_1 f, x_2 f), (x_3 f, x_4 f)). \tag{3.13}$$

The proofs of the following results are routine, using Proposition 3.4.

PROPOSITION 3.5
Let V *be a central congruence on a quasigroup* Q, *with centering congruence* W.

1. *If* $f : Q \to P$ *is a surjective quasigroup homomorphism, then* Vf^{II} *is a central congruence on* P, *centered by* Wf^{IV}.
2. *If* P *is a subquasigroup of* Q, *then* $V \cap P^2$ *is a central congruence on* P, *centered by* $W \cap (V \cap P^2)^2$.

COROLLARY 3.4
Homomorphic images and subquasigroups of central quasigroups are central.

PROPOSITION 3.6
For each element i *of an index set* I, *suppose that* V_i *is a central congruence on a quasigroup* Q_i, *with centering congruence* W_i. *Then on the product quasigroup* $Q = \prod_{i \in I} Q_i$, *the congruence* V *defined by*

$$(q, q') \in V \Leftrightarrow \forall\ i \in I,\ (q\pi_i, q'\pi_i) \in V_i$$

is central, with centering congruence W *given by*

$$(p, p')W(q, q') \Leftrightarrow \forall\ i \in I,\ (p\pi_i, p'\pi_i)W_i(q\pi_i, q'\pi_i).$$

COROLLARY 3.5
Products of central quasigroups are central.

As an instance of Birkhoff's Theorem (Theorem B.1), Corollaries 3.4 and 3.5 yield:

THEOREM 3.2
The class $\mathfrak{Z}$ *of central quasigroups forms a variety.*

Birkhoff's Theorem implies that central quasigroups may be characterized by the satisfaction of certain identities (which of course just specify the normality of the diagonal — Exercises 14 and 16). Corollary 3.7 below gives identities characterizing central piques.

A *central series* in a quasigroup Q is a series

$$\widehat{Q} = V_0 \leq V_1 \leq \cdots \leq V_n = Q^2$$

of congruences on Q such that $V_i \operatorname{nat} V_{i-1}$ is a central congruence of $Q \operatorname{nat} V_{i-1}$ for $1 \leq i \leq n$. Set $\zeta_0(Q) = \widehat{Q}$, and inductively define

$$\zeta_{i+1}(Q) = \ker(\operatorname{nat} \zeta_i(Q) \operatorname{nat} \zeta(Q^{\zeta_i})). \tag{3.14}$$

Note that $\zeta_0 \leq \zeta_1 \leq \zeta_2 \leq \ldots$. If there is a minimal natural number c such that $\zeta_c(Q) = Q^2$, then Q is said to be *nilpotent*, of *nilpotence class* c. If c is positive, then

$$\widehat{Q} = \zeta_0 < \zeta = \zeta_1 < \zeta_2 \cdots < \zeta_c = Q^2$$

is a central series in Q called the *upper central series* or *ascending central series* of Q. For a variety $\mathbf{V}$ of quasigroups, the class of nilpotent $\mathbf{V}$-quasigroups of class at most c is denoted by $\mathfrak{N}_c(\mathbf{V})$. Note that $\mathfrak{N}_1(\mathbf{Q})$ is just the variety $\mathfrak{Z}$ of central quasigroups. By analogy with Theorem 3.2, one may show that each class $\mathfrak{N}_c(\mathbf{V})$ is again a variety.

3.4 Central isotopy

DEFINITION 3.3 *Let P be a quasigroup, with center congruence $\zeta(P)$ centered by a congruence W. Then a quasigroup Q is said to be a* central isotope *of P, in symbols $Q \simeq P$, if and only if there is a bijection $t : Q \to P$, called a* central shift*, such that*

$$\exists\ (p, p') \in \zeta(P)\,.\ \forall\ q_1, q_2 \in Q\,,\ (p, p')W((q_1 \cdot q_2)^t, q_1^t \cdot q_2^t). \tag{3.15}$$

Centrally isotopic quasigroups are isotopic:

PROPOSITION 3.7
If (3.15) *holds, then there is an isotopy*

$$(t, t, t\rho(p, p')) : Q \to P.$$

PROOF According to (3.5), the relation (3.15) gives

$$q_1^t \cdot q_2^t = (q_1 q_2)t\rho(p, p'), \tag{3.16}$$

as required to show that (1.3) holds. □

On the other hand, since there are nonassociative isotopes of groups, the following proposition shows that central isotopy is a strictly tighter relation than isotopy.

PROPOSITION 3.8
Central isotopes of groups are groups.

PROOF Suppose that the identity map on a set Q is a central shift from a quasigroup structure $(Q, \circ)$ to a group structure $(Q, \cdot)$ on the set Q. By (3.16), there is an element $z = p^{-1}p'$ of the center of the group $(Q, \cdot)$ such that $q_1 \circ q_2 = q_1 q_2 z$ for q_1, q_2 in Q. Then $q_1 \circ z^{-1} = q_1$ and $z^{-1} \circ q_2 = q_2$, so that $(Q, \circ, z^{-1})$ is a loop isotopic to the group $(Q, \cdot)$. By Proposition 1.4 (p. 9), it follows that $(Q, \circ)$ is isomorphic to the group $(Q, \cdot)$. □

Isomorphic quasigroups are centrally isotopic. Indeed, since $\widehat{P}$ is a W-class, the central shift t of Definition 3.3 is an isomorphism if and only if $p = p'$. Later, examples of nonisomorphic but centrally isotopic quasigroups will be given. However, note the following.

PROPOSITION 3.9
A central shift $t : Q \to P$ is an isomorphism if it maps an idempotent of Q to an idempotent of P.

PROOF Let e be an idempotent of Q mapping to an idempotent of P. Then (3.15) gives

$$(p, p')W((e \cdot e)t, e^t e^t) = (e^t, e^t),$$

whence $p = p'$ and t is an isomorphism. □

Definition 3.3 was given in terms of quasigroup multiplication. The following lemma relates central isotopy to the divisions.

LEMMA 3.1
Suppose that (3.15) *holds. Then so do*

$$\forall\ q_1, q_2 \in Q,\ (p'/p, p/p)W((q_1/q_2)^t, q_1^t/q_2^t) \tag{3.17}$$

and

$$\forall\ q_1, q_2 \in Q,\ (p\backslash p', p\backslash p)W((q_1\backslash q_2)^t, q_1^t\backslash q_2^t). \tag{3.18}$$

PROOF By (3.15), one has

$$(p, p')W([(q_1/q_2)\cdot q_2]t, (q_1/q_2)^t \cdot q_2^t) = (q_1^t, (q_1/q_2)^t \cdot q_2^t). \tag{3.19}$$

Also, respect for reflexivity yields

$$(p, p)W(q_2^t, q_2^t). \tag{3.20}$$

Equation (3.17) follows on dividing (3.19) by (3.20) and using respect for symmetry. Equation (3.18) is proved similarly. □

THEOREM 3.3
Central isotopy is an equivalence relation. Further, if $t : Q \to P$ is a central shift, and the center congruence $\zeta(Q)$ of Q is centered by X, then $\zeta(Q)t^{\mathsf{II}} = \zeta(P)$ and Xt^{IV} centers $\zeta(P)$.

PROOF Use the notation of Definition 3.3. Let $u : P \to Q$ be the inverse of the bijection $t : Q \to P$. If $(q_1^t, q_2^t), (q_3^t, q_4^t) \in \zeta(P)$, then by (3.15) and the closure of $\zeta(P)$ under multiplication,

$$(q_1 \cdot q_3)t\ \zeta(P)\ q_1^t q_3^t\ \zeta(P)\ q_2^t q_4^t\ \zeta(P)\ (q_2 \cdot q_4)t\,,$$

so that $\zeta(P)u^{\mathsf{II}}$ is also closed under multiplication. Similar use of (3.17) and (3.18) yields the closure of $\zeta(P)u^{\mathsf{II}}$ under the divisions, so that it becomes a subquasigroup of Q^2. Since $\widehat{Q} = \widehat{P}u^{\mathsf{II}} \leq \zeta(P)u^{\mathsf{II}}$, Proposition 3.1 shows that $\zeta(P)u^{\mathsf{II}}$ is a congruence on Q. Now if

$$(q_1^t, q_2^t)\, W\, (r_1^t, r_2^t) \text{ and } (q_3^t, q_4^t)\, W\, (r_3^t, r_4^t),$$

(3.15) gives

$$\left((q_1 \cdot q_3)t, q_1^t \cdot q_3^t\right) W\, (p, p')\, W\, \left((r_1 \cdot r_3)t, r_1^t \cdot r_3^t\right). \tag{3.21}$$

Since W is a congruence on $\zeta(P)$,

$$(q_1^t \cdot q_3^t, q_2^t \cdot q_4^t)\, W\, (r_1^t \cdot r_3^t, r_2^t \cdot r_4^t). \tag{3.22}$$

Again, (3.15) gives

$$\left(q_2^t \cdot q_4^t, (q_2 \cdot q_4)t\right) W\, (p', p)\, W\, \left(r_2^t \cdot r_4^t, (r_2 \cdot r_4)t\right). \tag{3.23}$$

Since W respects the transitivity of $\zeta(P)$, the relations (3.21) through (3.23) yield

$$\big((q_1 \cdot q_3)t, (q_2 \cdot q_4)t\big)\, W\, \big((r_1 \cdot r_3)t, (r_2 \cdot r_4)t\big)\,,$$

so Wu^{IV} is closed under multiplication. Similar use of (3.17) and (3.18) in place of (3.15) yields the closure of Wu^{IV} under the divisions, so that it becomes a subquasigroup of $\zeta(P)u^{\mathsf{II}} \times \zeta(P)u^{\mathsf{II}}$. Since $\widehat{\zeta(P)u^{\mathsf{II}}} = \widehat{\zeta(P)}u^{\mathsf{IV}} \leq Wu^{\mathsf{IV}}$, Proposition 3.1 shows that Wu^{IV} is a congruence on Q. Since $\widehat{Q}t^{\mathsf{II}} = \widehat{P}$ is a W-class, $\widehat{Q}$ is a Wu^{IV}-class. Thus $\zeta(P)u^{\mathsf{II}}$ is a central congruence on Q, whence $\zeta(P)u^{\mathsf{II}} \leq \zeta(Q)$ by Corollary 3.3. By Proposition 3.4, $Wu^{\mathsf{IV}} = X \cap (\zeta(P)u^{\mathsf{II}} \times \zeta(P)u^{\mathsf{II}})$.

For p_1, p_2 in P, setting $q_i = p_i u$ in (3.15) gives

$$(p, p')\, W\, \big((p_1^u \cdot p_2^u)t, p_1 \cdot p_2\big)\,.$$

Applying u^{II} and using the respect of W for the symmetry of $\zeta(P)$,

$$(p'u, pu)\, W\, u^{\mathsf{IV}}\big((p_1 \cdot p_2)u, p_1^u \cdot p_2^u\big)\,.$$

From above, this can be written as

$$(p'u, pu)\, X\, \big((p_1 \cdot p_2)u, p_1^u \cdot p_2^u\big)\,.$$

Thus $u : P \to Q$ is also a central shift. In particular, the relation of central isotopy is symmetric. Repeating the above procedure for the new central shift u, one obtains $\zeta(Q)t^{\mathsf{II}} \leq \zeta(P)$. Thus $\zeta(Q)t^{\mathsf{II}} = \zeta(P)$ and $Xt^{\mathsf{IV}} = W$.

Now let R be a quasigroup centrally isotopic to Q, say by a central shift $s : R \to Q$ with

$$\exists\ (q, q') \in \zeta(Q).\ \forall\ r_1, r_2 \in R,\ (q, q')\, X\, \big((r_1 \cdot r_2)^s, r_1^s \cdot r_2^s\big)\,. \tag{3.24}$$

Applying t to (3.24) and using the above,

$$\forall\ r_1, r_2 \in R,\ (qt, q't) W \big((r_1 \cdot r_2)^{st}, (r_1^s \cdot r_2^s)t\big)\,.$$

By property (C1) for W, there is a unique element p'' of P such that the relation $(p'', p)\, W\, (qt, q't)$ holds, whence

$$(p'', p)\, W\, \big((r_1 \cdot r_2)^{st}, (r_1^s \cdot r_2^s)t\big)\,.$$

On the other hand, (3.15) gives

$$(p, p')\, W\, \big((r_1^s \cdot r_2^s)t, r_1^{st} \cdot r_2^{st}\big)\,.$$

Respect of W for the transitivity of $\zeta(P)$ yields

$$(p'', p')\, W\, \big((r_1 \cdot r_2)^{st}, r_1^{st} \cdot r_2^{st}\big)\,,$$

so that the composite st is a central shift. Thus central isotopy is a transitive relation. Finally, recall that the isomorphism $1_P : P \to P$ is a central shift, so that central isotopy is reflexive. □

COROLLARY 3.6
Central isotopes of central quasigroups are central.

PROPOSITION 3.10
Centrally isotopic quasigroups have similar multiplication group actions. In particular, their multiplication groups are isomorphic.

PROOF By the symmetry of central isotopy, it suffices to prove the containment $\mathrm{Mlt}(Q,*) \leq \mathrm{Mlt}(Q,\circ)$ for two quasigroup structures $(Q,*)$ and $(Q,\circ,/,\backslash)$ on the same set Q, centrally isotopic via the identity map on Q as central shift. But by (3.16),

$$\exists\ (p,p') \in \zeta(Q,\circ)\,.\ \forall\ q_1,q_2 \in Q\,,\ \ q_1 \circ q_2 = (q_1 * q_2)R_\circ(p\backslash p)^{-1}R_\circ(p\backslash p')\,.$$

Thus

$$L_*(q_1) = L_\circ(q_1)R_\circ(p\backslash p')^{-1}R_\circ(p\backslash p)$$

and

$$R_*(q_2) = R_\circ(q_2)R_\circ(p\backslash p')^{-1}R_\circ(p\backslash p),$$

as required. □

This section concludes with a brief discussion relating central quasigroups and central isotopy to noncancellation phenomena for the isomorphism relation $\cong$ under the direct product. The main result requires an important preliminary lemma that connects central congruences with central quasigroups.

LEMMA 3.2
Let V be a central congruence on a quasigroup Q. Then the quotient $V/\widehat{Q}$ is a central quasigroup.

PROOF Let W center V. Define a relation Ω on $V/\widehat{Q} \times V/\widehat{Q}$ by

$$\left((q_1,q_2)^W,(r_1',r_2')^W\right)\,\Omega\,\left((q_1',q_2')^W,(r_1,r_2)^W\right) \Leftrightarrow (q_1,q_3)\,W\,(q_1',q_3')\,,$$

where $(q_2,q_3)\,W\,(r_1,r_2)$ and $(q_2',q_3')\,W\,(r_1',r_2')$. It is then routine to check that Ω is a congruence centering $V/\widehat{Q} \times V/\widehat{Q}$. □

THEOREM 3.4

If the quasigroups P and Q are centrally isotopic, then there is a nonempty central quasigroup Z such that $P \times Z \cong Q \times Z$. If P and Q are finite, then Z may be taken to be finite.

PROOF Use the notation of Definition 3.3. Set

$$N = \{(p, q) \in P \times Q \mid (p, q^t) \in \zeta(P)\}.$$

Let $(p_1, q_1), (p_2, q_2)$ be elements of N. Then $\left(p_1 p_2, q_1^t q_2^t\right) \in \zeta(P)$, while (3.15) shows $\left(q_1^t q_2^t, (q_1 q_2)^t\right) \in \zeta(P)$. Thus $\left(p_1 p_2, (q_1 q_2)^t\right) \in \zeta(P)$ or $(p_1 p_2, q_1 q_2) \in N$, showing that N is closed under multiplication. Similar use of (3.17) and (3.18) shows the closure of N under the divisions. Thus N is a subquasigroup of $P \times Q$. Define congruences U, U' on N by

$$(p_1, q_1)\, U\, (p_2, q_2) \Leftrightarrow q_1 = q_2$$

and

$$(p_1, q_1)\, U'\, (p_2, q_2) \Leftrightarrow p_1 = p_2\,,$$

so that $N^U \cong P$ and $N^{U'} \cong Q$.

Define a relation V on N by

$$(p_1, q_1)\, V\, (p_2, q_2) \Leftrightarrow (p_1, q_1^t)\, W\, (p_2, q_2^t)\,.$$

Since W centers $\zeta(P)$ and t bijects, V is an equivalence relation on N with

$$V \cap U = V \cap U' = \widehat{N}, \quad V \circ U = V \circ U' = N^2.$$

Let $(p_1, q_1)\, V\, (p_1', q_1')$, $(p_2, q_2)\, V\, (p_2', q_2')$. Then

$$(p_1 \cdot p_2, q_1 t \cdot q_2 t)\, W\, (p_1' \cdot p_2', q_1' t \cdot q_2' t)\,,$$

since W is a congruence on $\zeta(P)$. Also,

$$\left(q_1 t \cdot q_2 t, (q_1 \cdot q_2)t\right) W\, (p', p)\, W\, \left(q_1' t \cdot q_2' t, (q_1' \cdot q_2')t\right)$$

by (3.15). Since W respects the transitivity of $\zeta(P)$,

$$\left(p_1 \cdot p_2, (q_1 \cdot q_2)t\right) W\, \left(p_1' \cdot p_2', (q_1' \cdot q_2')t\right)$$

or

$$(p_1 \cdot p_2, q_1 \cdot q_2)\, V\, (p_1' \cdot p_2', q_1' \cdot q_2')\,,$$

so that V is closed under multiplication. Similar use of (3.17) and (3.18) shows the closure of V under the divisions. The equivalence relation V on N becomes a congruence. Proposition 3.2 yields the interior isomorphisms of the chain

$$P \times N^V \cong N^U \times N^V \cong N \cong N^{U'} \times N^V \cong Q \times N^V$$

of isomorphisms. Finally, $N^V \cong \zeta(P)^W$ via $(p,q)^V \mapsto (p,qt)^W$, so that N^V is a central quasigroup Z by Lemma 3.2. □

Under appropriate finiteness conditions on the nonempty quasigroups P, Q, R involved, in particular if all are finite, one may in fact show that

$$P \times R \cong Q \times R \;\Rightarrow\; P \simeq Q \tag{3.25}$$

[147, 424]. For another application of central isotopy, see Exercise 5.

3.5 Central piques

Suppose that V is a central congruence on a nonempty quasigroup Q, with centering congruence W. By Lemma 3.2, the quotient $V/\widehat{Q}$ is a central quasigroup. It may be considered as a pique with $\widehat{Q}$ as the pointed idempotent. By Corollary 2.3 (p. 45), the cloop of this pique has a muliplication given by

$$(q_1,q_2)^W + (r_1,r_2)^W = \big((q_1,q_2)^W, \widehat{Q}, (r_1,r_2)^W\big)P\,.$$

Now by Corollary 3.4, and using the centering congruence Ω introduced in the proof of Lemma 3.2,

$$\big(\widehat{Q}, (r_1,r_2)^W\big)\,\Omega\,\big((q_1,q_2)^W, (q_1,q_2)^W + (r_1,r_2)^W\big)\,. \tag{3.26}$$

By the definition of Ω,

$$(q_1,q_2)^W + (r_1,r_2)^W = (q_1,q_3)^W,$$

where $(q_2,q_3)\,V\,(r_1,r_2)$. In particular, this means that the operation $+$ is associative: given $(q_1,q_2)^W, (r_1,r_2)^W, (s_1,s_2)^W$ in the quotient $V/\widehat{Q}$, take $(q_2,q_3)\,V\,(r_1,r_2)$ and $(q_3,q_4)\,V\,(s_1,s_2)$. Then

$$\begin{aligned}
\big((q_1,q_2)^W + (r_1,r_2)^W\big) + (s_1,s_2)^W &= (q_1,q_3)^W + (q_3,q_4)^W \\
&= (q_1,q_4)^W \\
&= (q_1,q_2)^W + (q_2,q_4)^W \\
&= (q_1,q_2)^W + \big((q_2,q_3)^W + (q_3,q_4)^W\big) \\
&= (q_1,q_2)^W + \big((r_1,r_2)^W + (s_1,s_2)^W\big)\,.
\end{aligned}$$

Thus the cloop of $V/\widehat{Q}$ is a group. It is an abelian group, since by Corollary 3.4

$$\begin{aligned}
(q_2,q_3)^W + (q_1,q_2)^W &= \big(q_1,(q_1,q_2,q_3)P\big)^W + \big((q_1,q_2,q_3)P,q_3\big)^W \\
&= (q_1,q_3)^W \\
&= (q_1,q_2)^W + (q_2,q_3)^W.
\end{aligned}$$

Further, the multiplications R and L are automorphisms of this abelian group, as is seen on multiplying (3.26) by the relation $(\widehat{Q},\widehat{Q})\,\Omega\,(\widehat{Q},\widehat{Q})$ and applying the fact that Ω is a congruence. Summarizing:

PROPOSITION 3.11
If V is a central congruence on a nonempty quasigroup Q, then the cloop $(V/\widehat{Q},+,\widehat{Q})$ of the pique $(V/\widehat{Q},\cdot,\widehat{Q})$ is an abelian group, with R and L as automorphisms.

The case of a central pique $(P,\cdot,e)$ is particularly interesting. Suppose that the congruence P^2 is centered by W. Then there is a pique isomorphism

$$P^2/\widehat{P} \to P; (e,p)^W \mapsto p. \tag{3.27}$$

By Proposition 3.11 it follows that the cloop $B(P)$ is an abelian group, for which the right and left multiplications R, L by the pointed idempotent are automorphisms. Since the inner multiplication group of the abelian group $B(P)$ is trivial, $\operatorname{Inn} P = \langle R, L\rangle$. The structure of the multiplication group of P is then specified as follows.

THEOREM 3.5
The multiplication group $\operatorname{Mlt} P$ *of a central pique P is the split extension of its abelian cloop $B(P)$ by the inner multiplication group* $\operatorname{Inn} P$.

PROOF The split extension $Q \ltimes M$ of an abelian group $(M,+)$ by a group Q of automorphisms is the set $\{(q,m) \mid q \in Q,\, m \in M\}$ of ordered pairs equipped with the product

$$(q_1,m_1)(q_2,m_2) = (q_1q_2, m_1q_2 + m_2)$$

for $q_1, q_2 \in Q$ and $m_1, m_2 \in M$ [compare (10.5)]. The map

$$\operatorname{Inn} P \ltimes B(P) \to \operatorname{Mlt} P; (w,p) \mapsto wR_+(p)$$

is a homomorphism, since

$$\begin{aligned} xw_1R_+(p_1)w_2R_+(p_2) &= (xw_1 + p_1)w_2 + p_2 \\ &= xw_1w_2 + (p_1w_2 + p_2) \\ &= x(w_1w_2)R_+(p_1w_2 + p_2) \end{aligned}$$

for x, p_1, p_2 in P and w_1, w_2 in $\operatorname{Inn} P$. The map bijects, since it has

$$\operatorname{Mlt} P \to \operatorname{Inn} P \ltimes B(P); \alpha \mapsto (\alpha R_+(e\alpha)^{-1}, e\alpha)$$

as a two-sided inverse. ∎

Conversely, given a module $(B, +, 0)$ for a group generated by two elements R, L, one may use (2.17) to define a pique $(B, \cdot, 0)$. It is easily checked that the subtraction mapping

$$- : B^2 \to B; (b, b') \mapsto b - b'$$

is a pique homomorphism whose kernel congruence has the diagonal $\widehat{B}$ as a congruence class. Thus $(B, \cdot, 0)$ is a central pique. In summary:

THEOREM 3.6
A pique $(P, \cdot, e)$ is central if and only if:

1. *The cloop $B(P)$ is an abelian group, and*
2. *$\operatorname{Inn} P$ is a group of automorphisms of $B(P)$.*

COROLLARY 3.7
The class of central piques forms a variety $\mathfrak{Z}_0$, defined relatively to the class of all piques by the following equations:

(a) $\Big(\big((x/0)(0\backslash y)\big)/0\Big)(0\backslash z) = (x/0)\Big(0\backslash\big((y/0)(0\backslash z)\big)\Big)$;

(b) $(x/0)(0\backslash y) = (y/0)(0\backslash x)$;

(c) $\big((x/0)(0\backslash y)\big)0 = (x0/0)(0\backslash y0)$;

(d) $0\big((x/0)(0\backslash y)\big) = (0x/0)(0\backslash 0y)$.

PROOF The identity (a) specifies the associativity of the cloop, while (b) gives its commutativity. The identities (c) and (d) state that the respective right and left multiplications by the pointed idempotent 0 are automorphisms of the cloop. □

3.6 Central quasigroups

If $(Q, \cdot)$ is a nonempty central quasigroup, the congruence Q^2 on Q is central. By Proposition 3.11, $(Q^2/\widehat{Q}, \cdot, \widehat{Q})$ is then a central pique.

PROPOSITION 3.12
Each nonempty central quasigroup Q is centrally isotopic to the corresponding central pique $(Q^2/\widehat{Q}, \cdot, \widehat{Q})$.

PROOF Suppose that W centers Q^2. Fix an element e of Q. (Of course, the element e need not be idempotent.) By analogy with (3.27), consider the map

$$t : Q^2/\widehat{Q} \to Q; (e, q)^W \mapsto q.$$

Since W centers Q^2, the map t bijects. It will be shown that t is a central shift. Consider general elements q_1, q_2 of Q. Define $q_3 = (e, e \cdot e, q_1 \cdot q_2)P$. On the one hand, Proposition 3.4 gives

$$(e, e \cdot e)\, W\, (q_3, q_1 \cdot q_2). \tag{3.28}$$

On the other hand, it gives

$$(e, q_3)\, W\, (e \cdot e, q_1 \cdot q_2),$$

so that $q_3 = (e, q_3)^W t = ((e, q_1)^W \cdot (e, q_2)^W)t$. The relation (3.28) then reads as

$$(e, e \cdot e)\, W\, (((e, q_1)^W \cdot (e, q_2)^W)t, (e, q_1)^W t \cdot (e, q_2)^W t),$$

showing that t is indeed a central shift. □

THEOREM 3.7

A nonempty quasigroup is central if and only if it is centrally isotopic to a central pique.

PROOF By Corollary 3.6, central isotopes of central piques are central quasigroups. The converse follows by Proposition 3.12. □

A further consequence stresses the way in which central isotopy of quasigroups is more significant than isomorphism.

THEOREM 3.8

Under the assignment $Q \mapsto Q^2/\widehat{Q}$, central isotopy classes of nonempty central quasigroups correspond exactly to isomorphism classes of central piques.

PROOF It remains to be shown that if two central piques are centrally isotopic, then they are isomorphic. Let $(Q, \cdot, e)$ and $(P, \cdot, f)$ be central piques with a central shift $t : Q \to P$. Let $(B(P), +, f)$ be the cloop of P. Then there is an element a of P such that (3.15) takes the form

$$(q_1 \cdot q_2)^t = q_1^t \cdot q_2^t + a$$

for q_1, q_2 in Q. Now

$$\begin{aligned}(q_1^t - e^t)\cdot(q_2^t - e^t) &= (q_1^t - e^t)R + (q_2^t - e^t)L \\ &= q_1^t R + q_2^t L - (e^t R + e^t L) \\ &= q_1^t \cdot q_2^t - (e^t \cdot e^t) \\ &= ((q_1 \cdot q_2)^t - e^t) - a + e^t - (e^t \cdot e^t),\end{aligned}$$

so that $s : Q \to P; q \mapsto q^t - e^t$ is also a central shift. But $e^s = e^t - e^t = f$, whence $(Q, \cdot)$ and $(P, \cdot)$ are isomorphic by Proposition 3.9, as required. □

The final result of this section concerns multiplication groups of central quasigroups.

THEOREM 3.9

Let G be the multiplication group of a central quasigroup Q. Then neither G nor its derived subgroup G' can be simple nonabelian.

PROOF By Propositions 3.10 and 3.12, it is sufficient to assume that Q is a pique with pointed idempotent e and inner multiplication group I. Then G certainly cannot be simple nonabelian, since $\mathrm{Mlt}\, B(Q) \triangleleft G$ by Theorem 3.5. By Theorem 3.6, the cloop $B(Q)$ is an I-module, and for the augmentation ideal $J = \sum_{h\in I}(h-1)\mathbb{Z}I$ of the integral group algebra of I, the submodule QJ is a subpique of Q. Now for x, q in Q and g in I,

$$xR_+\big(q(1-g)\big) = x + q - qg = \big((x+q)g^{-1} - q\big)g = x[R_+(-q), g].$$

Thus $\mathrm{Mlt}\, B(QJ)$ is a subgroup of G'. Indeed, since the cloop QJ is G-subset of Q, the abelian group $\mathrm{Mlt}\, B(QJ)$ is a normal subgroup of G'. If G' were to be simple nonabelian, $QJ = \{e\}$, so that I would act trivially on Q. By (2.17) this would yield the contradiction that Q is abelian and G' is trivial. □

3.7 Quasigroups of prime order

Throughout this section, let Q be a quasigroup of prime order p with multiplication group G. In this case the mutually exclusive possibilities Q central or G' simple nonabelian offered by Theorem 3.9 are the only ones.

PROPOSITION 3.13

Let Q be a quasigroup of prime order p with multiplication group G. Then either Q is central, or else G' is a simple nonabelian transitive permutation group on Q.

PROOF First assume that Q has an idempotent e, so that $(Q, \cdot, e)$ may be regarded as a pique. If Q is a cyclic group, it is certainly central. Otherwise $|G| > p$. Then G acts primitively on Q, whence G' acts transitively [83, Satz II.1.5]. If G' is not abelian, it is simple [83, V.21.1e]. Otherwise, G is solvable. If the cloop $B(Q)$ is abelian, than $\mathbb{Z}/p\mathbb{Z} \cong \operatorname{Mlt} B(Q) \leq G$. By Galois' theorem classifying solvable transitive permutation groups of prime degree [83, Satz II.3.6], G is similar to a group of affine transformations on the p-element field $\mathsf{GF}(p)$. Thus $G' = \operatorname{Mlt} B(Q)$ and $\operatorname{Inn} Q = \langle R, L \rangle$, with R and L as automorphisms of $B(Q)$. In this case Q is central. The other possibility, in which the loop $B(Q)$ is not abelian, leads to a contradiction. For then by Galois' theorem $\operatorname{Mlt} B(Q)$ on $B(Q)$ is itself similar to a group of affine transformations on $\mathsf{GF}(p)$. If x is an element of Q distinct from e with $R_+(x)$ lying in $(\operatorname{Mlt} B(Q))'$, then $R_+(x)$ is of order p, a p-cycle, and then $B(Q) = \langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$, a contradiction. Otherwise, $R_+(x)$ does not lie in $(\operatorname{Mlt} B(Q))'$, and thus has a fixed point y, i.e., $y + x = y$. But $y + e = y$ and $x \neq e$, a contradiction. The proposition is thus proved for quasigroups with idempotents.

Now suppose Q is a general quasigroup. If G' is not simple non-abelian, i.e. [83, Satz V.21.1e] if G is solvable, it must be shown that $(Q, \cdot)$ is central. Fix an element e of Q. If e is idempotent, the result follows as above. Otherwise, by Galois' theorem, G contains a cycle t of length p. Without loss of generality $(e \cdot e)t = e$: if this does not hold immediately, replace t by an appropriate power of itself. Define $(Q, \circ)$ by

$$x \circ y = (x \cdot y)t\,.$$

Then $(Q, \circ, e)$ is a pique. Now $t \in G$, so $\operatorname{Mlt}(Q, \circ) \leq G$. Thus $\operatorname{Mlt}(Q, \circ)$ is solvable, and so the pique $(Q, \circ, e)$ is central. Its cloop $(Q, +, e)$ is an abelian group, and so cyclic. In particular, there is an element b of Q with $L_+(b) = t^{-1}$. Then

$$\begin{aligned} x \cdot y &= (x \circ y)t^{-1} \\ &= b + x \circ y \\ &= (b, e.x \circ y)P, \end{aligned}$$

i.e. $(x \cdot y, x \circ y)\, W\, (b, e)$ for the congruence W centering Q^2 on $(Q, \circ)$. This shows that $(Q, \cdot)$ is a central isotope of the central quasigroup $(Q, \circ)$, and so by Corollary 3.6 is itself central. □

Using Burnside's Theorem [22][83, Satz V.21.3] that a transitive permutation group of prime degree is either solvable or doubly transitive, together with the classification of insolvable doubly transitive permutation groups of prime degree that is a corollary of the classification of finite simple groups [58, Cor. 4.2], one may apply Proposition 3.13 to obtain the following classification of quasigroups of prime order.

THEOREM 3.10
Let Q be a quasigroup of prime order p, with multiplication group G. Then one of the following holds:

(a) *Q is central;*

(b) *G is the alternating or symmetric group on Q;*

(c) *$p = 11$ and G is $\mathrm{PSL}_2(11)$ or M_{11};*

(d) *$p = 23$ and G is M_{23};*

(e) *$p = (q^k - 1)/(q - 1)$ for a prime power q and positive integer k, while $\mathrm{PSL}_k(q) \leq G \leq \mathrm{P\Gamma L}_k(q)$.*

REMARK 3.2 Vesanen [172] has shown that $\mathrm{PSL}_2(q)$ cannot be the multiplication group of a loop. On the other hand, for a 2-power q with $p = q + 1$ prime, the group $\mathrm{PSL}_2(q)$ has a subgroup $(Q, \oplus, 0)$ of order p generated by the so-called *Singer cycle* that projects from the automorphism of the vector space $\mathsf{GF}(q)^2$ corresponding to multiplication by a primitive element of the field $\mathsf{GF}(q^2)$ [83, Satz II.8.4a]. This subgroup acts regularly on the projective line $\mathsf{PG}(1, q)$, with which it may be identified. Letting S and T be the elements of $\mathrm{PSL}_2(q)$ corresponding to the respective fractional linear transformations $x \mapsto \frac{1}{x}$ and $x \mapsto x + 1$, one may then define a quasigroup multiplication on Q by

$$x \circ y = x^S \oplus y^T,$$

so that $R_\circ(-1) = S$ and $L_\circ(\infty) = T$. Since $\mathrm{PSL}_2(q)$ is generated by S and T [83, Aufg. II.14], one has $\mathrm{Mlt}(Q, \circ) = \mathrm{PSL}_2(q)$. □

3.8 Stability congruences

Related to the concept of centrality, based on the center congruence $\zeta(Q)$ of a quasigroup Q, there is also a concept of *stability*, based on a smaller congruence σ or $\sigma(Q)$ called the *stability congruence* and defined by

$$\sigma(Q) = \{(x, y) \in Q^2 \mid G_x = G_y\}. \tag{3.29}$$

In other words, two elements x, y of the quasigroup Q are related by the stability congruence if and only if their stabilizers G_x, G_y in the multiplication group G coincide. Now (3.29) is clearly an equivalence relation. Moreover, for $x, y \in Q$ and $g \in G$, one has

$$G_x = G_y \Rightarrow G_{xg} = G_x^g = G_y^g = G_{yg},$$

so $(x, y) \in \sigma(Q) \Rightarrow (xg, yg) \in \sigma(Q)$. Proposition 2.1 (p. 39) then shows that $\sigma(Q)$ is a congruence on Q.

PROPOSITION 3.14
Let Q be a quasigroup with multiplication group G.

(a) *The restriction of the map $\rho : Q^2 \to G$ to the stability congruence $\sigma(Q)$ is a quasigroup homomorphism $\rho : \sigma(Q) \to Z(G)$ into the center $Z = Z(G)$ of G.*

(b) *The stability congruence is contained in the center congruence.*

(c) *For each element e of Q, the normal subgroup $\sigma(Q)^\sharp$ of G determined by* (2.14) *may be expressed as* $\mathrm{Core}_G(G_e \cdot Z)$.

(d) *The normal subgroup $\sigma(Q)^\sharp$ of G is abelian.*

PROOF **(a)**: Let $q \in Q$ and $(x_i, y_i) \in \rho$ for $i = 1, 2$. Recall $1 = \rho(x_1x_2, x_1x_2) = \rho(x_1, x_2)$. Then $q = q\rho(x_1x_2, x_1x_2) = q\rho(x_1, x_2)$

$$
\begin{aligned}
&\Rightarrow x_2L(x_1)L(x_1x_2)^{-1}L(q/(x_1x_2\backslash x_1x_2)) = x_2L(x_2)^{-1}L(q/(x_2\backslash x_2))\\
&\Rightarrow y_2L(x_1)L(x_1x_2)^{-1}L(q/(x_1x_2\backslash x_1x_2)) = y_2L(x_2)^{-1}L(q/(x_2\backslash x_2))\\
&\Rightarrow (q/(x_1x_2\backslash x_1x_2))(x_1x_2\backslash x_1y_2) = (q\rho(x_1, x_1)/(x_2\backslash x_2))(x_2\backslash y_2)\\
&\Rightarrow x_1R(y_2)L(x_1x_2)^{-1}L(q/(x_1x_2\backslash x_1x_2))\\
&\qquad\qquad = x_1L(x_1)^{-1}L(q/(x_1\backslash x_1))R(x_2\backslash x_2)^{-1}R(x_2\backslash y_2)\\
&\Rightarrow y_1R(y_2)L(x_1x_2)^{-1}L(q/(x_1x_2\backslash x_1x_2))\\
&\qquad\qquad = y_1L(x_1)^{-1}L(q/(x_1\backslash x_1))R(x_2\backslash x_2)^{-1}R(x_2\backslash y_2)\\
&\Rightarrow q\rho(x_1x_2, y_1y_2) = q\rho(x_1, y_1)\rho(x_2, y_2).
\end{aligned}
$$

Thus $\rho : \sigma(Q) \to G$ is a quasigroup homomorphism. By (P7) of Proposition 2.6 (p. 44), ρ maps $\sigma(Q)$ into $Z(G)$.

(b): By (P3) of Proposition 2.6, the kernel of the quasigroup homomorphism $\rho : \sigma(Q) \to Z(G)$ is a congruence on $\sigma(Q)$ having the diagonal $\widehat{Q}$ as an equivalence class. Thus $\sigma(Q)$ is central, and by Corollary 3.3, $\sigma(Q) \leq \zeta(Q)$.

(c): For an element g of G, one has

$$
\begin{aligned}
&g \in \sigma(Q)^\sharp\\
&\quad \Leftrightarrow \forall\ q \in Q,\ G_q = G_{qg} = G_q^g\\
&\quad \Leftrightarrow \forall\ h \in G,\ G_{eh} = G_{eh}^g\\
&\quad \Leftrightarrow \forall\ h \in G,\ g \in N_G(G_eh) = N_G(G_e)^h\\
&\quad \Leftrightarrow g \in \mathrm{Core}(N_G(G_e)) = \mathrm{Core}(G_e \cdot Z),
\end{aligned}
$$

the last equality holding by Corollary 2.4 (p. 45).

(d): For $k, k' \in \sigma(Q)^\sharp$ and $(x, y) \in \sigma(Q)$, one has

$$xk = x\rho(x, xk) \Rightarrow k\rho(x, xk)^{-1} \in G_x = G_y \Rightarrow yk = y\rho(x, xk),$$

i.e. the restriction of k to $x^{\sigma(Q)}$ is $\rho(x, xk) = \rho(y, yk)$. Also

$$x\rho(x, xkk') = xkk' = xk\rho(xk, xkk') = xk\rho(x, xk') = x\rho(x, xk)\rho(x, xk'),$$

i.e. $\rho(x, xkk') = \rho(x, xk)\rho(x, xk')$ on $x^{\sigma(Q)}$. Consider a set $\{x_i \mid i \in Q^\sigma\}$ of representatives for the σ-classes. Then

$$f : \sigma(Q)^\sharp \to Z(G)^{Q^\sigma}; k \mapsto \big(\rho(x_i, x_i k) \mid i \in Q^\sigma\big)$$

embeds $\sigma(Q)^\sharp$ into an abelian group, a Cartesian power of $Z(G)$. □

For an element e of a quasigroup Q, Corollary 2.6 gives

$$e^{\sigma(Q)} = \{z \mid \forall\ q, r \in Q,\ zT_e(q) = zR_e(q, r) = zL_e(q, r) = z\}. \tag{3.30}$$

In particular, if e is the identity element of a loop Q, (3.30) reduces to

$$e^{\sigma(Q)} = \{z \mid \forall\ q, r \in Q,\ zq = qz, zq \cdot r = z \cdot qr, r \cdot qz = rq \cdot z\}, \tag{3.31}$$

the set of elements z commuting and associating with the rest of the loop. This is just the *center* of the loop as defined by Albert and Bruck [20].

PROPOSITION 3.15
In a loop Q, the stability congruence and center congruence coincide.

PROOF By Proposition 3.14(b), it remains to show that $\zeta(Q) \leq \sigma(Q)$. Suppose that z is in the $\zeta(Q)$-class of the identity element e of Q. Let W center $\zeta(Q)$. Then for $q, r \in Q$, one has

$$(e, z)\, W\, (e, z), (e, e)\, W\, (q, q), (e, e)\, W\, (r, r), (e, e)\, W\, (qr, qr),$$

the latter three relations from the respect of W for the reflexivity of $\zeta(Q)$. Now since W is a congruence,

$$\begin{aligned}(e, z) &= [(e, z)(e, e) \cdot (e, e)]/(e, e)\\ &\quad W\,[(e, z)(q, q) \cdot (r, r)]/(qr, qr) = (e, zR_e(q, r)).\end{aligned}$$

By (C1) for W, it follows that $z = zR_e(q, r)$. Similar arguments show $z = zT_e(q) = zL_e(q, r)$. Thus $e^{\zeta(Q)} \leq e^{\sigma(Q)}$. Since quasigroup congruences are determined by each of their classes, the desired containment $\zeta(Q) \leq \sigma(Q)$ follows. □

COROLLARY 3.8

For a loop Q with identity element e, the pique center $Z(Q) = e^{\zeta(Q)}$ is the loop center (3.31).

PROPOSITION 3.16

Let Q be a nonempty quasigroup with multiplication group G. Then the following conditions are equivalent:

(a) $\sigma(Q) = Q^2$;

(b) $\forall\ e \in Q,\ G_e \triangleleft G$;

(c) $\exists\ e \in Q,\ G_e \triangleleft G$;

(d) *G is abelian;*

(e) *Q is an abelian group.*

PROOF (a) $\Rightarrow$ (b): For e in Q and g in G, $(e, eg) \in \sigma(Q)$. Thus $G_e^g = G_{ge} = G_e$.

(b) $\Rightarrow$ (c): Immediate.

(c) $\Rightarrow$ (d): $G_e = \bigcap_{g\in G} G_{eg} = \{1\}$, since G is faithful on Q. Then by Corollary 2.4,

$$G = N_G(G_e) = G_e \cdot Z(G) = \{1\} \cdot Z(G) = Z(G)$$

is abelian.

(d) $\Rightarrow$ (e): Consider $q_1, q_2, q_3 \in Q$. Then $q_1q_2 \cdot q_3 = q_2L(q_1)R(q_3) = q_2R(q_3)L(q_1) = q_1 \cdot q_2q_3$, so that Q is associative, say with identity element 1. Then $q_1q_2 = 1R(q_1)R(q_2) = 1R(q_2)R(q_1) = q_2q_1$, so that Q is commutative.

(e) $\Rightarrow$ (a): $G_1 = \{1\} = G_x$ for all x in Q. ∎

COROLLARY 3.9

A quasigroup Q is abelian if and only if its multiplication group G is abelian.

By analogy with (3.14), set $\sigma_0(Q) = \widehat{Q}$, and inductively define

$$\sigma_{i+1}(Q) = \ker(\operatorname{nat}\sigma_i(Q) \operatorname{nat}\sigma(Q^{\sigma_i})). \tag{3.32}$$

Note that $\sigma_0 \leq \sigma_1 \leq \sigma_2 \leq \ldots$. If there is a minimal natural number d such that $\sigma_d(Q) = Q^2$, then Q is said to be *stably nilpotent*, of *stable nilpotence class d*. If d is positive, then

$$\widehat{Q} = \sigma_0 < \sigma = \sigma_1 < \sigma_2 \cdots < \sigma_d = Q^2$$

is a central series in Q called the *upper stability series* or *ascending stability series* of Q. For loops, Proposition 3.15 shows that stable nilpotence and (central) nilpotence coincide. Proposition 3.16 shows that nonempty quasigroups of stable nilpotence class at most 1 are just abelian groups.

PROPOSITION 3.17
A nonempty stably nilpotent quasigroup contains a unique idempotent.

PROOF Work by induction on the stable nilpotence class d of a nonempty stably nilpotent quasigroup Q, the induction basis being the trivial case $d = 0$. Suppose the result is true for stably nilpotent quasigroups of class less than d, for positive d. Then $Q^{\sigma(Q)}$ is of stable nilpotence class $d-1$, and so $\sigma(Q)$ has a unique congruence class E that is a subquasigroup of Q. Now

$$E^2 = \sigma(Q) \cap E^2 = \zeta(Q) \cap E^2 \leq \zeta(E),$$

the containment holding by Proposition 3.5(2). Thus $\widehat{E} \lhd E^2$, and by (C1) for $\sigma(Q)$, there is an isomorphism $E^2/\widehat{E} \cong \sigma(Q)/\widehat{Q}$. By the First Isomorphism Theorem applied to the homomorphism ρ of Proposition 3.14(1), the latter quotient is an abelian group. By Proposition 3.12, E is centrally isotopic to the abelian group $E^2/\widehat{E}$, and thus is itself an abelian group. As such, it has a unique idempotent. If e is an idempotent of Q, then the σ-class of e is a subquasigroup of Q, and so coincides with E. Thus the unique idempotent of E is the unique idempotent of Q. □

Proposition 3.16 shows how the normality of stabilizers in the multiplication group corresponds to abelianness of the quasigroup. The next theorem extends this result by showing that subnormality of stabilizers corresponds to stable nilpotence. Recall that a subgroup H of a group G is said to be *subnormal* in G if there is a finite chain

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_d = G \tag{3.33}$$

of subgroups H_i of G, each normal in the next. The least natural number d for which (3.33) holds is called the *subnormal depth* of H in G.

THEOREM 3.11
Let G be the multiplication group of a nonempty quasigroup Q. Then Q is stably nilpotent if and only if, for each element e of Q, the stabilizer G_e is subnormal in G. If these equivalent conditions hold, then the subnormal depth of each stabilizer is equal to the stable nilpotence class of Q.

PROOF For e in Q and $Z = Z(G)$, one has

$$G_e Z \leq G_e \cdot \mathrm{Core}_G(G_e \cdot Z) \leq G_e \cdot Z,$$

so that $G_e \cdot Z = G_e \cdot \mathrm{Core}_G(G_e \cdot Z)$. Then by Proposition 3.14,

$$\big(\mathrm{Mlt}(Q^\sigma)\big)_{e^\sigma} = \frac{G_e\sigma^\sharp}{\sigma^\sharp} = \frac{G_e \cdot \mathrm{Core}_G(G_e \cdot Z)}{\mathrm{Core}_G(G_e \cdot Z)} = \frac{G_e \cdot Z}{\mathrm{Core}_G(G_e \cdot Z)}. \tag{3.34}$$

Suppose Q is stably nilpotent of class $d > 1$. Then Q^σ is stably nilpotent of class $d-1$, so by induction on the stable nilpotence class $\big(\mathrm{Mlt}(Q^\sigma)\big)_{e^\sigma}$ is subnormal in $\mathrm{Mlt}(Q^\sigma)$, of depth $d-1$. By (3.34) and Corollary 2.4 (p. 45), this means that $G_e \cdot Z = N_G(G_e)$ is subnormal in $\mathrm{Mlt}(Q^\sigma)$ of depth $d-1$, whence G_e is subnormal in G of depth d. Conversely, suppose G_e is of subnormal depth d in G. Then $N_G(G_e) = G_e \cdot Z$ is of subnormal depth $d-1$ in G, whence by (3.34) the group $\big(\mathrm{Mlt}(Q^\sigma)\big)_{e^\sigma}$ is of subnormal depth $d-1$ in $\mathrm{Mlt}(Q^\sigma)$. By induction on the subnormal depth of stabilizers it follows that Q^σ is stably nilpotent of class $d-1$, so Q is stably nilpotent of depth d. □

There is no direct analogue of Corollary 3.9 to accompany Theorem 3.11, but the following two results here go some way in this direction.

COROLLARY 3.10
If the multiplication group of a finite quasigroup is nilpotent, then the quasigroup is stably nilpotent.

PROOF Subgroups of finite nilpotent groups are subnormal. □

PROPOSITION 3.18
The multiplication group of a stably nilpotent quasigroup Q is solvable.

PROOF By induction on the stable nilpotence class of Q, the group

$$\mathrm{Mlt}(Q^\sigma) \cong \mathrm{Mlt}\, Q \big/ \sigma^\sharp$$

is solvable. Then by Proposition 3.14(4), $\sigma^\sharp$ is abelian, so $\mathrm{Mlt}\, Q$ itself is solvable. □

3.9 No-go theorems

The possibility of representing abstract groups as multiplication groups, or of representing permutation group actions as multiplication group actions, raises the question as to which abstract groups or group actions possess such a representation. Example 2.2 (p. 37) gave a taste of the benefits that may ensue from a multiplication group representation. Since it appears that many

groups or actions do admit such representations, interest attaches to so-called "no-go" theorems showing that certain classes of groups or actions cannot arise as multiplication groups. This section presents a small sample of such no-go theorems. As illustrated in Remark 3.2 above, requiring the quasigroup to lie in a special class (such as the class of loops) may impose further restrictions.

A group is said to be *Hamiltonian* if it is not abelian, but nevertheless has each of its subgroups normal. Dedekind identified the finite groups of this type as direct products of the quaternion group of order 8 with an abelian group of odd order and an abelian group of exponent 2 [83, Satz III.7.12].

PROPOSITION 3.19

No Hamiltonian group can be the multiplication group of a quasigroup.

PROOF Suppose that a Hamiltonian group G is the multiplication group of a quasigroup Q. Since the stabilizers of elements of Q are normal subgroups of G, Proposition 3.16 shows that Q is abelian. But then Corollary 3.9 implies the contradiction that G is abelian. □

There is a further class of infinite groups which may be shown not to be multiplication groups. These are the so-called *Heineken-Mohamed* groups satisfying the normalizer condition that proper subgroups are properly contained in their normalizers, but nevertheless having trivial center [75] [76] [77] [112]. (By [83, Hauptsatz III.2.3], there are no finite groups with trivial center satisfying the normalizer condition.)

PROPOSITION 3.20

No Heineken-Mohamed group can be the multiplication group of a quasigroup.

PROOF Suppose that a Heineken-Mohamed group G is the multiplication group of a quasigroup Q. Since G is infinite, so is Q. Let e be an element of Q. Since $Z(G)$ is trivial, Corollary 2.4 (p. 45) shows that $G_e = N_G(G_e)$. By the normalizer condition, it follows that $G_e = G$, giving the contradiction $Q = \{e\}$ to the infiniteness of Q. □

A group H of permutations of a set X is said to be *quasiprimitive* if each nontrivial normal subgroup of H acts transitively on X [131] [132]. The following result is analogous to Corollary 2.1 (p. 39).

PROPOSITION 3.21

A quasigroup Q is simple if and only if its combinatorial multiplication group G acts quasiprimitively on Q.

PROOF Recall that for a nontrivial congruence V on a quasigroup Q, the normal subgroup $V^\sharp$ of G, as the kernel of (2.11), is nontrivial. If Q is not simple, having a proper, nontrivial congruence V, then $V^\sharp$ is not transitive, so that G is not quasiprimitive. Conversely, suppose that G is not quasiprimitive, having a nontrivial normal subgroup N that is not transitive. Then $N^\flat$ is a proper, nontrivial congruence on Q, so that Q is not simple. □

COROLLARY 3.11
An imprimitive, quasiprimitive group action cannot be a multiplication group action.

PROOF If the quasiprimitive action were a multiplication group action, then the quasigroup would be simple by Proposition 3.21. But then the action would be primitive, by Corollary 2.1. □

Examples of imprimitive, quasiprimitive actions were given in [131].

3.10 Exercises

1. Let P be a nonempty subquasigroup of an entropic quasigroup Q.

   (a) For each element q of Q, define

   $$qP = \{qp \mid p \in P\}.$$

   Then define Q/P to be the set

   $$\{qP \mid q \in Q\}.$$

   Show that Q/P is a quasigroup under a well-defined multiplication

   $$q_1P \cdot q_2P = (q_1q_2)P.$$

   (b) Show that the map

   $$Q \to Q/P; q \mapsto qP$$

   is a quasigroup homomorphism.

   (c) Show that P is a normal subquasigroup of Q.

2. Show that entropic quasigroups are central.

3. Show that a central pique is entropic if and only if its inner multiplication group is abelian.

4. (a) Show that a central isotope of an entropic quasigroup is entropic.
   (b) Exhibit an isotope P of an entropic quasigroup Q such that the quasigroup P is not central.

5. (a) [111] Let c be an element of the center of a commutative Moufang loop $(L, +, 1)$. Show that $G_c(L, +, 1) = (L, \cdot)$ with $x \cdot y = c - x - y$ is a CH-quasigroup. (Compare Exercise 24 of Chapter 1.)
   (b) [147] Let c and d be central elements of a commutative Moufang loop $(L, +, 1)$. Show that the CH-quasigroups $G_c(Q, +, 1)$ and $G_d(Q, +, 1)$ are centrally isotopic.
   (c) [147] Let $(Q, \cdot)$ be a nonempty CH-quasigroup. Show that each central isotope of $(Q, \cdot)$ is of the form $G_d F_e(Q, \cdot)$ for each element e of Q and for a suitable central element d of $F_e(Q, \cdot)$.

6. Let N be a set equipped with three equivalence relations V_1, V_2, V_3 such that
$$\forall\, 1 \leq i \neq j \leq 3\,,\ V_i \cap V_j = \widehat{N} \text{ and } V_i \circ V_j = N^2$$
[using the relation product (3.2)].
   (a) Show that the cardinality of N is a perfect square.
   (b) Show that (N, V_1, V_2, V_3) is the 3-net of a quasigroup Q.

7. Let V be a congruence on a quasigroup Q.
   (a) For y, z in Q, show that the map $\rho(y, z)$ of (2.26) is a bijection from y^V to z^V.
   (b) Show that V is uniquely determined by any one of its classes.
   (c) If Q is finite, with element x, show that $|x^V|$ divides $|Q|$.

8. [99] Show that a quasigroup Q is a union of three proper normal subquasigroups whose common intersection is nonempty if and only if the noncyclic group of order 4 is a quotient of Q.

9. [165, Prop. I.2.4.6] Let P be a nonempty subquasigroup of a quasigroup Q with combinatorial multiplication group G. Show that the following conditions on P are equivalent:
   (a) $P \lhd Q$;
   (b) $\forall\, e \in P\,,\ PG_e = P$;
   (c) $\exists\, e \in P\,.\, PG_e \subseteq P$.

10. [87] Let e be an element of a subset P of a quasigroup Q. Show that P is the class of a congruence on Q if and only if:

    (a) $PG_e \subseteq P$, and

    (b) For elements a, b, c of Q, whenever $(a/e)b = c$ and two of a, b, c lie in P, then so does the third.

11. [10] Show that a nonempty subset P of a quasigroup Q is the class of a congruence on Q if and only if the following elements of Q lie in P for all p_1, p_2, p_3 in P and q_1, q_2 in Q:

$$\begin{cases} p_1 \cdot (p_2 \backslash p_3)\,; \\ p_1 / (p_1 \backslash p_3)\,; \\ \Big(q_1 \cdot q_2\Big) \Big/ \Big(p_3 \Big\backslash \big(p_3(p_1 \backslash q_1) \cdot p_3(p_2 \backslash q_2)\big)\Big)\,; \\ \Big(q_1 / q_2\Big) \Big/ \Big(p_3 \Big\backslash \big(p_3(p_1 \backslash q_1) / p_3(p_2 \backslash q_2)\big)\Big)\,; \\ \Big(q_1 \backslash q_2\Big) \Big/ \Big(p_3 \Big\backslash \big(p_3(p_1 \backslash q_1) \backslash p_3(p_2 \backslash q_2)\big)\Big)\,. \end{cases}$$

12. Show that a quasigroup of prime order is simple.

13. Is it possible for a nontrivial, nonsimple quasigroup to be devoid of proper, nontrivial normal subquasigroups?

14. (a) Show that a quasigroup Q is central if and only if, for all elements x, y, z, t, u, v of Q, one has:

$$\begin{cases} (x,x)T_{(y,y)}\big((z,u)\big) \in \widehat{Q}\,; \\ (x,x)R_{(y,y)}\big((z,u),(t,v)\big) \in \widehat{Q}\,; \\ (x,x)L_{(y,y)}\big((z,u),(t,v)\big) \in \widehat{Q}\,. \end{cases}$$

    (b) Show that a quasigroup Q is central if and only if it satisfies the identities:

$$\begin{cases} xT_y(z) = xT_y(u)\,; \\ xR_y(z,t) = xR_y(u,v)\,; \\ xL_y(z,t) = xL_y(u,v)\,. \end{cases}$$

    (c) Show that a quasigroup Q is central if and only if it satisfies the identities:

$$\begin{cases} xT_y(z) = xT_y(y)\,; \\ xR_y(z,t) = xR_y(y,y)\,; \\ xL_y(z,t) = xL_y(y,y)\,. \end{cases}$$

15. [47] Show that a nonempty quasigroup is an isotope of an abelian group if and only if it satisfies the identity

$$(ux/v)y = (uy/v)x\,. \tag{3.35}$$

[Hint: If e is an element of a quasigroup satisfying (3.35), show that $(x, y) \mapsto (x/e) \cdot (e\backslash y)$ defines an abelian group operation with identity ee.]

16. [47] Show that a quasigroup Q is central if and only if it satisfies the identities:

$$\begin{cases} (ux/v)y = (uy/v)x\,; \\ (y.xz)/(xy) = (y.yz)/(yy)\,; \\ (yx)\backslash(zx.y) = (yy)\backslash(zy.y)\,. \end{cases}$$

17. [147, p. 29] Let U and V be congruences on a quasigroup Q.

    (a) Show that if U centralizes V, then V centralizes U.

    (b) Conclude that V on Q is central if and only if it centralizes Q^2.

18. [147, Cor. 227] Let V be a congruence on a quasigroup Q.

    (a) Show that if U_1 and U_2 centralize V, then so does their relation product $U = U_1 \circ U_2$.

    (b) Conclude that there is a unique maximal congruence $\eta(V)$ on Q centralizing V. The congruence $\eta(V)$ is called the *centralizer* of V.

    (c) Show that $\zeta(Q) = \eta(Q^2)$.

19. [147, p. 39] Let U and V be congruences on a quasigroup Q.

    (a) If U centralizes V, show that $U \circ V$ centralizes $U \cap V$.

    (b) Conclude that $V \circ \eta(V)$ centralizes $V \cap \eta(V)$.

20. Define a multiplication $x \circ y = x^{(12)} + y + 1$ on $\mathbb{Z}/n\mathbb{Z}$ for $n > 2$. (Here (12) denotes the transposition of the classes 1 and 2 in cycle notation.) Show that $(\mathbb{Z}/n\mathbb{Z}, \circ)$ is a quasigroup whose multiplication group is the symmetric group S_n of degree n.

21. Define a multiplication $x \circ y = x^{(123)} + y^{(34\ldots n)}$ on $\mathbb{Z}/n\mathbb{Z}$ for odd $n > 3$. Show that $(\mathbb{Z}/n\mathbb{Z}, \circ)$ is a quasigroup whose multiplication group is the alternating group A_n of degree n.

22. [113, Th. 12] Let G be a finite group. Show that there is a finite Steiner triple system Q such that G is the group of automorphisms of Q.

3.11 Notes

Section 3.3

The concept of nilpotence for quasigroups presented here goes back to [147]. It generalizes Bruck's concept of "central nilpotence" for loops [20], [21]. These concepts specialize to the usual notions of nilpotence for groups.

Section 3.4

A slightly different definition of central isotopy was used in [28, §III.4]. Lemma 3.1 gives the equivalence of that definition with the simpler one used here.

Section 3.7

Albert [2, §14] classified quasigroups of order 5. Theorem 3.10 was published as [28, Th. III.5.10] after circulating for about ten years. For further discussion of examples such as that of Remark 3.2, see [84].

Section 3.8

Bruck [20, Corollaries 1.8B II,III] proved Corollary 3.10 and Proposition 3.18 for the case of loops. (Recall the remark preceding Proposition 3.17.)

Section 3.9

Corollary 3.11 appeared in [127].

In contrast to the no-go theorems for multiplication groups, E. Mendelsohn [113, Th. 12] showed that each finite group is the automorphism group of a finite quasigroup — compare Exercise 22. Pigozzi and Sichler showed that each infinite group is the automorphism group of each member of a proper class of (mutually nonisomorphic) infinite quasigroups [129].

Chapter 4

HOMOGENEOUS SPACES

A subquasigroup P of a quasigroup Q determines a homogeneous space $P\backslash Q$. This space is defined as the set of orbits on Q of the relative left multiplication group of the subquasigroup P. If P is a subgroup of a group Q, then $P\backslash Q$ is just the set (2.10) of cosets of P in Q, and the group Q acts on $P\backslash Q$ by permutations specified by permutation matrices (Corollary 4.3). For a general quasigroup Q with subquasigroup P, there is an analogous action of elements of Q on $P\backslash Q$ by Markov matrices (4.14), the action being probabilistic rather than combinatorial.

In mathematics, exact symmetry is understood conceptually as the action of a group. For example, the symmetry of a square corresponds to the permutation action of the dihedral group $\mathrm{Mlt}(\mathbb{Z}/4\mathbb{Z}, -, 0)$ on the cosets of the subgroup $\mathrm{Inn}(\mathbb{Z}/4\mathbb{Z}, -, 0)$ — compare Example 2.2 and Section 2.4. Section 4.2 shows how the action of a quasigroup on one of its homogeneous spaces may be understood as an example of approximate symmetry, so-called macroscopic symmetry. The general version of this symmetry (for a finite quasigroup) is studied in Section 4.3.

Section 4.4 considers regular homogeneous spaces, in which a quasigroup acts on its own underlying set. The concluding Section 4.5 applies quasigroup homogeneous spaces in a new approach to issues concerning the breakdown of Lagrange's Theorem for quasigroups.

4.1 Quasigroup homogeneous spaces

Let P be a subgroup of a group Q. The permutation representation of Q on the homogeneous coset space $P\backslash Q$ is given by the actions

$$R_{P\backslash Q}(q) : P\backslash Q \to P\backslash Q\,;\, Px \mapsto Pxq \tag{4.1}$$

for elements q of Q. For a quasigroup Q, the construction of homogeneous space actions depends on a concept from linear algebra. For a matrix A over the complex numbers, let A^+ be the pseudoinverse or "(Moore-)Penrose

inverse." This is the unique (Exercise 1) matrix A^+ satisfying the equations

$$AA^+A = A\ , \tag{4.2}$$
$$A^+AA^+ = A^+, \tag{4.3}$$
$$(A^+A)^* = A^+A, \tag{4.4}$$
$$(AA^+)^* = AA^+, \tag{4.5}$$

in which the * denotes the conjugate transpose.

PROPOSITION 4.1
Let $\varphi : X \to Y$ be a surjective function defined on a finite set X. Let F be the incidence matrix of φ, the $X \times Y$-matrix with

$$F_{xy} = \begin{cases} 1 & \textit{for} \quad x\varphi = y\,; \\ 0 & \textit{otherwise}\,. \end{cases}$$

Then the pseudoinverse F^+ of F is given by

$$F^+_{yx} = \begin{cases} |\varphi^{-1}\{y\}|^{-1} & \textit{for} \quad x\varphi = y\,; \\ 0 & \textit{otherwise}\,. \end{cases}$$

PROOF Throughout the proof, matrix suffices x and x' will correspond to elements of X, while suffices y and y' will correspond to elements of Y. The equations (4.2) through (4.5) have to be verified. For (4.2) and (4.3), consideration of the relationship

$$x \in \varphi^{-1}\{y'\} \ni x' \in \varphi^{-1}\{y\} \tag{4.6}$$

will be critical. For fixed x in $\varphi^{-1}\{y'\}$ and x' in $\varphi^{-1}\{y\}$, note that (4.6) can hold only if $y = y'$, and that it will then hold for each of the $|\varphi^{-1}\{y\}|$ elements x' of $\varphi^{-1}\{y\}$.

(4.2) For $x \in X$ and $y \in Y$, consider the equation

$$(FF^+F)_{xy} = \sum_{y' \in Y} \sum_{x' \in X} F_{xy'} F^+_{y'x'} F_{x'y}\ . \tag{4.7}$$

A summand on the right-hand side is nonzero precisely when (4.6) holds. For $x \notin \varphi^{-1}\{y\}$, there are no such summands, so $(FF^+F)_{xy}$ takes the value zero of F_{xy} for this case. On the other hand, if $x \in \varphi^{-1}\{y\}$, then each of the $|\varphi^{-1}\{y\}|$ nonzero summands in (4.7) is $|\varphi^{-1}\{y\}|^{-1}$, so that the sum yielding $(FF^+F)_{xy}$ agrees with the value of F_{xy} (namely 1) for this case as well.

(4.3) For $x \in X$ and $y \in Y$, consider the equation

$$(F^+FF^+)_{yx} = \sum_{x' \in X} \sum_{y' \in Y} F^+_{yx'} F_{x'y'} F^+_{y'x}\ . \tag{4.8}$$

A summand on the right-hand side of (4.8) is nonzero precisely when (4.6) holds. For $x \notin \varphi^{-1}\{y\}$, there are no such summands, so $(F^+FF^+)_{yx}$ takes the value zero of F^+_{yx} for this case. On the other hand, if $x \in \varphi^{-1}\{y\}$, then each of the $|\varphi^{-1}\{y\}|$ nonzero summands in (4.8) is $|\varphi^{-1}\{y\}|^{-2}$, so that the sum yielding $(F^+FF^+)_{yx}$ agrees with the value of F^+_{yx} (namely $|\varphi^{-1}\{y\}|^{-1}$) for this case as well.

(4.4) For y and y' in Y, consider the equation

$$(F^+F)_{yy'} = \sum_{x' \in X} F^+_{yx'} F_{x'y'} \ .$$

Here, the relation

$$\varphi^{-1}\{y\} \ni x' \in \varphi^{-1}\{y'\} \ , \tag{4.9}$$

holding only if $y = y'$, and then precisely for each of the $|\varphi^{-1}\{y\}|$ elements x' of $\varphi^{-1}\{y\}$, is critical. If (4.9) holds, then $F^+_{yx'} F_{x'y'}$ takes the value $|\varphi^{-1}\{y\}|^{-1}$. Thus

$$(F^+F)_{yy'} = \delta_{yy'} \ , \tag{4.10}$$

from which (4.4) follows.

(4.5) For x and x' in X, consider the equation

$$(FF^+)_{xx'} = \sum_{y \in Y} F_{xy} F^+_{yx'} \ . \tag{4.11}$$

Note that a summand $F_{xy}F^+_{yx'}$ of (4.11) is nonzero if and only if both x and x' lie in $\varphi^{-1}\{y\}$, in which case the nonzero value is the real number $|\varphi^{-1}\{y\}|^{-1}$. Since the kernel of φ is a symmetrical relation on X, Equation (4.5) holds. □

COROLLARY 4.1

By (4.10)*, it follows that*

$$F^+F = I_Y \ , \tag{4.12}$$

the identity matrix of size $|Y|$.

Now let P be a subquasigroup of a finite quasigroup Q. Let $P\backslash Q$ denote the set of orbits of the permutation group $\mathrm{LMlt}_Q P$ on the set Q. Let A_P or A be the incidence matrix of the membership relation between the set Q and the set $P\backslash Q$ of subsets of Q. Thus A is a $|Q| \times |P\backslash Q|$ matrix, with rows indexed by the elements x of Q and columns indexed by the elements X of $P\backslash Q$, such that the (x, X)-entry of the matrix is 1 if $x \in X$, and zero otherwise. The matrix A is the incidence matrix of the surjective projection function

$$Q \to P\backslash Q; x \mapsto x\mathrm{LMlt}_Q P \, .$$

By Proposition 4.1, the pseudoinverse A^+_P or A^+ of the incidence matrix A_P or A is the $|P\backslash Q| \times |Q|$ matrix whose entry A^+_{Xx} in the row indexed by the

$\mathrm{LMlt}_Q P$-orbit X and in the column indexed by the Q-element x is given by

$$A^+_{Xx} = \begin{cases} |X|^{-1} & \text{if } x \in X\,; \\ 0 & \text{otherwise}\,. \end{cases} \tag{4.13}$$

For each element q of Q, the right multiplication $R_Q(q)$ in Q by q yields a permutation of Q. Let $R_Q(q)$ also denote the corresponding $|Q|\times|Q|$ permutation matrix.

DEFINITION 4.1 *Let P be a subquasigroup of a finite quasigroup Q.*

(a) *The* action matrix *or* transition matrix *or* Markov matrix *of an element q of Q on the set $P\backslash Q$ is defined to be the $|P\backslash Q| \times |P\backslash Q|$ matrix*

$$R_{P\backslash Q}(q) = A^+_P R_Q(q) A_P\,. \tag{4.14}$$

(b) *The* homogeneous space *$P\backslash Q$ or $(P\backslash Q, Q)$ is understood as the set $P\backslash Q$ together with the map*

$$q \mapsto R_{P\backslash Q}(q)$$

assigning an action matrix to each element of the quasigroup Q.

(c) *The* total matrix *of the homogeneous space $P\backslash Q$ is defined to be the $|P\backslash Q| \times |P\backslash Q|$ matrix*

$$\sum_{q\in Q} R_{P\backslash Q}(q)\,. \tag{4.15}$$

(d) *The* Markov matrix *of the homogeneous space $P\backslash Q$ is a $|P\backslash Q| \times |P\backslash Q|$ matrix. For nonempty Q, it is given by*

$$\frac{1}{|Q|} \sum_{q\in Q} R_{P\backslash Q}(q)\,. \tag{4.16}$$

LEMMA 4.1
The total matrix (4.15) *of the homogeneous space $P\backslash Q$ may be written as*

$$A^+_P J A_P\,, \tag{4.17}$$

where J denotes the $|P\backslash Q| \times |P\backslash Q|$ all-ones matrix.

PROOF For given x, y in Q, there is a unique element $q = x\backslash y$ of Q such that $y = xq$ (compare Exercise 7 of Chapter 2). Thus

$$\sum_{q\in Q} R_Q(q) = J\,.$$

The result then follows from (4.14). □

Recall that a matrix is *stochastic* if its entries are all nonnegative real numbers, and each of its row sums is 1.

COROLLARY 4.2

Let $P_1, \dots, P_r$ be the orbits of the relative left multiplication group of P in Q.

(a) Each row of the total matrix of $P\backslash Q$ takes the form

$$[\,|P_1|, \dots, |P_r|\,]\,. \tag{4.18}$$

(b) Each row of the Markov matrix of $P\backslash Q$ takes the form

$$\Big[\,\frac{|P_1|}{|Q|}, \dots, \frac{|P_r|}{|Q|}\,\Big]\,. \tag{4.19}$$

In particular, the matrix is stochastic.

PROOF Let X and Y be orbits of the relative left multiplication group of P in Q. By (4.17), the XY-entry of the total matrix is

$$[A^+JA]_{XY} = \sum_{x,y\in Q} A^+_{Xx} J_{xy} A_{yY} = \sum_{x,y\in Q} A^+_{Xx} A_{yY}\,.$$

By (4.13), this reduces to

$$\sum_{x\in X} \sum_{y\in Y} |X|^{-1} \cdot 1 = |Y|\,,$$

as required for (4.18). Equation (4.19) follows. □

THEOREM 4.1

For each element q of Q, Definition 4.1(*a*) *yields a Markov chain with transition matrix $R_{P\backslash Q}(q)$ on the state space $P\backslash Q$ of orbits of the permutation group* $\mathrm{LMlt}_Q P$ *on the set Q. The probability of transition from an orbit X to an orbit Y is given as*

$$\frac{|X \cap R(q)^{-1}(Y)|}{|X|}\,. \tag{4.20}$$

PROOF By (4.14), one has

$$\begin{aligned}
[R_{P\backslash Q}(q)]_{XY} &= \sum_{x\in Q}\sum_{y\in Q} A^{+}_{Xx} R(q)_{xy} A_{yY} \\
&= \sum_{x\in Q} A^{+}_{Xx} A_{(xq)Y} \\
&= \sum_{x\in X} A^{+}_{Xx} A_{(xq)Y} \\
&= |X|^{-1} |\{x \mid x \in X,\ xq \in Y\}| \\
&= \frac{|X \cap R(q)^{-1}(Y)|}{|X|}
\end{aligned}$$

giving (4.20). Moreover, summing (4.20) over all elements Y of $P\backslash Q$ yields the value 1. □

COROLLARY 4.3

In the group case, the matrix (4.14) *is just the permutation matrix given by the permutation* (4.1).

PROOF In this case, the numerator of (4.20) is $|X|$ if $XR(q) = Y$, and zero otherwise. □

4.2 Approximate symmetry

This section examines a specific example of the action of a quasigroup on one of its homogeneous spaces, and shows how the action may be interpreted as an instance of approximate symmetry. Consider the quasigroup Q whose multiplication table is displayed in Figure 1.2. Let P be the singleton subquasigroup $\{1\}$. Note that $\mathrm{LMlt}_Q P$ is the cyclic subgroup of $Q!$ generated by (23)(456). Thus

$$P\backslash Q = \big\{\{1\}, \{2,3\}, \{4,5,6\}\big\}, \tag{4.21}$$

yielding

$$A_P = \begin{bmatrix} 1&0&0 \\ 0&1&0 \\ 0&1&0 \\ 0&0&1 \\ 0&0&1 \\ 0&0&1 \end{bmatrix} \quad \text{and} \quad A_P^{+} = \begin{bmatrix} 1&0&0&0&0&0 \\ 0&\frac{1}{2}&\frac{1}{2}&0&0&0 \\ 0&0&0&\frac{1}{3}&\frac{1}{3}&\frac{1}{3} \end{bmatrix}.$$

Now (4.14) gives

$$R_{P\backslash Q}(5) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix} . \tag{4.22}$$

One may view this Markov chain action graphically according to Figure 4.1. Denote the elements of the state space $P\backslash Q$, the orbits of $\mathrm{LMlt}_Q P$ on Q, respectively as

$$\begin{aligned} a &= \{1\}, \\ a' &= \{2, 3\}, \\ b &= \{4, 5, 6\} . \end{aligned}$$

The incidence matrix A_P, giving the assignment of quasigroup elements to state space elements, is represented by the right-hand side of the figure. The permutation $R_Q(5)$ of Q is represented in the center of the figure. The left-hand side represents the pseudoinverse A_P^+. In the Markov chain, each element of the state space on the left of the figure has a uniform chance of transitioning along each of the arrows leading from it. After that, its path through Q and back to the state space $P\backslash Q$ is uniquely specified, according to the matrix $R_{P\backslash Q}(5)$. For example, the element b has a two-thirds chance of transitioning to a', and a one-third chance of transitioning to a.

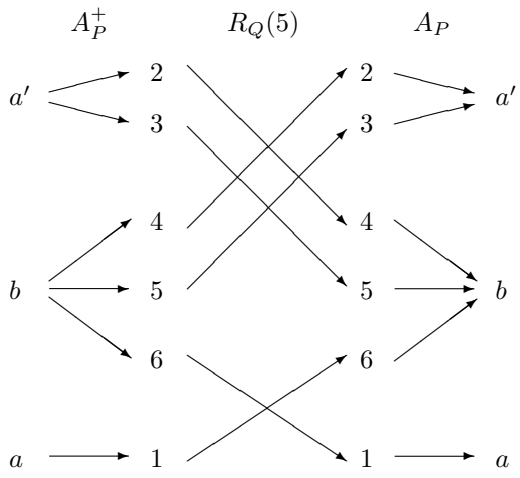


FIGURE 4.1: The Markov chain $R_{P\backslash Q}(5)$.

In order to study the action of the full quasigroup Q on $P\backslash Q$, define Markov matrices

$$\iota = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad , \quad \varepsilon = \begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \tau = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix} \quad . \tag{4.23}$$

Note that

$$R_{P\backslash Q}(1) = \iota, \qquad R_{P\backslash Q}(2) = R_{P\backslash Q}(3) = \varepsilon\,,$$

and

$$R_{P\backslash Q}(4) = R_{P\backslash Q}(5) = R_{P\backslash Q}(6) = \tau\,.$$

Moreover, the matrices (4.23) commute with each other. (For the origin of this commutativity, see Section 9.4 below.)

Consider the commutative monoid generated by the matrices ε and τ. Each element of the monoid may be expressed uniquely in the form $\varepsilon^l\tau^m$ for non-negative integers l and m. The action of these elements on the state space $\{a, a', b\}$ is then given by Figure 4.2, which displays the image of a under $\varepsilon^l\tau^m$. The symbol k stands for any positive integer. The information in the table is complete, since $b = a\tau$ and $a' = a\varepsilon$. In other words, $a'\varepsilon^l\tau^m = a\varepsilon^{l+1}\tau^m$ and $b\varepsilon^l\tau^m = a\varepsilon^l\tau^{m+1}$. Convex combinations of states are used to specify finite probability distributions. For example, $\frac{1}{3}a + \frac{2}{3}a'$ denotes the mixed state consisting of a one-third chance of state a and a two-thirds chance of state a'. With this notation, the action on the full set of mixed states, the set

$$\{pa + p'a' + (1-p-p')b \mid 0 \le p,\ 0 \le p',\ 0 \le (1-p-p')\} \tag{4.24}$$

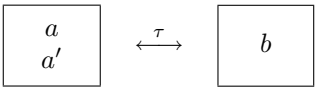
of all convex combinations of the states from $P\backslash Q$, is given by

$$\varepsilon^l\tau^m : pa + p'a' + (1-p-p')b \mapsto pa\varepsilon^l\tau^m + p'a\varepsilon^{l+1}\tau^m + (1-p-p')a\varepsilon^l\tau^{m+1}.$$

$m \setminus l$	0	1	2	3	4	...
0	a	a'	$\frac{1}{2}a + \frac{1}{2}a'$	$\frac{1}{4}a + \frac{3}{4}a'$	$\frac{3}{8}a + \frac{5}{8}a'$	...
1	b	b	b	b	b	...
$2k$	$\frac{1}{3}a + \frac{2}{3}a'$	$\frac{1}{3}a + \frac{2}{3}a'$	$\frac{1}{3}a + \frac{2}{3}a'$	$\frac{1}{3}a + \frac{2}{3}a'$	$\frac{1}{3}a + \frac{2}{3}a'$	...
$2k+1$	b	b	b	b	b	...

FIGURE 4.2: Permutation action of Q on $\{a, a', b\}$

The quasigroup action may be interpreted as an approximate two-fold symmetry between the state b on the one hand, and the states a, a' on the other.



If the distinction between a and a' is suppressed, then one obtains an exact two-fold symmetry between a and b, with ε acting as an identity element (just like ι), while τ acts as a transposition between a and b.

$$a \quad \overset{\tau}{\longleftrightarrow} \quad b \tag{4.25}$$

Acknowledging the distinction between a and a', however, this symmetry is seen to be only approximate. For example, applying τ once to a gives b, but a repeated application of τ leads back to a only with probability one-third, and otherwise gives a'. In [164], *approximate symmetry* has been defined as exact symmetry holding at one level of a hierarchical system. In the present case, there is a hierarchy with just two levels: macroscopic and microscopic.

Macrostates:	$\{a, a'\}$		$\{b\}$
Microstates:	a	a'	b

The macrostates are $\{a, a'\}$ and $\{b\}$, the distinction between a and a' lying at the microscopic level. The approximate symmetry consists of exact two-fold symmetry at the macroscopic level.

4.3 Macroscopic symmetry

This section establishes a general framework for approximate symmetry of the kind observed in the model of the previous section. It depends on the quasigroup analogue of a group-theoretic concept, the core of a subgroup. Recall that the core $K_Q(H)$ of a subgroup H of a group Q is the intersection

$$\bigcap_{q \in Q} H^q$$

of all the conjugates of H in Q.

Let Q be a quasigroup with a congruence V. A subquasigroup Q_0 of Q is said to be *compatible* with V if it is the preimage of its image under the natural projection by V, i.e., if

$$Q_0 = (\mathrm{nat}\, V)^{-1}(Q_0^V)\,.$$

Compatibility means that Q_0 is a union $\bigcup Q_0^V$ of V-classes. The *core* or *core congruence* of a subquasigroup Q_0 in a quasigroup Q is defined to be the largest congruence κ or $\kappa(Q_0)$ or $\kappa_Q(Q_0)$ on Q that is compatible with Q_0. This concept matches its group-theoretical analogue.

PROPOSITION 4.2
Let H be a subgroup of a group Q. Then the group-theoretical core $K_Q(H)$ of H in Q is the class of the identity element 1 of Q under the quasigroup-theoretical core $\kappa_Q(H)$ of H in Q.

PROOF Consider $K_Q(H)$ as the largest normal subgroup N of Q that is contained in the subgroup H. The map $V \mapsto 1^V$ provides an order-preserving isomorphism from the set of congruences on Q that are compatible with H to the set of normal subgroups contained in H. Under this isomorphism, one has $\kappa_Q(H) \mapsto K_Q(H)$. □

The following definition specifies the general features of the sort of approximate symmetry observed in Section 4.2. (Note that this is but one form of approximate symmetry.) In the definition, an exact symmetry is described by a certain transitive permutation action, a faithful (or, in analysts' terminology, "effective") group homogeneous space. The exact symmetry underlying the approximate symmetry observed in Section 4.2 is the symmetry $(\{a, b\}, \langle\tau\rangle)$ of (4.25).

DEFINITION 4.2 *Let G be a group, and let (X, G) be a faithful homogeneous space for G. A system is said to exhibit* macroscopic approximate symmetry *of type (X, G) if it consists of two hierarchical levels, macroscopic and microscopic, with an exact symmetry of type (X, G) holding at the macroscopic level.*

THEOREM 4.2
Suppose that a nonempty finite quasigroup Q contains a subquasigroup Q_0 compatible with the group replica congruence of Q. Let κ be the core of Q_0 in Q. Then for a subquasigroup P of Q_0, the homogeneous space $P\backslash Q$ exhibits macroscopic approximate symmetry of type $(Q_0^\kappa\backslash Q^\kappa, Q^\kappa)$.

PROOF Since Q_0 is compatible with the group replica congruence of Q,

the quotient Q^κ is a group. As a consequence of the isomorphism theorems, $K_{Q^\kappa}(Q_0^\kappa)$ is trivial, so the group homogeneous space $(Q_0^\kappa\backslash Q^\kappa, Q^\kappa)$ is faithful.

The microstates of the homogeneous space $P\backslash Q$ are its elements, namely the $\mathrm{LMlt}_Q(P)$-orbits on Q. The macrostates are the $\mathrm{LMlt}_Q(Q_0)$-orbits on Q. Since P is a subquasigroup of Q_0, it is immediate that each macrostate is a union of microstates, so that $P\backslash Q$ forms a two-level hierarchical system.

Suppose that $(x, y) \in \kappa$. Let e be an element of Q for which e^κ is the identity element of the group Q^κ. Then

$$y/x \in (y/x)^\kappa = y^\kappa/x^\kappa = e^\kappa.$$

Now e^κ is a subquasigroup of Q_0. Since $xL(y/x) = y$ by (SR), it follows that each $\mathrm{LMlt}_Q(Q_0)$-orbit is a union of κ-classes.

For x in Q, the map

$$\beta : Q_0\backslash Q \to Q_0^\kappa\backslash Q^\kappa; x\mathrm{LMlt}_Q(Q_0) \mapsto x^\kappa \mathrm{LMlt}_{Q^\kappa}(Q_0^\kappa)$$

bijects. Certainly it is well defined, since

$$xL(q_1)^{\pm 1} \dots L(q_r)^{\pm 1} = y$$

(with $x, y \in Q$ and $q_1, \dots, q_r \in Q_0$) implies

$$x^\kappa L(q_1^\kappa)^{\pm 1} \dots L(q_r^\kappa)^{\pm 1} = y^\kappa .$$

The map β is clearly surjective. For the injectivity, suppose

$$x^\kappa L(p_1^\kappa)^{\pm 1} \dots L(p_r^\kappa)^{\pm 1} = y^\kappa L(q_1^\kappa)^{\pm 1} \dots L(q_s^\kappa)^{\pm 1}$$

for $x, y \in Q$ and $p_1, \dots p_r, q_1, \dots, q_s \in Q_0$. Then

$$(xL(p_1)^{\pm 1} \dots L(p_r)^{\pm 1}, yL(q_1)^{\pm 1} \dots L(q_s)^{\pm 1}) \in \kappa ,$$

so x and y share the same $\mathrm{LMlt}_Q(Q_0)$-orbit.

Finally, for $x, y, q \in Q$ and $q_1, \dots, q_r \in Q_0$, the equation

$$xL(q_1)^{\pm 1} \dots L(q_r)^{\pm 1} R(q) = y$$

implies

$$x^\kappa L(q_1^\kappa)^{\pm 1} \dots L(q_r^\kappa)^{\pm 1} R(q^\kappa) = y^\kappa .$$

Thus the transition matrix of $R_{Q_0\backslash Q}(q)$ on $Q_0\backslash Q$ is the permutation matrix of $R_{Q_0^\kappa\backslash Q^\kappa}(q^\kappa)$ on $Q_0^\kappa\backslash Q^\kappa$. It follows that the macroscopic homogeneous space $(Q_0\backslash Q, Q)$ has the required symmetry type $(Q_0^\kappa\backslash Q^\kappa, Q^\kappa)$. □

4.4 Regularity

For a quasigroup Q, the *regular* homogeneous space is the homogeneous space $\varnothing\backslash Q$. Recall that the relative left multiplication group of the empty subquasigroup is trivial. Thus the state space of $\varnothing\backslash Q$ is the set

$$\big\{\{q\} \,\big|\, q \in Q\big\}$$

of singleton subsets of Q, often simply identified with Q itself. If Q is a loop with identity element e, then the relative left multiplication group of the singleton subquasigroup $\{e\}$ of Q is again trivial. Thus the regular homogeneous space of a loop may be described as $\{e\}\backslash Q$ (or just $e\backslash Q$) rather than $\varnothing\backslash Q$.

A finite quasigroup Q may be recovered from its regular space.

PROPOSITION 4.3
The multiplication table of the conjugate $(Q, \backslash)$ is the formal sum

$$\sum_{q\in Q} qR_{\varnothing\backslash Q}(q) \tag{4.26}$$

of multiples of the action matrices of $\varnothing\backslash Q$.

PROOF For the regular space, the incidence matrix $A_\varnothing$ is just the identity matrix, so that $R_{\varnothing\backslash Q}(q) = R_Q(q)$ for each element q of Q. For elements x, y of Q, consider the entry of the matrix (4.26) in the row labeled by x and the column labeled by y. Since there is a unique quasigroup element q such that $xR_Q(q) = y$, namely $q = x\backslash y$, this matrix entry is $x\backslash y$. Thus (4.26) is the multiplication table of the conjugate $(Q, \backslash)$, as required. □

COROLLARY 4.4
The multiplication table of a finite quasigroup $(Q, \cdot)$ is the formal sum

$$\sum_{q\in Q} qR_S(q) \tag{4.27}$$

of action matrices of the regular homogeneous space S of its conjugate $(Q, \backslash)$.

PROOF By (1.9), the original multiplication $\cdot$ on Q is the left division corresponding to $\backslash$ as a multiplication operation. □

By Cayley's Theorem, a finite group Q is immediately recovered from its regular space as the group formed by the action (permutation) matrices under

multiplication. More general quasigroups with the action matrices of the regular space forming a group under multiplication have occasionally appeared in the literature (compare [21], [28, Ex. II.5.27], [85, Prop. 1], [169]). Define a *right quasiloop* to be a quasigroup Q having a *right identity*, an element e such that $xe = x$ for all x in Q.

THEOREM 4.3

Let $(Q, \cdot)$ be a finite, nonempty quasigroup with right multiplication group G. Then the following conditions are equivalent:

(a) *The group G acts regularly on Q;*

(b) *There is a group structure $(Q, +)$ on Q, and a permutation λ of Q, such that*

$$x \cdot y = x + y^{\lambda} \tag{4.28}$$

for all x, y in Q;

(c) *There is a group structure $(Q, +)$ on Q, and a permutation λ of Q fixing the identity element of $(Q, +)$, such that (4.28) holds for all x, y in Q;*

(d) *$(Q, \cdot)$ is a right quasiloop isotopic to a group.*

PROOF (a)⇒(b): If (a) holds, then there is a G-isomorphism s from the action of G on Q to the right regular action of the group G or $(G, +)$ on itself. In this latter action, there is a permutation λ of Q such that, for each y in Q, the element $R(y) : Q \to Q; x \mapsto x \cdot y$ of G acts as the group right multiplication $R_+(y\lambda^s)$ by the element $y\lambda^s$ of G. Thus for x and y in Q, one has $xR(y)s = x^s R(y)$ or

$$(x \cdot y)^s = x^s + y\lambda^s. \tag{4.29}$$

Now the bijection $s : Q \to G$ may be used to induce a group operation $+$ on Q by $(x + y)^s = x^s \circ y^s$. The equation (4.29) then takes the form

$$(x \cdot y)^s = (x + y^{\lambda})^s.$$

Since s injects, the desired result (4.28) follows.

(b)⇒(c): See [169] or Exercise 5.

(c)⇒(d): If (c) holds, then the identity element of the group $(Q, +)$ is a right identity for the quasigroup $(Q, \cdot)$, so that $(Q, \cdot)$ is a right quasiloop. By (4.28), the right quasiloop $(Q, \cdot)$ is isotopic to the group $(Q, +)$.

(d)⇒(c): See [85, Prop. 1] or Exercise 5.

(c)⇒(b): Immediate.

(b)⇒(a): Suppose that (b) holds. Then each quasigroup right multiplication $R(y)$ for y in Q may be written as the group right multiplication $R_+(y^\lambda)$. It follows that G is equal to the right multiplication group of the group $(Q,+)$. As such, G acts regularly on Q. □

4.5 Lagrangean properties

For a group Q, Lagrange's Theorem states that the order of a subgroup always divides the order of Q. For a general quasigroup Q, even the order of a nonempty subquasigroup need not divide the order of Q. Pflugfelder [125] describes a subloop P of a loop Q as *Lagrange-like* in Q if $|P|$ does divide $|Q|$. The loop Q is said to satisfy the *weak Lagrange property* if each subloop is Lagrange-like. It is said to satisfy the *strong Lagrange property* if each of its subloops satisfies the weak Lagrange property. Nonassociative loops satisfying the strong Lagrange property were discussed in [27], [63], [64]. Recalling that Lagrange's Theorem for a group Q relies on the uniformity of the sizes of the elements of a homogeneous space $P\backslash Q$, this section formulates Lagrangean properties in homogeneous space terms. Let P be a subquasigroup of a finite, nonempty quasigroup Q. The *type* of the homogeneous space $P\backslash Q$ is the partition of $|P\backslash Q|$ given by the sizes of the orbits of the relative left multiplication group of P in Q. Note that the type of a homogeneous space is determined by its Markov matrix, according to (4.19). The type of a homogeneous space $P\backslash Q$, or the space itself, is said to be *uniform* if all the parts of the partition are equal. For example, the regular space of any finite, nonempty quasigroup Q is uniform.

A subquasigroup P of a quasigroup Q is said to be (*right*) *Lagrangean* in Q if the type of $P\backslash Q$ is uniform, i.e., if the relative left multiplication group of P in Q acts semitransitively (in the sense of [83, Defn. II.1.14b]). Similarly, P is *left Lagrangean* if the relative right multiplication group of P in Q acts semitransitively. Note that a Lagrangean subloop P of a loop Q is Lagrange-like in Pflugfelder's sense, since P is one of the states of $P\backslash Q$. On the other hand, the subloop P of the loop Q of Example 4.2 below is Lagrange-like in Q, but not right Lagrangean in Q.

PROPOSITION 4.4

Each normal subloop P of a finite loop Q is right Lagrangean in Q.

PROOF Let P be an equivalence class of a congruence V on Q. It will be shown that the $\mathrm{LMlt}_Q P$-orbits on Q coincide with the V-classes. The uniformity of $P\backslash Q$ then follows by Exercise 7 of Chapter 3.

First, suppose that $(q_1, q_2) \in V$. Note that $(q_2, q_2) \in V$ by reflexivity. Then V contains the right quotient $(q_2, q_2)/(q_1, q_2) = (q_2/q_1, e)$, whence $q_2/q_1 \in P$. Thus $q_2 = q_1 L(q_2/q_1)$ lies in the orbit of q_1 under $\mathrm{LMlt}_Q P$, i.e. the V-class of q_1 is contained in an $\mathrm{LMlt}_Q P$-orbit.

Conversely, it must be shown that the $\mathrm{LMlt}_Q P$-orbit of an element q of Q is contained in the V-class of q. It will be proved by induction on the length of a word w of $\mathrm{LMlt}_Q P$ that $(q, qw) \in V$. The induction basis (length 0) is the observation that (q, q) lies in V by reflexivity. Suppose $(q, qw) \in Q$ and $p \in P$. Then V contains $(e, p) \cdot (qw, qw) = (qw, qwL(p))$, so that $(q, qwL(p)) \in V$ by transitivity. Similarly, V contains $(e, p)\backslash(qw, qw) = (qw, qwL(p)^{-1})$, so that $(q, qwL(p)^{-1}) \in V$ by transitivity. □

REMARK 4.1 The example of Section 4.2 shows that normality of a nonempty subquasigroup P of a finite quasigroup Q does not imply that P is right Lagrangean in Q. In the example, the subquasigroup $P = \{1\}$ is normal, being a class of the trivial congruence on Q. Nevertheless, the type of $P\backslash Q$ is not uniform. □

The Lagrangean property is more robust than Lagrange-likeness. It may happen that a subloop P of a loop Q is Lagrange-like in Q, but not in a subloop of Q that contains P. For example, suppose that a loop Q has a subloop P that is not Lagrange-like in Q. Then $P \times \{e\}$ is Lagrange-like in the loop $Q \times P$, but not in the subloop $Q \times \{e\}$. The following proposition shows that the Lagrangean property does not exhibit such pathology.

PROPOSITION 4.5

Let P be a Lagrangean subquasigroup in a finite quasigroup Q. Then P is Lagrangean in each subquasigroup S of Q that contains P.

PROOF Since P is a subquasigroup of the quasigroup S, the action of the relative left multiplication group $\mathrm{LMlt}_S P$ of P in S is just a restriction to S of the action of the relative left multiplication group $\mathrm{LMlt}_Q P$ of P in Q. Thus the uniformity of the sizes of the orbits of $\mathrm{LMlt}_Q P$ implies the uniformity of the sizes of the orbits of $\mathrm{LMlt}_S P$. □

DEFINITION 4.3 *A finite quasigroup Q is said to* satisfy the (right) Lagrange property *if each subquasigroup of Q is (right) Lagrangean in Q. It is said to* satisfy the left Lagrange property *if each subquasigroup of Q is left Lagrangean in Q. Finally, Q is said to* satisfy the total Lagrange property *if it satisfies both the right and left Lagrange properties.*

Example 4.1
The only proper, nontrivial subloop of the loop T with multiplication table

1	2	3	4	5	6
2	1	6	5	4	3
3	6	5	1	2	4
4	5	1	6	3	2
5	3	4	2	6	1
6	4	2	3	1	5

is the subloop $\{1, 2\}$, which is Lagrangean in T. Thus T is a nonassociative loop satisfying the right Lagrange property. □

In contrast with the global properties based on Lagrange-likeness, Proposition 4.5 shows that one does not need to make a distinction between "weak" and "strong" versions of the Lagrangean property of Definition 4.3.

COROLLARY 4.5
Suppose that a finite quasigroup Q satisfies the right Lagrange property. Then each subquasigroup of Q also satisfies the right Lagrange property.

PROOF Let P be a subquasigroup of a subquasigroup Q' of Q. Then by Proposition 4.5, P is Lagrangean in Q'. □

COROLLARY 4.6
If a finite loop Q satisfies the right Lagrange property, then it also satisfies the strong Lagrange property.

PROOF Let P be a subloop of a subloop Q' of Q. By Corollary 4.5, Q' satisfies the right Lagrange property, so that P is Lagrangean in Q'. It then follows that P is Lagrange-like in Q'. Thus each subloop Q' of Q satisfies the weak Lagrange property, so that Q itself satisfies the strong Lagrange property. □

Example 4.2
The converse of Corollary 4.6 is false: the strong Lagrange property is too weak to imply the right Lagrange property. For a "natural" example, compare

Exercise 10. More directly, consider the loop Q whose multiplication table is the following Latin square.

1	2	3	4	5	6
2	1	4	5	6	3
3	4	5	6	1	2
4	3	6	1	2	5
5	6	1	2	3	4
6	5	2	3	4	1

The proper, nontrivial subloops of Q are $P = \{1, 2\}$, $P' = \{1, 4\}$, and $P'' = \{1, 6\}$, each Lagrange-like in Q, and without mutual containments. Thus Q does satisfy the strong Lagrange property. On $P\backslash Q$, the action matrices (4.14) of the elements of P are the identity I_2, while the action matrices of the remaining elements of Q are

$$A = \begin{bmatrix} 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

(Exercise 3). The type of $P\backslash Q$ is $2 + 4$, so that P is not Lagrangean in Q, and Q does not satisfy the right Lagrange property. □

Corollary 4.5 shows that the right Lagrange property is inherited by subquasigroups. The property is also inherited by homomorphic images.

PROPOSITION 4.6

Suppose that a finite quasigroup Q satisfies the right Lagrange property. Then each homomorphic image of Q also satisfies the right Lagrange property.

PROOF Suppose that $\overline{Q}$ is a quotient of Q by a projection

$$Q \to \overline{Q}; q \mapsto \overline{q}. \tag{4.30}$$

Let $\overline{P}$ be a subquasigroup of $\overline{Q}$ whose preimage under (4.30) is a nonempty subqausigroup P of Q. The projection (4.30) induces a group epimorphism

$$\mathrm{LMlt}_Q P \to \mathrm{LMlt}_{\overline{Q}} \overline{P}; l \mapsto \overline{l} \tag{4.31}$$

acting on the set (2.8) of generators of its domain by $L(p) \mapsto L(\overline{p})$. Set $L = \mathrm{LMlt}_Q P$ and $\overline{L} = \mathrm{LMlt}_{\overline{Q}} \overline{P}$. Now for q in Q, one has

$$\overline{q}\overline{L} = \overline{qL}. \tag{4.32}$$

To see this, consider an element $\overline{q}\overline{l}$ of the left hand side of (4.32), where the element l of $\mathrm{LMlt}_Q P$ is given by

$$l = L(p_1) \dots L(p_r)$$

with elements $p_1, \dots, p_r$ of P. Then

$$\overline{q}\overline{l} = \overline{q}L(\overline{p_1}) \dots L(\overline{p_r}) = \overline{qL(p_1) \dots L(p_r)} \in \overline{qL},$$

the second equality holding since (4.30) is a quasigroup homomorphism. Conversely, the typical element of the right-hand side of (4.32) is of the form

$$\overline{qL(p_1) \dots L(p_r)}$$

with q in Q and elements $p_1, \dots, p_r$ of P. Such an element may be rewritten in the form

$$\overline{q}L(\overline{p_1}) \dots L(\overline{p_r}),$$

exhibiting it as an element of the left-hand side of (4.32).

Let p_0 be a fixed element of P. Since the homogeneous space $P \setminus Q$ has uniform type, it follows that for each element q of Q the injection

$$R(p_0 \backslash q) : P \to qL; p \mapsto p(p_0 \backslash q)$$

bijects. In other words, $qL = \{p(p_0 \backslash q) \mid p \in P\}$. Then by (4.32), one has

$$\overline{q}\overline{L} = \overline{qL} = \left\{ \overline{p \cdot (p_0 \backslash q)} \,\middle|\, p \in P \right\} = \{\overline{p} \cdot (\overline{p}_0 \backslash \overline{q}) \mid \overline{p} \in \overline{P}\},$$

so that each state of $\overline{P} \setminus \overline{Q}$ has cardinality $|\overline{P}|$. Thus $\overline{P}$ is Lagrangean in $\overline{Q}$, as required. □

4.6 Exercises

1. [18, Th. 1.5], [124] Suppose that A_1^+ and A_2^+ are matrices satisfying the equations (4.2) through (4.5) for A^+. Show that $A_1^+ = A_2^+$.

2. Let P be a subquasigroup of a finite quasigroup Q. Show that for each element q of Q, each column sum of the action matrix $R_{P\backslash Q}(q)$ is nonzero.

3. Let P be a subquasigroup of positive order m in a quasigroup Q of finite order n. Suppose $|P\backslash Q| = 2$. Show that for an element q of Q,

$$R_{P\backslash Q}(q) = \begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \text{if } q \in P\,; \\ \\ \begin{bmatrix} 0 & 1 \\ \frac{m}{n-m} & \frac{n-2m}{n-m} \end{bmatrix} & \text{otherwise.} \end{cases}$$

4. Formulate the "left-handed" version of Theorem 4.3.

5. In Theorem 4.3, show that condition (c) follows from each of the conditions (b) and (d).

6. For an $(m \times p)$-matrix A and an $(n \times p)$-matrix B, the *cracovian* product is defined by
$$A \copyright B = AB^T .$$

   (a) Let
   $$\mathbf{b} = \mathbf{x}A \tag{4.33}$$
   be an overdetermined system of linear equations, with a real coefficient row vector $\mathbf{b}$ of dimension n, a real $m \times n$ coefficient matrix A, and an m-dimensional row vector $\mathbf{x}$ of unknowns, for $n \geq m$. Show that $\mathbf{x}$ is a least squares solution to (4.33) if and only if
   $$\mathbf{b} \copyright A = \mathbf{x}(A \copyright A) .$$

   (b) Let Q be a finite set of orthogonal real $n \times n$ matrices that is closed under the cracovian product. Show that $(Q, \copyright)$ forms a quasigroup satisfying the equivalent conditions of Theorem 4.3.

7. Consider the two conjugates of a group of order 3 under right and left division respectively. (Compare Exercise 5 of Chapter 1.)

   (a) Show that in each, the singleton subquasigroup is left and right Lagrangean respectively.

   (b) Show that the conjugates have the left and right Lagrange properties respectively, but that neither has the total Lagrange property.

8. Exhibit a quasigroup of order 4 which does not have the right Lagrange property.

9. Suppose that a finite quasigroup Q has a subquasigroup P which is not right Lagrangean. Show that
$$|P| < \frac{|Q|}{|P \backslash Q|} .$$

10. Show that the Moufang loop $\mathrm{M}_1(2)$ does satisfy the strong Lagrange property, but not the right Lagrange property.

11. Consider a finite central pique Q with pointed idempotent 0. Show that the following are equivalent:

   (a) $\{0\}$ is left Lagrangean in Q;

   (b) Q satisfies the equivalent conditions of Theorem 4.3;

   (c) Q satisfies the left Lagrange property.

4.7 Notes

Section 4.1

The concept of a quasigroup homogeneous space goes back to [157], [160]. Many of the results of Chapters 4 and 5 carry over verbatim to left quasigroups.

If Q is associative, the notation $P\backslash Q$ is consistent with (2.10). However, the subquasigroup $P = \{1\}$ of the Steiner triple system $Q = \mathsf{PG}(1, 2)$ is normal, being a class of the trivial congruence on Q. Nevertheless, the quotient set of singleton classes, written as Q/P according to the notation of Section 3, is not the set of orbits of $\mathrm{RMlt}_Q P$ on Q.

Section 4.3

A different kind of approximate symmetry is presented in [164]. There, exact symmetry holds at the mesoscopic level of a three-level linearly-ordered complex system, but not at the microscopic or macroscopic levels. The problem of constructing mathematical models for general kinds of approximate symmetry is completely open, as is the question of a taxonomy for approximate symmetries.

Section 4.4

Some sources, such as [85], use the term "right loop" for right quasiloops. However, the term "right loop" is best reserved for right quasigroups having a two-sided identity, as in Section 2.5. In [11], left quasigroups having a right identity were described as *semiloops*.

Chapter 5

PERMUTATION REPRESENTATIONS

This chapter is devoted to the theory of permutation representations or Q-sets of a finite quasigroup Q. In Section 5.1, general finite sets acted upon by a Q-indexed set of Markov matrices are described as Q-IFS or iterated function systems in the sense of fractal geometry. However, the most satisfactory general description is in terms of coalgebras, which are summarized briefly in Appendix C. The Q-IFS are interpreted as certain coalgebras in Section 5.2. Following the technical Section 5.3 describing irreducible coalgebras, the permutation representations or Q-sets of a finite quasigroup Q are then defined in Section 5.4 as the members of the covariety of coalgebras generated by the homogeneous spaces of Q. Section 5.5 introduces the Burnside algebra of a quasigroup, as a direct generalization of the Burnside algebra of a group. Section 5.6 computes the Burnside algebra for the quasigroup of Figure 1.2. Section 5.7 examines the idempotents of the Burnside algebra. Finally, Section 5.8 presents Burnside's Lemma for quasigroup permutation actions: its proof specializes to a new proof of Burnside's Lemma for group permutation representations.

5.1 The category $\mathbf{IFS}_Q$

Let P be a subquasigroup of a nonempty finite quasigroup Q. The set of convex combinations of the states from the homogeneous space $P\backslash Q$ forms a complete metric space, and the actions (4.14) of the quasigroup elements form an iterated function system or IFS in the sense of fractal geometry [7]. More generally, for any finite quasigroup Q, define a Q-IFS (X, Q) as a finite set X together with an *action map*

$$R : Q \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}X); q \mapsto R_X(q) \tag{5.1}$$

from Q to the set of endomorphisms of the complex vector space with basis X (identified with their matrices with respect to the basis X), such that each *action matrix* $R_X(q)$ is stochastic. For a nonempty finite quasigroup Q, the

Markov matrix of (X, Q) is the arithmetic mean

$$M_{(X,Q)} = \frac{1}{|Q|} \sum_{q \in Q} R_X(q) \tag{5.2}$$

of the action matrices of the elements of Q. For a finite set X, define $M_{(X,\varnothing)}$ as the $|X| \times |X|$ identity matrix. Note that the Markov matrix of a Q-IFS is stochastic. If P is a subquasigroup of a finite nonempty quasigroup Q, then the homogeneous space $P\backslash Q$ is a Q-IFS with the action map specified by (4.14), and the definitions above are consistent with Definition 4.1.

A *morphism*

$$\phi : (X, Q) \to (Y, Q) \tag{5.3}$$

from a Q-IFS (X, Q) to a Q-IFS (Y, Q) is a function $\phi : X \to Y$ whose graph has an incidence matrix F satisfying the intertwining equation

$$R_X(q)F = FR_Y(q) \tag{5.4}$$

for each element q of Q. It is readily checked that the class of morphisms (5.3), for a fixed quasigroup Q, forms a concrete category $\mathbf{IFS}_Q$.

PROPOSITION 5.1
Let Q be a finite group.

(a) The category of finite Q-sets forms the full subcategory of $\mathbf{IFS}_Q$ consisting of those objects for which the action map (5.1) *is a monoid homomorphism.*

(b) A Q-IFS (X, Q) is a Q-set if and only if it is isomorphic to a Q-set (Y, Q) in $\mathbf{IFS}_Q$.

PROOF For (a), suppose that the action map (5.1) of a Q-IFS (X, Q) is a monoid homomorphism. Let A be in the image of (5.1). Then A is a stochastic matrix with $A^r = I$ for some positive integer r. It follows that A is a permutation matrix (cf. §XV.7 of [59]). Part (b) follows from part (a): if the morphism $\phi : (X, Q) \to (Y, Q)$ is an isomorphism whose graph has incidence matrix F, then the action map of (X, Q) is the composite of the action map of (Y, Q) with the monoid isomorphism $R_Y(q) \mapsto FR_Y(q)F^{-1}$ given by Equation (5.4). □

For a fixed finite quasigroup Q, the category $\mathbf{IFS}_Q$ has finite coproducts. Consider objects (X, Q) and (Y, Q) of $\mathbf{IFS}_Q$. Their *sum* or *disjoint union* $(X + Y, Q)$ consists of the disjoint union $X + Y$ of the sets X and Y together with the action map

$$q \mapsto R_X(q) \oplus R_Y(q) \tag{5.5}$$

sending each element q of Q to the direct sum of the matrices $R_X(q)$ and $R_Y(q)$. One obtains an object of $\mathbf{IFS}_Q$, since the direct sum of stochastic matrices is stochastic.

THEOREM 5.1
Let (X, Q) and (Y, Q) be objects of $\mathbf{IFS}_Q$. The sum $(X + Y, Q)$ forms the coproduct of (X, Q) and (Y, Q) in the category $\mathbf{IFS}_Q$.

PROOF Consider the diagram

$$\begin{array}{ccccc}
\mathbb{C}X & \xrightarrow{J_X} & \mathbb{C}X \oplus \mathbb{C}Y & \xleftarrow{J_Y} & \mathbb{C}Y \\
\| & & \downarrow{\scriptstyle F\oplus G} & & \| \\
\mathbb{C}X & \xrightarrow{F} & \mathbb{C}Z & \xleftarrow{G} & \mathbb{C}Y \\
\| & & \downarrow{\scriptstyle R_Z(q)} & & \| \\
\mathbb{C}X & \xrightarrow{FR_X(q)} & \mathbb{C}Z & \xleftarrow{GR_Y(q)} & \mathbb{C}Y
\end{array} \tag{5.6}$$

in the category of complex vector spaces. Here q is an element of Q, the linear transformation F is (described by) the incidence matrix of an $\mathbf{IFS}_Q$-morphism $f : (X, Q) \to (Z, Q)$, and the linear transformation G is the incidence matrix of an $\mathbf{IFS}_Q$-morphism $g : (Y, Q) \to (Z, Q)$. The linear transformations on the top row are linear extensions of the insertions of the summands X, Y in the disjoint union $X + Y$. Then

$$\begin{aligned}
R_{X+Y}(q)(F \oplus G) &= \big(R_X(q) \oplus R_Y(q)\big)(F \oplus G) \\
&= R_X(q)F \oplus R_Y(q)G = FR_Z(q) \oplus GR_Z(q) \\
&= (F \oplus G)R_Z(q),
\end{aligned}$$

the latter equality following by the commuting of (5.6). It follows that the direct sum matrix $F \oplus G$ is the incidence matrix of a uniquely specified sum $\mathbf{IFS}_Q$-morphism $f + g : (X + Y, Q) \to (Z, Q)$, as required. □

The *tensor product* $(X \otimes Y, Q)$ of (X, Q) and (Y, Q) is the direct product $X \times Y$ of the sets X and Y together with the action map

$$q \mapsto R_X(q) \otimes R_Y(q) \tag{5.7}$$

sending each element q of Q to the tensor (or Kronecker) product of the matrices $R_X(q)$ and $R_Y(q)$. Thus for elements (x, y) and (x', y') of $X \times Y$, the $(x, y)(x', y')$-entry of the matrix $R_X(q) \otimes R_Y(q)$ is given as the product of the xx'-entry of $R_X(q)$ with the yy'-entry of $R_Y(q)$. Again, one obtains an object of $\mathbf{IFS}_Q$, since the tensor product of stochastic matrices is stochastic. The abstract significance of the tensor product is given by Corollary 5.3 below in the context of coalgebras.

5.2 Actions as coalgebras

For a finite set Q, the Q-IFS are realized as coalgebras for the Q-th power of the endofunctor B sending a set to (the underlying set of) the free barycentric algebra that it generates. It is worth recalling some basic facts about barycentric algebras. For more details, readers may consult [134] or [135]. Let I° denote the open unit interval $]0,1[$, the interior of the closed unit interval $I = [0,1]$. For p, q in I, define $p' = 1 - p$ and $p \circ q = (p'q')'$.

DEFINITION 5.1 *A* barycentric algebra A *or* (A, I°) *is an algebra of type* $I^\circ \times \{2\}$*, equipped with a binary operation*

$$\underline{p} : A \times A \to A; (x, y) \mapsto xy\,\underline{p} \tag{5.8}$$

for each p *in* I°*, satisfying the identities*

$$xx\,\underline{p} = x \tag{5.9}$$

of idempotence *for each* p *in* I°*, the identities*

$$xy\,\underline{p} = yx\,\underline{p'} \tag{5.10}$$

of skew-commutativity *for each* p *in* I°*, and the identities*

$$xy\,\underline{p}\ z\,\underline{q} = x\ yz\,\underline{q/(p \circ q)}\ \underline{p \circ q} \tag{5.11}$$

of skew-associativity *for each* p, q *in* I°*. Let* $\mathbf{B}$ *denote the variety of all barycentric algebras, construed as a category having all the barycentric algebra homomorphisms as its morphisms. The corresponding free algebra functor is* $B : \mathbf{Set} \to \mathbf{B}$*.*

A convex set C forms a barycentric algebra (C, I°), with $xy\,\underline{p} = (1-p)x + py$ for x, y in C and p in I°. A semilattice $(S, \cdot)$ becomes a barycentric algebra on setting $xy\,\underline{p} = x \cdot y$ for x, y in S and p in I°. For the following result, see [120], [134, §2.1], [135, §5.8].

THEOREM 5.2
Let X *be a set. Then the free barycentric algebra* XB *on* X *is realized as the set of all finitely-supported probability distributions on* X*. If* X *is finite, the free algebra* XB *on* X *is also realized as the simplex spanned by* X*.*

In the latter case, the theorem relies on the identification of the barycentric coordinates in a simplex with the weights in finite probability distributions.

DEFINITION 5.2 *Let Q be a finite set. The functor $B^Q : \mathbf{Set} \to \mathbf{Set}$ sends a set X to the set XB^Q of functions from Q to the free barycentric algebra XB over X. For a function $f : X \to Y$, its image under the functor B^Q is the function $fB^Q : XB^Q \to YB^Q$ defined by*

$$fB^Q : (Q \to XB; q \mapsto w) \mapsto (Q \to YB; q \mapsto wf^B).$$

Some standard "coalgebraic" properties of the functor B^Q are listed for reference in the following proposition. The meaning of these properties is discussed in Appendix C.2.

PROPOSITION 5.2
Let Q be a finite set.

(a) *The functor B^Q preserves weak pullbacks.*

(b) *The functor B^Q is bounded.*

(c) *Each covariety of B^Q-coalgebras is bicomplete.*

PROOF (a) By Appendix A of [173], the functor B preserves weak pullbacks. Thus the finite power B^Q of B also preserves weak pullbacks (compare [68, Lemma 8.11]).
(b) See the proof of [173, Th. 4.6].
(c) Since B^Q is bounded, the result follows according to [68, §7.4]. □

THEOREM 5.3
Let Q be a finite set. Then the category $\mathbf{IFS}_Q$ is isomorphic with the category of finite B^Q-coalgebras.

PROOF
Given a Q-IFS (X, Q) with action map R as in (5.1), define a B^Q-coalgebra $L_X : X \to XB^Q$ with structure map

$$L_X : X \to XB^Q; x \mapsto (Q \to XB; q \mapsto xR_X(q)). \tag{5.12}$$

(Note the use of Theorem 5.2 interpreting the vector $xR_X(q)$, lying in the simplex spanned by X, as an element of XB.) Given a Q-IFS morphism $\phi : (X, Q) \to (Y, Q)$ as in (5.3), with incidence matrix F, one has

$$xL_X.\phi B^Q : Q \to YB; q \mapsto xR_X(q)F \tag{5.13}$$

for each x in X, by Definition 5.2. On the other hand, one also has

$$x\phi L_Y : Q \to YB; q \mapsto xFR_Y(q). \tag{5.14}$$

By (5.4), it follows that the maps (5.13) and (5.14) agree. Thus $\phi : X \to Y$ is a coalgebra homomorphism. These constructions yield a functor from $\mathbf{IFS}_Q$ to the category of finite B^Q-coalgebras.

Conversely, consider a given finite B^Q-coalgebra X with structure map $L_X : X \to XB^Q$. Define a Q-IFS (X, Q) with action map

$$R_X : Q \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}X); q \mapsto (x \mapsto qL_X(x)), \tag{5.15}$$

well-defined by Theorem 5.2. Let $\phi : X \to Y$ be a coalgebra homomorphism with incidence matrix F. Then the maps (5.13) and (5.14) agree for all x in the basis X of $\mathbb{C}X$, whence (5.4) holds and $\phi : (X, Q) \to (Y, Q)$ becomes a Q-IFS morphism. In this way one obtains mutually inverse functors between the two categories. □

COROLLARY 5.1

Each homogeneous space over a finite quasigroup Q yields a B^Q-coalgebra.

Example 5.1

Consider the structure map of the coalgebra corresponding to the homogeneous space presented in Section 4.2. In accordance with (4.22), the image of the state $\{4, 5, 6\}$ sends the element 5 of Q to the convex combination weighting the state $\{1\}$ with $1/3$ and the state $\{2, 3\}$ with $2/3$. □

COROLLARY 5.2

Let Q be a finite group. Then the category of finite Q-sets embeds faithfully as a full subcategory of the category of all B^Q-coalgebras.

PROOF Apply Theorem 5.3 and Proposition 5.1. □

COROLLARY 5.3

Let Q be a finite quasigroup. Let (X, Q) and (Y, Q) be objects of $\mathbf{IFS}_Q$, with corresponding B^Q-coalgebras $X \to XB^Q$ and $Y \to YB^Q$ under the isomorphism of Theorem 5.3. Then the tensor product $(X \otimes Y, Q)$ corresponds to a bisimulation between $X \to XB^Q$ and $Y \to YB^Q$.

PROOF Consider the diagram

$$\mathbb{C}X \xleftarrow{P_X} \mathbb{C}X \otimes \mathbb{C}Y \xrightarrow{P_Y} \mathbb{C}Y$$

in the category of complex vector spaces, the linear extension of the product diagram

$$X \xleftarrow{\pi_X} X \times Y \xrightarrow{\pi_Y} Y \tag{5.16}$$

in the category of sets. Now for $x \in X, y \in Y, q \in Q$, one has

$$\begin{aligned}(x \otimes y)p_X R_X(q) &= xR_X(q) \\ &= \big(xR_X(q) \otimes yR_Y(q)\big)p_X \\ &= (x \otimes y)R_{X\otimes Y}(q)p_X.\end{aligned}$$

Thus π_X, and similarly π_Y, are $\mathbf{IFS}_Q$-morphisms as required. □

COROLLARY 5.4

Let Q be a finite quasigroup. Let (X, Q) and (Y, Q) be objects of $\mathbf{IFS}_Q$, with corresponding B^Q-coalgebras $X \to XB^Q$ and $Y \to YB^Q$ under the isomorphism of Theorem 5.3. Then the tensor product $X \otimes Y$ forms a subcoalgebra of the product $X \times Y$ of X and Y in the category of all B^Q-coalgebras.

PROOF Consider the diagram

$$\begin{array}{ccccc} X & \xleftarrow{\varpi_X} & X \otimes Y & \xrightarrow{\varpi_Y} & Y \\ \| & & \uparrow{\scriptstyle \pi_X \times \pi_Y} & & \| \\ X & \xleftarrow{\pi_X} & X \times Y & \xrightarrow{\pi_Y} & Y \\ \| & & \uparrow{\scriptstyle \varpi_X \times \varpi_Y} & & \| \\ X & \xleftarrow{\varpi_X} & X \otimes Y & \xrightarrow{\varpi_Y} & Y \end{array} \tag{5.17}$$

in the category of sets. The middle row of the diagram is the image, under the underlying set functor, of the product object and projections in the category of B^Q-coalgebras. This configuration exists by Proposition 5.2. The top and bottom rows, instances of (5.16) rewritten with a notation more appropriate to the context of B^Q-coalgebras, just denote the product object and projections in the category of sets. By Corollary 5.3, these rows are the images of a diagram in the category of B^Q-coalgebras. The whole lower rectangle of (5.17) is the image of a product diagram in the category of B^Q-coalgebras, while the top rectangle is a product diagram in the category of sets. However, the outer rectangle of (5.17) is also a product diagram in the category of sets, with product map realized by $1_{X\otimes Y}$. Thus the coalgebra homomorphism $\varpi_X \times \varpi_Y$ injects as required, since it is retracted by $\pi_X \times \pi_Y$ in the category of sets. □

5.3 Irreducibility

Let Q be a finite set. Let Y be a B^Q-coalgebra equipped with the structure map $L : Y \to YB^Q$. For elements y, y' of Y, the element y' is said to be *reachable* from y in Y if there is an element q of Q such that y' appears in the support of the distribution $qL(y)$ on Y. The *reachability graph* of Y is the directed graph of the reachability relation on Y. The coalgebra Y is said to be *irreducible* if its reachability graph is strongly connected.

PROPOSITION 5.3

If $P\backslash Q$ is a homogeneous space over a finite quasigroup Q, realised as a B^Q-coalgebra according to Corollary 5.1, then $P\backslash Q$ is irreducible.

PROOF Let H be the relative left multiplication group of P in Q. For an arbitrary pair x, x' of elements of Q, consider the corresponding elements xH and $x'H$ of $P\backslash Q$. For $q = x\backslash x'$ in Q, the element $x'H$ then appears in the support of $qL(xH)$. □

COROLLARY 5.5

Let Q be a finite quasigroup. Suppose that Y is a B^Q-coalgebra that is a homomorphic image of a homogeneous space S over Q. Then Y is irreducible.

PROOF Since S and Y are finite, one may use the correspondence of Theorem 5.3. Let $\phi : S \to Y$ be the homomorphism, with incidence matrix F. Consider elements y and y' of Y. Suppose x and x' are elements of S with $x\phi = y$ and $x'\phi = y'$. By Proposition 5.3, there is an element q of Q with x' in the support of the distribution $xR_S(q)$. Then $yR_Y(q) = xFR_Y(q) = xR_S(q)F$, so the support of $yR_Y(q)$, as the image of the support of $xR_S(q)$ under ϕ, contains $x'\phi = y'$. □

For a group Q, each homogeneous space $(P\backslash Q, Q)$ is obtained as a homomorphic image of the regular homogeneous space $(\{1\}\backslash Q, Q)$. The following considerations show that the corresponding property does not hold for general quasigroups.

DEFINITION 5.3 *Let Q be a finite set. A Q-IFS (X, Q) is said to be* crisp *if, for each q in Q, the action matrix $R_X(q)$ is a* 0-1*-matrix. Then a B^Q-coalgebra $L : X \to XB^Q$ is said to be* crisp *if its structure map corestricts to $L : X \to X^Q$.*

Note that crisp Q-IFS and finite crisp B^Q-coalgebras correspond under the isomorphism of Theorem 5.3. (Compare Exercise 6.)

PROPOSITION 5.4
A homomorphic image of a finite crisp B^Q-coalgebra is crisp.

PROOF Using Theorem 5.3, it is simpler to work in the category $\mathbf{IFS}_Q$. Let $\phi : X \to Y$ be a surjective $\mathbf{IFS}_Q$-morphism with incidence matrix F and crisp domain. For an element y of Y, suppose that x is an element of X with $x\phi = y$. Then for each element q of Q, one has $yR_Y(q) = x\phi R_Y(q) = xFR_Y(q) = xR_X(q)F$, using (5.4) for the last step. Since X is crisp, there is an element x' of X with $xR_X(q) = x'$. Then $yR_Y(q) = x'F = y'$ for the element $y' = x'\phi$ of Y. Thus Y is also crisp. □

For each finite quasigroup Q, the regular homogeneous space $\varnothing\backslash Q$ determines the *regular* (*permutation*) *representation* $(\varnothing\backslash Q, Q)$ or (Q, Q). This permutation representation is crisp. On the other hand, the homogeneous space exhibited in Section 4.2 is not crisp. Proposition 5.4 shows that such spaces are not homomorphic images of the regular representation.

5.4 The covariety of Q-sets

DEFINITION 5.4 *Let Q be a finite quasigroup. Then the* category $\underline{\underline{Q}}$ of Q-sets *is defined to be the covariety of B^Q-coalgebras generated by the (finite) set of homogeneous spaces over Q. Coalgebra homomorphisms between Q-sets are described as* Q-homomorphisms. *A* permutation representation *of Q is a finite Q-set.*

For a finite quasigroup Q, the terms (finite) "Q-set" or "permutation representation of Q" are used for finite objects of the category of Q-sets, and also for those Q-IFS which correspond to finite Q-sets via Theorem 5.3.

THEOREM 5.4
For a finite quasigroup Q, the Q-sets are precisely the sums of homomorphic images of homogeneous spaces.

PROOF Let $\mathcal{H}$ be the set of homogeneous spaces over Q. By [70, Prop. 2.4], the covariety generated by $\mathcal{H}$ is $\mathsf{HS\Sigma}(\mathcal{H})$. By [70, Prop. 2.5], the operators

S and Σ commute. By Proposition 5.3, the homogeneous spaces do not contain any proper, nonempty subcoalgebras. Thus the covariety generated by $\mathcal{H}$ becomes $\mathsf{H}\Sigma(\mathcal{H})$. By [70, Prop. 2.4(iii)], one has $\Sigma\mathsf{H}(\mathcal{H}) \subseteq \mathsf{H}\Sigma(\mathcal{H})$. It thus remains to be shown that each homomorphic image of a sum of homogeneous spaces is a sum of homomorphic images of homogeneous spaces.

Let Y be a Q-set, with structure map L_Y, that is a homomorphic image of a sum X of homogeneous spaces under a homomorphism ϕ. It will first be shown that each element y of Y lies in a subcoalgebra Y_y of Y that is a homomorphic image of a homogeneous space. Since y lies in the image Y of X under ϕ, there is an element x of X such that $x\phi = y$. Since X is a sum of homogeneous spaces, the element x lies in such a space S. Consider the restriction of ϕ to S. Let Y_y be the image of this restriction. Then Y_y is a subcoalgebra of Y that is a homomorphic image of a homogeneous space (cf. [68, Lemma 4.5]).

Now suppose that for elements y and z of Y, the corresponding images Y_y and Y_z of homogeneous spaces intersect nontrivially, say with a common element t. By Corollary 5.5, there is an element q of Q such that z lies in the support of $qL_Y(t)$. On the other hand, since t lies in the subcoalgebra Y_y, the support of the distribution $qL_Y(t)$ lies entirely in Y_y. Thus z is an element of Y_y, and for each q in Q, the support of the distribution $qL_Y(z)$ lies entirely in Y_y. It follows that Y_z is entirely contained in Y_y. Similarly, one finds that Y_y is contained in Y_z, and so the two images agree. Thus Y is a sum of such images. □

COROLLARY 5.6

A finite quasigroup Q has only finitely many isomorphism classes of irreducible Q-sets.

PROOF By Theorem 5.4, the irreducible Q-sets are precisely the homomorphic images of homogeneous spaces. Since Q is finite, it has only finitely many homogeneous spaces. The (First) Isomorphism Theorem for coalgebras (cf. [68, Th. 4.15]) then shows that each of these homogeneous spaces has only finitely many isomorphism classes of homomorphic images. □

COROLLARY 5.7

For a finite group Q, the quasigroup Q-sets coincide with the group Q-sets.

PROOF For a group Q, each homomorphic image of a homogeneous space is isomorphic to a homogeneous space, and each group Q-set is isomorphic to a sum of homogeneous spaces. □

In considering the final corollary of Theorem 5.4, it is helpful to recall that

the intersection of a family of subcoalgebras of a coalgebra is not necessarily itself a subcoalgebra (cf. [68, Cor. 4.9]).

COROLLARY 5.8
Let y be an element of a Q-set Y over a finite quasigroup Q. Then the intersection of all the subcoalgebras of Y containing the element y is itself a subcoalgebra of Y.

PROOF In the notation of the proof of Theorem 5.4, this intersection is the subcoalgebra Y_y. □

DEFINITION 5.5 *Consider a Q-set Y over a finite quasigroup Q.*

(a) *The irreducible summands of Y given by Theorem 5.4 are called the* orbits *of Y.*

(b) *For an element y of Y, the smallest subcoalgebra of Y containing y is called the* orbit *of the element y. (Note that such a coalgebra is guaranteed to exist by Corollary 5.8.)*

(c) *A permutation representation Y is said to be* transitive *if it consists of a single orbit.*

5.5 The Burnside algebra

By definition, the category $\underline{\underline{Q}}$ of Q-sets is closed under coalgebra sums, as described in Appendix C.1. Thus the sum of two sums of images of homogeneous spaces is immediately obtained as a new sum of images of homogeneous spaces. In particular, the underlying set of a sum of Q-sets is the disjoint union of their underlying sets. However, as shown by examples such as those in Section 5.6 below, the tensor product of two homogeneous spaces over Q in $\mathbf{IFS}_Q$ need not decompose as a sum of images of homogeneous spaces. By Corollary 5.4, it also follows that the direct product will not decompose as such a sum either. Nevertheless, the category $\underline{\underline{Q}}$ is actually bicomplete (Proposition 5.2). Limits in the covariety $\underline{\underline{Q}}$ are constructed by a procedure dual to that used for the construction of colimits in a (pre)variety of τ-algebras of a given type τ (compare [165, §IV.2.2]). That procedure first builds the corresponding colimit L in the category $\underline{\tau}$ of all τ-algebras, and then takes the replica of L in the (pre)variety, its largest homomorphic image lying in the (pre)variety. Given a B^Q-coalgebra L, its replica in $\underline{\underline{Q}}$ is obtained dually

as the largest subcoalgebra of L that lies in the covariety $\underline{\underline{Q}}$. In particular, given two finite Q-sets X and Y, their *product* $X \times Y$ in $\underline{\underline{Q}}$ is formed as the largest $\underline{\underline{Q}}$-subcoalgebra contained in the product of X and Y in the category of all $B^{\underline{\underline{Q}}}$-coalgebras. Note that the underlying set of a product of Q-sets is not necessarily the product of their underlying sets. (A specific example is exhibited at the end of Section 5.6 below.) In similar fashion the *restricted tensor product* $X \widehat{\otimes} Y$ of X and Y is defined to be the largest $\underline{\underline{Q}}$-subcoalgebra contained in the bisimulation $X \otimes Y$.

For a finite Q-set X, let $[X]$ denote its isomorphism type in the category $\underline{\underline{Q}}$. Let $A^+(Q)$ denote the set of all such isomorphism types. Let B be the set of so-called *basic* types, the isomorphism types of homomorphic images of homogeneous spaces over Q. It is often convenient to consider each element b of B as represented by a specified Q-set H_b. Now

$$\forall\ [X] \in A^+(Q),\ \forall\ b \in B,\ \exists\ n_b \in \mathbb{N}.\ [X] = \sum_{b \in B} n_b b. \tag{5.18}$$

An inner product is defined on $A^+(Q)$ by

$$\left\langle \sum_{b \in B} m_b b, \sum_{b \in B} n_b b \right\rangle = \sum_{b \in B} m_b n_b. \tag{5.19}$$

With respect to this inner product, the set of basic types is orthonormal. The equation of (5.18) may then be rewritten as

$$[X] = \sum_{b \in B} \langle b, [X] \rangle b. \tag{5.20}$$

THEOREM 5.5
Let Q be a finite quasigroup.

1. *The set $A^+(Q)$ forms a commutative unital semiring, with zero $[\varnothing]$ and unit $[\{1\}]$, under the sum $[X] + [Y] = [X + Y]$ and each of the following multiplications:*
   (a) *the* (direct) product $[X] \cdot [Y] = [X \times Y]$, *and*
   (b) *the* restricted tensor product $[X] \widehat{\otimes} [Y] = [X \widehat{\otimes} Y]$.
2. *The $\mathbb{N}$-semimodule $A^+(Q)$ is free over the basis B.*
3. $\forall\ x, y, z \in A^+(Q),\ \langle x, y \widehat{\otimes} z \rangle \leq \langle x, y \cdot z \rangle$.

PROOF Statement (2) follows by Theorem 5.4, and statement (3) by Corollary 5.4. Most of the statement (1) is routine, following by standard properties of sums and products in bicomplete categories. For the distributive

law with the reduced tensor product, consider Q-sets X, Y, Z. Then for each q in Q, the matrix $(R_X(q) \oplus R_Y(q)) \otimes R_Z(q)$ is permutationally similar to $(R_X(q) \otimes R_Z(q)) \oplus (R_Y(q) \otimes R_Z(q))$, so that the Q-IFS $(X + Y) \otimes Z$ and $(X \otimes Z) + (Y \otimes Z)$ are isomorphic. Since these Q-IFS contain the same irreducible summands from $\underline{\underline{Q}}$, with the same multiplicities, the distributive law in $(A^+(Q), +, \widehat{\otimes})$ follows. □

The mark concept introduced for quasigroups in the following definition is a natural extension of Burnside's original [23, §180].

DEFINITION 5.6 *Let Q be a finite quasigroup, and let X be a Q-set. For each basic Q-set type $b = [H_b]$, the* mark *of b in X or $x = [X]$ is defined to be the cardinality*

$$Z_{xb} = \left|\underline{\underline{Q}}(H_b, X)\right| \tag{5.21}$$

of the set of Q-homomorphisms from H_b to X. The mark matrix *or Z-*matrix *Z or Z_Q of Q is the $|B| \times |B|$ matrix $[Z_{bc}]$ for b and c in B.*

PROPOSITION 5.5
For x, y in $A^+(Q)$ and b in B:

1. $Z_{(x\cdot y)b} = Z_{xb} Z_{yb}$;
2. $Z_{(x+y)b} = Z_{xb} + Z_{yb}$;
3. $Z_{xb} = \sum_{a \in B} \langle a, x \rangle Z_{ab}$.

PROOF Suppose $x = [X]$ and $y = [Y]$.
(1) is an immediate consequence of the definition (5.21) and the universality property of products:

$$\left|\underline{\underline{Q}}(H_b, X \times Y)\right| = \left|\underline{\underline{Q}}(H_b, X)\right| \cdot \left|\underline{\underline{Q}}(H_b, Y)\right| .$$

(2): The image of a Q-homomorphism from H_b to $X + Y$ is either a summand of X, or else a summand of Y. Thus

$$\left|\underline{\underline{Q}}(H_b, X + Y)\right| = \left|\underline{\underline{Q}}(H_b, X)\right| + \left|\underline{\underline{Q}}(H_b, Y)\right|.$$

(3) follows directly from (2) and (5.20). □

COROLLARY 5.9
The product of two finite Q-sets is finite.

PROOF Using notation as in the proof of Proposition 5.5, suppose that X and Y are finite. Then for each basic type b, the marks Z_{xb} and Z_{yb} are

finite. By (1) of Proposition 5.5, the mark $Z_{(x\cdot y)b}$ is finite, so that $X \times Y$ can only contain finitely many summands of type b. □

REMARK 5.1 Corollary 5.9 contrasts with examples constructed as in [71, Prop. 9.4], where for a bounded endofunctor F preserving weak pullbacks, it may still happen that a product of finite F-coalgebras is infinite. On the other hand, Section 5.6 exhibits two nonempty Q-sets X, Y whose product is empty. Indeed, this will happen whenever there is no Q-set H that is the domain of homomorphisms to both X and Y. □

PROPOSITION 5.6
With notation as in Definition 5.6:

1. *The set B may be ordered so that Z is triangular.*

2. *The Z-matrix is invertible over $\mathbb{Q}$.*

PROOF (1): Linearly order B by increasing order of the cardinality of the representing Q-set, so that $b = [H] \leq [K] = c$ in B iff $|H| \leq |K|$. Then for $b > c \in B$, one has $|K| \leq |H|$. Suppose that

$$0 < Z_{bc} = \left|\underline{\underline{Q}}(K, H)\right|. \tag{5.22}$$

Now H is irreducible [161, Cor. 7.3], so there can be a Q-homomorphism $f : K \to H$ in (5.22) only if $|H| = |K|$ and f bijects. Let F be the invertible incidence matrix of f. Then

$$\begin{aligned} &\forall\ q \in Q,\ FR_K(q) = R_H(q)F \\ &\quad \Rightarrow \forall\ q \in Q,\ R_K(q)F^{-1} = F^{-1}R_H(q), \end{aligned}$$

so that f is a Q-isomorphism. This yields the contradiction $b = [H] = [K] = c$ to the hypothesis $b > c$ of (5.22). Thus with the ordering of B as given, the Z-matrix is upper triangular.
(2): For $b = [H] \in B$, the identity map 1_H lies in $\underline{\underline{Q}}(H, H)$, so the diagonal entries of the triangular matrix Z are all nonzero. □

THEOREM 5.6
Let Q be a finite quasigroup, with set B of basic types of Q-set. Then the mark map

$$(A^+(Q), +, \cdot) \to \mathbb{Q}^B; x \mapsto (b \mapsto Z_{xb}) \tag{5.23}$$

is an embedding of semirings.

PROOF By Proposition 5.5(1)(2), the mark map is a semiring homomorphism. To see that it injects, use Proposition 5.5(3) to consider it in the equivalent form

$$(A^+(Q),+,\cdot) \to \mathbb{Q}^B; x \mapsto \Big(b \mapsto \sum_{a\in B} \langle a,x\rangle Z_{ab}\Big). \tag{5.24}$$

Apply Proposition 5.6 and note that

$$\sum_{c\in B}\sum_{b\in B}\Big(\sum_{a\in B}\langle a,x\rangle Z_{ab}\Big)Z^{-1}_{bc}c = \sum_{c\in B}\langle c,x\rangle c = x$$

by (5.20). □

COROLLARY 5.10

Define $A(Q)$ as the $\mathbb{Q}$-vector space with basis B. Note that $A(Q)$ contains the free $\mathbb{N}$-semimodule $A^+(Q)$ of Theorem 5.5(2) as a subreduct. Then $A(Q)$ carries a $\mathbb{Q}$-algebra structure $(A(Q),+,\cdot)$ such that:

(a) *The semiring $(A^+(Q),+,\cdot)$ is identified as a subreduct of the $\mathbb{Q}$-algebra $(A(Q),+,\cdot)$;*

(b) *The mark map* (5.23) *extends to a $\mathbb{Q}$-algebra isomorphism*

$$(A(Q),+,\cdot) \to \mathbb{Q}^B; \sum_{a\in B} r_a a \mapsto \Big(b \mapsto \sum_{a\in B} r_a Z_{ab}\Big). \tag{5.25}$$

Furthermore, the reduced tensor product operation $\widehat{\otimes}$ extends by linearity from $A^+(Q)$ to $A(Q)$, yielding a $\mathbb{Q}$-algebra $(A(Q),+,\widehat{\otimes})$.

DEFINITION 5.7 *For a finite quasigroup Q, the* (rational) Burnside algebra *is defined to be the double $\mathbb{Q}$-algebra $(A(Q),+,\cdot,\widehat{\otimes})$ of Corollary 5.10.*

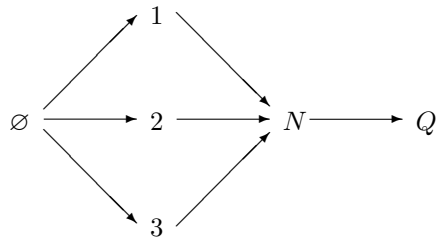
PROPOSITION 5.7

Let Q be a finite group. Then the two products on the Burnside algebra of Q in the quasigroup sense of Definition 5.7 coincide, yielding the Burnside algebra of Q in the classical group sense.

PROOF By Corollary 5.7, the quasigroup actions of Q coincide with the group actions of Q. □

5.6 An example

For a finite quasigroup Q, the isomorphism (5.25) shows that the reduct $(A(Q), +, \cdot)$ of the Burnside algebra is semisimple. The example of this section shows that the reduct $(A(Q), +, \widehat{\otimes})$ need not be semisimple. Consider the quasigroup Q whose multiplication table is displayed in Figure 1.2 (p. 2). Denote the singleton subquasigroups $\{1\}, \{2\}, \{3\}$ by their elements. The poset of subquasigroups is



with $N = \{1, 2, 3\}$. The 3-element homogeneous spaces $1 \setminus Q$, $2 \setminus Q$, and $3 \setminus Q$ all have the same isomorphism type x_3. This is the space studied in Section 4.2. Let the homogeneous spaces $Q\backslash Q$, $N\backslash Q$, and $\varnothing\backslash Q$ have respective isomorphism types x_1, x_2, and x_6. Thus the index on each isomorphism type denotes the cardinality of the corresponding Q-set. Note that x_6 is the isomorphism type of the regular homogeneous space $\varnothing \setminus Q$. There are no other quotients of homogeneous spaces, so the Burnside algebra $A(Q)$ has $\{x_1, x_2, x_3, x_6\}$ as a basis. The restricted tensor products of these basic elements, computed as described in Section 5.5, are listed in Figure 5.1.

$(A(Q), \widehat{\otimes})$	x_1	x_2	x_3	x_6
x_1	x_1			
x_2	x_2	$2x_2$		
x_3	x_3	$2x_3$	0	
x_6	x_6	$2x_6$	0	x_6

FIGURE 5.1: Restricted tensor products.

For example, the tensor square of $1 \setminus Q = \{a, b, c\}$ in $\underline{\underline{\mathrm{IFS}}}_Q$ has a Markov matrix given by (5.2) and (5.7) as $\frac{1}{6}\sum_{q\in Q} R_{1\setminus Q}(q) \otimes R_{1\setminus Q}(q)$. This Markov matrix, displayed as

$$\frac{1}{6}\begin{bmatrix}
1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 3 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 3 \\
0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 3 \\
\frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & \frac{3}{2} & 0 & 0 & 0 & 3 \\
0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 \\
0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 \\
0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 \\
\frac{1}{3} & \frac{2}{3} & 0 & \frac{2}{3} & \frac{4}{3} & 0 & 0 & 0 & 3
\end{bmatrix} \tag{5.26}$$

with respect to the ordered basis

$$\{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\},$$

is permutationally similar to the direct sum of two Markov matrices, one on the set

$$\{(a,a),(a,b),(b,a),(b,b),(c,c)\}$$

and one on the set

$$\{(a,c),(b,c),(c,a),(c,b)\}.$$

Since there are no (quotients of) homogeneous spaces with cardinality 4 or 5, the restricted tensor square of $1 \setminus Q$ is the empty Q-set. Thus $x_3^2 = 0$ in $(A(Q), \widehat{\otimes})$.

From Figure 5.1, it is apparent that the Jacobson radical of $(A(Q), +, \widehat{\otimes})$ is spanned by x_3. The semisimple part of $(A(Q), +, \widehat{\otimes})$ is spanned by the complete set

$$\{1 - \frac{x_2}{2}, \frac{x_2}{2} - x_6, x_6\} \tag{5.27}$$

of primitive idempotents. Corollary 5.12 below implies that $x_6 \cdot x_6 = x_6$, so the underlying set of the product $\underline{\underline{Q}}$-set $\varnothing\backslash Q \times \varnothing\backslash Q$ is not the direct square of the set $\varnothing\backslash Q$. Indeed, the Z-matrix for this example is

$$Z = \begin{bmatrix}
1 & 1 & 1 & 1 \\
0 & 2 & 2 & 2 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix} \tag{5.28}$$

with respect to the ordering

$$B = \{x_1 < x_2 < x_3 < x_6\}$$

of Proposition 5.6, while the full set of direct products of basic elements is given by Figure 5.2.

$(A(Q),\cdot)$	x_1	x_2	x_3	x_6
x_1	x_1			
x_2	x_2	$2x_2$		
x_3	x_3	$2x_3$	x_3	
x_6	x_6	$2x_6$	0	x_6

FIGURE 5.2: Direct products.

5.7 Idempotents

The isomorphism (5.25) gives an immediate description of the complete set of primitive idempotents for the semisimple reduct $(A(Q),+,\cdot)$ of the rational Burnside algebra of a finite quasigroup Q.

THEOREM 5.7
Let Q be a finite quasigroup, with mark matrix Z and set B of basic isomorphism types of Q-sets. For each element a of B, define the element

$$E_a = \sum_{b\in B} Z^{-1}_{ab} b \tag{5.29}$$

of $A(Q)$. Then $\{E_a \mid a \in B\}$ is a complete set of primitive idempotents for $(A(Q),+,\cdot)$.

PROOF Under (5.25), the element E_a of (5.29) maps to

$$c \mapsto \sum_{b\in B} Z^{-1}_{ab} Z_{bc} = \delta_{ac}. \tag{5.30}$$

Thus as a ranges through B, the elements (5.30) range through a complete set of primitive idempotents of $\mathbb{Q}^B$. □

COROLLARY 5.11
Let r be the (basic) type of the regular homogeneous space $[\varnothing\backslash Q]$. Then

$$E_r = Z^{-1}_{rr} r \tag{5.31}$$

is a primitive idempotent of $(A(Q),+,\cdot)$.

PROOF Apply Proposition 5.6(1): $Z_{rb} = 0$ for $r \neq b \in B$. □

In contrast with Theorem 5.7, the structure of the other $\mathbb{Q}$-algebra reduct $(A(Q), +, \widehat{\otimes})$ of the rational Burnside algebra of a finite quasigroup Q is not yet known (Problem 3). If Q is a group, then the reduct $(A(Q), +, \widehat{\otimes})$ contains a primitive idempotent that may be written in quasigroup terms as

$$|Q|^{-1}[\varnothing \setminus Q]. \tag{5.32}$$

Consider the example presented in Section 5.6. There, as described by (5.27), it is $r = x_6$ or $[\varnothing \setminus Q]$ itself which is a restricted tensor idempotent. Certainly some multiple of the isomorphism type of the regular permutation representation is always a primitive restricted tensor idempotent. (Indeed, for $r \neq b \in B$, one has $0 \leq \langle b, r \widehat{\otimes} r \rangle \leq \langle b, r \cdot r \rangle = 0$ by Theorem 5.5(3) and Corollary 5.11.) In the remainder of this section, the exact multiple will be specified. By Corollary 5.12 below, it turns out to agree with (5.31).

For a transitive action of a group G on a set Q, the *orbitals* of G on Q are defined as the orbits of G in its diagonal action on Q^2. Each orbital, as a subset of Q^2, represents a binary relation on Q. Such a relation ρ is said to be *functional* if it is the graph of a function. In other words, for each element x of Q, there is a unique element y of Q such that $(x, y) \in \rho$. In this case, the unique element y with $(x, y) \in \rho$ is written as $x\rho$.

THEOREM 5.8

Let Q be a finite, nonempty quasigroup. Let f be the number of functional orbitals in the action of the right multiplication group of Q. Then

$$\frac{1}{f}\,[\varnothing \setminus Q] \tag{5.33}$$

is a primitive restricted tensor idempotent of the rational Burnside algebra of the quasigroup Q.

PROOF Let G be the right multiplication group of Q. First note that the equality relation on Q is always a functional orbital of G on Q, so that $f \geq 1$ and (5.33) is well-defined. (Incidentally, the minimal case $f = 1$ is represented by the example of Section 5.6.)

For an element q of Q, the regular action matrix of q is expressed as the sum

$$R_{\varnothing \setminus Q}(q) = \sum_{x \in Q} E^{x,xq}$$

of elementary matrices. Then

$$R_{\varnothing \setminus Q}(q) \otimes R_{\varnothing \setminus Q}(q) = \Big[\sum_{x \in Q} E^{x,xq} \Big] \otimes \Big[\sum_{y \in Q} E^{y,yq} \Big]$$

$$= \sum_{(x,y) \in Q^2} E^{x,xq} \otimes E^{y,yq} = \sum_{(x,y) \in Q^2} E^{(x,y),(xq,yq)}.$$

Thus the Q-IFS $(\varnothing\backslash Q)\otimes(\varnothing\backslash Q)$ decomposes as a direct sum of subcoalgebras, one for each orbital of G on Q. These subcoalgebras are certainly irreducible. Each nonfunctional orbital is too large to be a homomorphic image of a homogeneous space of Q. Thus the restricted tensor square of $\varnothing \setminus Q$ in $\underline{\underline{Q}}$ contains at most f summands, corresponding to the functional orbitals of $\overline{G}$ on Q. It will now be shown that each of these summands is isomorphic to the regular homogeneous space.

Let ρ be a functional orbital of G on Q. Define a function

$$\phi : \varnothing \setminus Q \to \rho\,; \{x\} \mapsto (x, x\rho). \tag{5.34}$$

Certainly ϕ bijects. Consider elements x and q of Q. Since ρ is an orbital of G on Q, the image $(xq, x\rho q)$ of the element $(x, x\rho)$ of ρ under the diagonal action of right multiplication by q is again an element of ρ. Thus

$$xq\rho = x\rho q. \tag{5.35}$$

Then

$$\{x\}R_{\varnothing\backslash Q}(q)\phi = \{xq\}\phi = (xq, xq\rho) = (xq, x\rho q) = \{x\}\phi R_\rho(q)\,.$$

Comparing with (5.4), it is apparent that (5.34) yields an isomorphism of Q-IFS. Since this happens for each of the f functional orbitals of G on Q, one has

$$[\varnothing \setminus Q]\widehat{\otimes}[\varnothing \setminus Q] = f[\varnothing \setminus Q]$$

in the Burnside algebra of Q. The idempotence of (5.33) follows.

Finally, consider the restricted tensor product of $\varnothing\backslash Q$ with any other homomorphic image of a homogeneous space. Each irreducible summand of such a product has at least as many elements as Q, since it projects onto the regular representation in $\mathbf{IFS}_Q$. Thus the only such summands in $\underline{\underline{Q}}$ are isomorphic to the regular representation. In the rational Burnside algebra, this means that the principal reduced tensor ideal generated by (5.33) is minimal, namely the set of rational multiples of (5.33). Thus (5.33) is a primitive restricted tensor idempotent. □

COROLLARY 5.12

The idempotent elements (5.31) *of* $(A(Q), +, \cdot)$ *and* (5.33) *of* $(A(Q), +, \widehat{\otimes})$ *agree.*

PROOF By (5.35), the functional orbits are exactly the graphs of the various $\underline{\underline{Q}}$-automorphisms of the regular space $\varnothing\backslash Q$. On the other hand, each $\underline{\underline{Q}}$-endomorphism of $\varnothing\backslash Q$ bijects, so $Z_{rr} = f$. □

Using Theorem 5.8, one may give a characterization of those quasigroups Q for which the group formula (5.32) yields a primitive restricted tensor idempotent of the rational Burnside algebra. They are the right quasiloops isotopic to groups, as described by Theorem 4.3.

PROPOSITION 5.8
Let $(Q, \cdot)$ be a finite, nonempty quasigroup with right multiplication group G. Then the following conditions are equivalent:

(a) *The element*
$$|Q|^{-1}[\varnothing \setminus Q].$$
is a direct product idempotent of the rational Burnside algebra of $(Q, \cdot)$;

(b) *The element*
$$|Q|^{-1}[\varnothing \setminus Q].$$
is a restricted tensor idempotent of the rational Burnside algebra of $(Q, \cdot)$;

(c) *The group G acts regularly on Q;*

PROOF (a)⇔(b) follows by Corollary 5.12.

(b)⇔(c): By Theorem 5.8, (5.32) is a restricted tensor idempotent if and only if all the orbitals of G are functional. This happens if and only (c) holds. □

Example 5.2
The equivalent conditions of Proposition 5.8 on a quasigroup Q are not enough to guarantee that the entire rational Burnside algebra of Q will be semisimple. For example, consider the set Q of integers modulo 4, under the operation of subtraction. It forms a right quasiloop isotopic to the group $(\mathbb{Z}/4\mathbb{Z}, +)$, since (4.28) holds with $+$ as the usual addition and λ as negation. On the other hand, the isomorphism type of the homogeneous space $\{0\} \setminus Q$ is a nonzero element of the Jacobson radical of the reduct $(A(Q), +, \widehat{\otimes})$. □

5.8 Burnside's Lemma

The classical Burnside Lemma for a finite group Q (compare Theorem 3.1.2 in [165, Ch. I], for example) states that the number of orbits in a permutation representation X is equal to the average number of points of X fixed by elements q of Q. This section presents the generalization of Burnside's Lemma to quasigroup permutation representations. For a permutation representation

X of a finite quasigroup Q, the formulation and proof of Burnside's Lemma rely on the identification given by Theorem 5.3. The number of points fixed by a group element q is equal to the trace of the permutation matrix of q on X. In the IFS terminology of Section 5.1, this permutation matrix is the action matrix $R_X(q)$ of q on the corresponding Q-IFS (X, Q). Thus the following theorem specializes to the classical Burnside Lemma in the associative case.

THEOREM 5.9 (***Quasigroup Burnside Lemma***)
Let X be a finite Q-set over a finite, nonempty quasigroup Q. Then the trace of the Markov matrix of X is equal to the number of orbits of X.

PROOF Consider the Q-IFS (X, Q). By Theorem 5.3, Theorem 5.4, and (5.5), its Markov matrix decomposes as a direct sum of the Markov matrices of its orbits. Thus it suffices to show that the trace of the Markov matrix of a homomorphic image of a homogeneous space is equal to 1.

Consider a Q-set $Y = \{y_1, \ldots, y_m\}$ which is the image of a homogeneous space $P\backslash Q$ under a surjective homomorphism $\varphi : P\backslash Q \to Y$ with incidence matrix F. Let F^+ be the pseudoinverse of F. By Proposition 4.1, each row sum of F^+ is 1. Suppose that the Markov matrix Π of $P\backslash Q$ is given by (4.19). By (5.4), one has

$$R_Y(q) = F^+ R_{P\backslash Q}(q) F$$

for each q in Q. Thus the trace of the Markov matrix of Y is given by

$$\begin{aligned}
\mathrm{Tr}(F^+ \Pi F) &= \sum_{i=1}^{m} \sum_{j=1}^{r} \sum_{k=1}^{r} F^+_{ij} \Pi_{jk} F_{ki} \\
&= |Q|^{-1} \sum_{i=1}^{m} \left(\sum_{j=1}^{r} F^+_{ij} \right) \left(\sum_{k=1}^{r} |P_k| F_{ki} \right) \\
&= |Q|^{-1} \sum_{k=1}^{r} |P_k| = 1,
\end{aligned}$$

the penultimate equality following since for each $1 \le k \le r$, there is exactly one index i (corresponding to $P_k \varphi = y_i$) such that $F_{ki} = 1$, the other terms of this type vanishing. □

REMARK 5.2 Burnside's Lemma may fail for a Q-IFS which does not correspond to a Q-set. For example, consider the tensor square $1\backslash Q \otimes 1\backslash Q$ of the homogeneous space $1\backslash Q$ of Section 5.6. The trace of the Markov matrix (5.26) of $1\backslash Q \otimes 1\backslash Q$ is not even integral. □

5.9 Exercises

1. Let Q and X be finite sets. Show that the following are equivalent:

   (a) X is a Q-IFS;

   (b) There is a function

   $$X \times Q \times X \to I; (x, q, y) \mapsto \mathrm{Prob}\big(xq = y\big) \tag{5.36}$$

   such that

   $$\sum_{y \in X} \mathrm{Prob}\big(xq = y\big) = 1$$

   for each x in X and q in Q;

   (c) There is a function $X \times Q \to XB$.

2. Show that if X is an infinite set, then condition (c) of Exercise 1 is equivalent to condition (b) with the restriction that for each x in X and q in Q, the probability distribution

   $$\big\{\mathrm{Prob}\big(xq = y\big) \,\big|\, y \in Q\big\}$$

   has finite support.

3. For elements x, y of the closed unit interval $I = [0, 1]$, define

   $$x \to y = \begin{cases} 1 & \text{if } x \leq y\,; \\ y/x & \text{otherwise.} \end{cases} \tag{5.37}$$

   (a) Show that (5.37) is well defined.

   (b) Show that the skew-associativity identity (5.11) may be rewritten in the equivalent form

   $$xy\,\underline{p}\,z\,\underline{q} = x(\,yz\,\underline{p \circ q \to q}\,)\,\underline{p \circ q}\,. \tag{5.38}$$

4. Suppose that (A, I°) is a barycentric algebra. Extend the definition of (5.8) to the case of general p in I by setting $xy\,\underline{0} = x$ and $xy\,\underline{1} = y$. Consider the resulting algebra (A, I).

   (a) Show that (A, I) satisfies the idempotence identity (5.9) and the skew commutativity identity (5.10) for all p in I.

   (b) Show that (A, I) satisfies the new skew associativity identity (5.38) for all p, q in I.

5. Show that the Q-IFS X of Exercise 1 is crisp if and only if (5.36) corestricts to the boundary $\{0, 1\}$ of I.

6. Show that the Q-IFS X of Exercise 1 is crisp if and only if the function of (c) maps to the extreme points of the simplex XB.

7. Show that the category of $\varnothing$-IFS is equivalent to the category of finite sets.

8. Show that the structure map of a $B^{\varnothing}$-coalgebra X is the unique morphism from X to the (singleton) terminal object of the category of sets.

9. Show that each $B^{\varnothing}$-coalgebra X is crisp.

10. Let Q be a singleton quasigroup.

    (a) Identify the category of Q-IFS as the category of finite probabilistic dynamical systems.

    (b) Show that the category of Q-sets is equivalent to the category of sets.

11. Let P be a subset of a finite set Q. Given a B^Q-coalgebra X with structure map $\alpha : X \to XB^Q$, show that concatenation with the projection $\downarrow_P^Q\colon XB^Q \to XB^P$ yields a B^P-coalgebra $X\downarrow_P^Q$ with structure map $\alpha\downarrow_P^Q\colon X \to XB^P$.

12. If P is a subquasigroup of a quasigroup Q, show that the restriction $\downarrow_P^Q$ of Exercise 11 does not yield a functor from $\underline{\underline{Q}}$ to $\underline{\underline{P}}$.

13. Show that a finite, nonempty quasigroup Q may be recovered from the covariety $\underline{\underline{Q}}$ of Q-sets. (Hint: By Theorem 5.4, the largest irreducible Q-set is the regular space $\varnothing\backslash Q$. Apply Proposition 4.3.)

14. Verify the claims of Example 5.2.

15. Verify the form of the Z-matrix (5.28), and the table of direct products in Figure 5.2.

16. Confirm the validity of the Quasigroup Burnside Lemma for a 2-element quasigroup homogeneous space. (Compare Exercise 3 in Chapter 4.)

17. Determine which of the results of Chapters 4 and 5 remain valid for left quasigroups. (Recall that for an element q of a left quasigroup Q, the matrix $R_Q(q)$ will be a 0-1-matrix, but not necessarily a permutation matrix. In particular, the property of Exercise 2 in Chapter 4 will not hold in general.)

5.10 Problems

1. Despite the negative result of Exercise 12, is it still possible to develop a theory of restriction and induction for permutation representations of quasigroups?

2. Does the wreath product construction (compare [165, p. 40]) extend to quasigroup permutation representations?

3. For a finite quasigroup Q, specify a basis for the Jacobson radical and a complete set of primitive idempotents for the semisimple part of the reduct $(A(Q), +, \widehat{\otimes})$ of the rational Burnside algebra.

5.11 Notes

Section 5.2

Since the action matrices of quasigroup homogeneous spaces have rational entries, it actually suffices to consider $\mathrm{End}_{\mathbb{Q}}(\mathbb{Q}X)$ in the definition (5.1) of Q-IFS, and *rational barycentric algebras*, in which the operators p are taken from the rational unit interval $\mathbb{Q} \cap I^{\circ}$, for the specification of the free algebra functor B. The equivalent structures in Theorem 5.2 will then be the free rational barycentric algebra XB on a set X, the set of all finitely-supported rational probability distributions on X, and the rational simplex spanned by X. These restrictions of the general framework would have no effect on the specification of Q-sets in Section 5.4.

Section 5.4

For a finite loop Q, the term "Q-set" was used in a different, essentially broader sense — at least for the finite case — in [162, Defn. 5.2]. If necessary, one may refer to "loop Q-sets" in that context, and to "proper Q-sets" or "quasigroup Q-sets" in the present context.

Section 5.7

Theorem 5.7 generalizes the specifications of the primitive idempotents of group Burnside algebras that have appeared in the literature [65], [178].

Section 5.8

It has become customary to remark that "Burnside's Lemma" was already known to Cauchy and Frobenius. However, the popular names of mathematical results have never been guaranteed to reflect the original author — compare "Gaussian elimination" and "Euclidean geometry," for example.

Chapter 6

CHARACTER TABLES

The oldest branch of quasigroup representation theory is the combinatorial character theory. The source of the theory is the diagonal action of the multiplication group on the direct square Q^2 of a quasigroup Q, as introduced in Section 2.3. The conjugacy classes of a quasigroup Q are defined in Section 6.1 as the orbits of this action. Section 6.2 introduces the quasigroup class functions, complex-valued functions on Q^2 constant on these orbits. If Q is finite, the incidence matrices of the conjugacy classes form a basis for a complex vector space of matrices that is actually a commutative algebra, the centralizer ring of Section 6.3. In Section 6.4, this algebra is identified as the algebra of class functions under convolution, while Section 6.5 gives some other interpretations. As outlined in Section 6.6, the matrices of transition to and from a basis of primitive idempotents for the algebra normalize to yield a character table, which is the usual group character table if Q is a group. Section 6.7 shows how the familiar orthogonality relations of group character theory extend to quasigroups. Section 6.8 treats the common case of rank two quasigroups, in which the only diagonal orbits of the multiplication group are the equality and diversity relations. Section 6.9 introduces numerical invariants of entropy and asymptotic entropy for quasigroups. The entropy is determined by the character table of a quasigroup Q, while the asymptotic entropy is determined by the sequence of character tables of powers of Q.

6.1 Conjugacy classes

Let G be the multiplication group of a quasigroup Q, not necessarily finite. Recall the diagonal action (2.13) of G on $Q \times Q$. The orbits of this action (the *orbitals* of G on Q) are known as the (*quasigroup*) *conjugacy classes* of Q. Since G acts transitively on Q, one of the quasigroup conjugacy classes is the equality relation or diagonal

$$\widehat{Q} = \{(x, x) \mid x \in Q\}$$

of (3.1). Together, the quasigroup conjugacy classes furnish a disjoint union partition of Q^2 known as the *conjugacy class partition* Γ or $\Gamma(Q)$. The number s of conjugacy classes is called the *rank* of the quasigroup Q.

Interchange of factors in the direct square $Q \times Q$ is an automorphism of the diagonal action of G. Thus each quasigroup conjugacy class C determines a *converse* conjugacy class $C^{-1} = \{(y, x) \mid x, y \in C\}$. Note that the diagonal class $\widehat{Q}$ is its own converse. If each conjugacy class of Q is its own converse (i.e., if each class is a symmetric relation on Q), then the quasigroup Q is said to be of *real type*.

For a conjugacy class C and an element x of Q, write

$$C(x) = \{y \in Q \mid (x, y) \in C\}.$$

Now for an element e of Q, there is a bijection

$$\Gamma \to Q/G_e; C \mapsto C(e) \tag{6.1}$$

from the set of conjugacy classes of Q to the set of G_e-orbits on Q. Since

$$\rho(e, Q) = \{\rho(e, q) \mid q \in Q\}$$

is a right transversal to G_e in G, the bijection (6.1) has

$$D \mapsto \big(\{e\} \times D\big)\rho(e, Q)$$

as its two-sided inverse. If e is the pointed idempotent of a pique (Q, e), then the orbits D of G_e on Q are called the *pique conjugacy classes* of Q. If Q is a group with identity element e, then the pique conjugacy classes coincide with the usual group conjugacy classes. In this case

$$x \in C(e) \quad \Leftrightarrow \quad x^{-1} \in C^{-1}(e)$$

since $(e, x)R(x^{-1}) = (x^{-1}, e)$.

6.2 Class functions

From now on, consider a quasigroup $Q = \{q_1, \ldots, q_n\}$ of positive finite order n. Let $\mathbb{C}(Q^2)$ denote the set of all complex-valued functions on Q^2. This set carries a lot of algebraic structure. To begin with, it has the *pointwise* or *Hadamard* involutive $\mathbb{C}$-algebra structure induced from $\mathbb{C}$ with complex conjugation. The unit element of $\mathbb{C}(Q^2)$ under the Hadamard product is the *zeta function* ζ_Q or $\zeta : \mathbb{C}(Q^2) \to \{1\}$. Secondly, $\mathbb{C}(Q^2)$ has a right $\mathbb{C}G$-module structure given by

$$g : \mathbb{C}(Q^2) \to \mathbb{C}(Q^2); \theta \mapsto \big(\theta^g : (x, y) \mapsto \theta(xg^{-1}, yg^{-1})\big) \tag{6.2}$$

for g in G. Further, it has a bilinear *convolution* $*$ given by

$$\theta * \varphi(x, y) = \sum_{z \in Q} \theta(x, z)\varphi(z, y) \tag{6.3}$$

for x, y in Q. The unit element of the convolution is the *delta function* δ_Q or

$$\delta(x,y) = \begin{cases} 1 & \text{if } x = y\,; \\ 0 & \text{if } x \neq y\,, \end{cases} \tag{6.4}$$

the characteristic function of the subset $\widehat{Q}$ of Q^2.

The combinatorial multiplication group G of Q acts on $\mathbb{C}(Q^2)$ via

$$g : \theta \mapsto \left(\theta^g : (x,y) \mapsto \theta(xg^{-1}, yg^{-1})\right) \tag{6.5}$$

for g in G. The group G with this action is clearly a group of automorphisms of the $\mathbb{C}$-module and Hadamard structures. It is also a group of automorphisms of the convolution structure, since

$$\begin{aligned} \theta^g * \varphi^g(x,y) &= \sum_{z \in Q} \theta(xg^{-1}, zg^{-1})\varphi(zg^{-1}, yg^{-1}) \\ &= \sum_{z \in Q} \theta(xg^{-1}, z)\varphi(z, yg^{-1}) \\ &= \theta * \varphi(xg^{-1}, yg^{-1}) \\ &= (\theta * \varphi)^g(x,y)\,. \end{aligned}$$

It follows that the set $\mathbb{C}\mathrm{Cl}(Q)$ of G-invariant functions in $\mathbb{C}(Q^2)$ forms a Hadamard and convolution subalgebra. The G-invariant functions are called the (*quasigroup*) *class functions* on Q. Their restrictions to quasigroup conjugacy classes are constant. Indeed, a quasigroup class function is just a complex linear combination of characteristic functions of quasigroup conjugacy classes.

One may extend the definition of a class function θ on Q by defining

$$\theta(X) = \sum_{(x,y) \in X} \theta(x,y) \tag{6.6}$$

for any subset X of Q^2. Note that $(\theta \cdot \varphi)(X) \neq \theta(X) \cdot \varphi(X)$ in general. The complex space $\mathbb{C}\mathrm{Cl}(Q)$ has a bilinear form given by $\langle \theta, \varphi \rangle$ or

$$\langle \theta, \varphi \rangle_Q = |Q|^{-2} \theta * \varphi(\widehat{Q}) \tag{6.7}$$

The normalization of (6.7) assigns unit length to the zeta function ζ_Q.

If Q is a pique with pointed idempotent e (for example a loop with identity element e), a *pique class function* $f : Q \to \mathbb{C}$ on Q is defined as a complex linear combination of characteristic functions of pique conjugacy classes. Note that this definition reduces to the usual definition of class function for a finite group. Now a quasigroup class function $\theta : Q^2 \to \mathbb{C}$ determines a *derived* pique class function $\theta' : Q \to \mathbb{C}$ with

$$\theta'(x) = \theta(e,x) \tag{6.8}$$

for x in Q. If Q is a group and φ is also a quasigroup class function, then

$$\begin{aligned}(\theta * \varphi)'(x) &= \theta * \varphi(e, x)\\ &= \sum_{z\in Q} \theta(e, z)\varphi(z, x)\\ &= \sum_{z\in Q} \theta(e, z)\varphi(zL(z)^{-1}, xL(z)^{-1})\\ &= \sum_{z\in Q} \theta(e, z)\varphi(e, xL(z)^{-1})\\ &= \sum_{z\in Q} \theta'(z)\varphi'(z^{-1}x)\\ &= \sum_{zt=x} \theta'(z)\varphi'(t) = \theta' * \varphi'(x)\,,\end{aligned}$$

so that convolution of quasigroup class functions corresponds to the usual convolution of group class functions. Further,

$$\begin{aligned}\langle\theta, \varphi\rangle &= |Q|^{-2} \sum_{x\in Q}\sum_{z\in Q} \theta(x, z)\varphi(z, x)\\ &= |Q|^{-2} \sum_{x\in Q}\sum_{z\in Q} \theta'(x^{-1}z)\varphi(z^{-1}x)\\ &= |Q|^{-1} \sum_{y\in Q} \theta'(y)\theta'(y^{-1})\,,\end{aligned}$$

so the inner product (6.7) of θ with φ is the usual inner product of θ' and φ' as group class functions.

6.3 The centralizer ring

Let K be a field. Let KG be the group algebra of G over K, and let KQ be the K-vector space with basis Q. Then KQ is a right KG-module via

$$\Big(\sum_{q\in Q} k_q q\Big)\Big(\sum_{g\in G} k_g g\Big) = \sum_{q\in Q}\sum_{g\in G} k_q k_g qg\,.$$

Since the multiplication group G acts faithfully on Q, the monoid homomorphism

$$\lambda : G \to \mathrm{End}_K KQ \tag{6.9}$$

of G into the underlying monoid of the endomorphism ring of the vector space KQ is injective. Identify G with its image in $\mathrm{End}_K KQ$. Let $V_K(G, Q)$ or just

$V(G,Q)$ denote the subring $\mathrm{End}_{KG}KQ$ of $\mathrm{End}_K KQ$ that consists of all the KG-endomorphisms of KQ, i.e. of all those vector space endomorphisms that commute with each element g of G. The ring $V_K(G,Q)$ is called the *centralizer ring* of G on Q over K. The main task of this section is to show that the centralizer ring is commutative.

Let $\{C_1, C_2, \ldots, C_s\}$ be the full set of orbits of G in its diagonal action on Q^2, with $C_1 = \widehat{Q}$ as the diagonal. Thus the conjugacy class partition Γ is

$$Q^2 = C_1 + C_2 + \cdots + C_s\,. \tag{6.10}$$

Take a fixed element e of Q. Define elements $v_1, \ldots, v_s$ of KG by

$$v_i = \sum_{q \in C_i(e)} \rho(e,q)\,.$$

Define α_i to be the image v_i^λ of v_i in $\mathrm{End}_K KQ$. Define elements $c_1, \ldots, c_s$ of KQ by

$$c_i = e\alpha_i = \sum_{q \in C_i(e)} q.$$

Note that $c_i\sigma = c_i$ for each element σ of the stabilizer G_e.

LEMMA 6.1
Let α and β be elements of KG. Then

$$e\alpha = e\beta$$

in KQ implies

$$c_i\alpha = c_i\beta$$

for $1 < i \leq s$.

PROOF Let

$$\alpha = \sum_{g \in G} k_g g = \sum_{g \in G} k_g \sigma_g \rho(e, eg)\,, \tag{6.11}$$

where $\sigma_g \in G_e$. Collecting terms of (6.11) with common $eg = q$ in Q, one has

$$\alpha = \sum_{i=1}^{n} \Big(\sum_{j=1}^{m_i} k_{ij}\sigma_{ij} \Big) \rho(e, q_i)$$

with $k_{ij} \in K$ and $\sigma_{ij} \in G_e$. Similarly,

$$\beta = \sum_{i=1}^{n} \Big(\sum_{j=1}^{m_i} l_{ij}\tau_{ij} \Big) \rho(e, q_i)$$

with $l_{ij} \in K$ and $\tau_{ij} \in G_e$. Now $e\alpha = e\beta$ implies

$$\sum_{i=1}^{n}\sum_{j=1}^{m_i} k_{ij}q_i = \sum_{i=1}^{n}\sum_{j=1}^{m_i} l_{ij}q_i\,,$$

an equation in KQ. Equating coefficients of q_i yields

$$\sum_{j=1}^{m_i} k_{ij} = \sum_{j=1}^{m_i} l_{ij}$$

for $1 \le i \le n$. Thus

$$\begin{aligned} c_h\alpha &= c_h \sum_{i=1}^{n} \Big(\sum_{j=1}^{m_i} k_{ij}\sigma_{ij} \Big) \rho(e, q_i) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m_i} k_{ij} c_h \rho(e, q_i) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m_i} l_{ij} c_h \rho(e, q_i) \\ &= c_h \sum_{i=1}^{n} \Big(\sum_{j=1}^{m_i} l_{ij}\tau_{ij} \Big) \rho(e, q_i) = c_h\beta \end{aligned}$$

as required. □

THEOREM 6.1

The centralizer ring $V_K(G, Q)$ is commutative, with the set $\{\alpha_1, \ldots, \alpha_s\}$ as a K-linear basis.

PROOF First, it will be shown that each α_i commutes with each element γ of KG. Let q be an element of Q. Now

$$q\rho(e, e)\gamma = q\gamma = q\gamma\rho(e, e)\,. \tag{6.12}$$

Let $L : KQ \to KG$ denote the linear extension of the map $L : Q \to G$. Then (6.12) may be rewritten in the form

$$eR(e)^{-1}L(qR(e\backslash e)^{-1})\gamma = eR(e)^{-1}L(q\gamma R(e\backslash e)^{-1})\,.$$

Lemma 6.1 implies that

$$c_iR(e)^{-1}L(qR(e\backslash e)^{-1})\gamma = c_iR(e)^{-1}L(q\gamma R(e\backslash e)^{-1})$$

for $1 \leq i \leq s$. In other words,

$$\sum_{q \in C_i(e)} q\rho(e,q)\gamma = \sum_{q \in C_i(e)} q\gamma\rho(e,q)\,.$$

Thus $q\alpha_i\gamma = q\gamma\alpha_i$. It follows that $\alpha_i\gamma = \gamma\alpha_i$, so the α_i lie in $V(G,Q)$. As shown by consideration of their action on e, they are clearly linearly independent.

It thus remains to show that $\{\alpha_1, \ldots, \alpha_s\}$ spans $V(G,Q)$. Let α be an element of $V(G,Q)$, with $e\alpha = \sum_{q \in Q} k_q q$. If β is in G_e, then

$$\sum_{q \in Q} k_q q = e\alpha = e\beta\alpha = e\alpha\beta = \sum_{q \in Q} k_q q\beta\,,$$

whence $k_q = k_{q\beta}$. It follows that the coefficients k_q are identical as q ranges over G_e-orbits in Q. In other words,

$$e\alpha = \sum_{i=1}^{s} k_i c_i = e \sum_{i=1}^{s} k_i \alpha_i$$

for certain k_i in K. Then for each q in Q, one has

$$\begin{aligned} q\alpha &= e\rho(e,q)\alpha = e\alpha\rho(e,q) \\ &= e\Big(\sum_{i=1}^{s} k_i\alpha_i\Big)\rho(e,q) = e\rho(e, q\Big(\sum_{i=1}^{s} k_i\alpha_i\Big) = q\Big(\sum_{i=1}^{s} k_i\alpha_i\Big)\,, \end{aligned}$$

whence $\alpha = \sum_{i=1}^{s} k_i\alpha_i$. This shows that $\{\alpha_1, \ldots, \alpha_s\}$ spans $V(G,Q)$. □

6.4 Convolution of class functions

One of the main uses of the centralizer ring $V_{\mathbb{C}}(G,Q)$ is to give a natural proof that the convolution of class functions is commutative and associative. Using x to stand for elements of the basis Q of $\mathbb{C}Q$, define a map

$$\mathbb{C}(Q^2) \to \mathrm{End}_{\mathbb{C}}\mathbb{C}Q; \theta \mapsto \big(\widetilde{\theta} : x \mapsto \sum_{y \in Q} \theta(x,y)y\big)\,. \tag{6.13}$$

This is clearly linear. Also, the image of the delta function under (6.13) is the identity automorphism of $\mathbb{C}Q$. Then for x in Q,

$$\begin{aligned} x\widetilde{\theta}\widetilde{\varphi} &= \sum_{y\in Q} \theta(x,y) y\widetilde{\varphi} \\ &= \sum_{y\in Q}\sum_{z\in Q} \theta(x,y)\varphi(y,z) z \\ &= \sum_{z\in Q} \Big(\sum_{y\in Q} \theta(x,y)\varphi(y,z) \Big) z \\ &= \sum_{z\in Q} \theta * \varphi(x,z) z = x\widetilde{\theta * \varphi}\,, \end{aligned}$$

so (6.13) is an algebra isomorphism from $\mathbb{C}(Q^2)$ under convolution to the endomorphism ring. In particular, convolution is associative. Now $\theta(\widehat{Q}) = \mathrm{Tr}(\widetilde{\theta})$. Thus the bilinear form of (6.7) extended to all of $\mathbb{C}(Q^2)$ may be interpreted as

$$\langle \theta, \varphi \rangle = |Q|^{-2} \mathrm{Tr}(\tilde{\theta}\tilde{\varphi})\,. \tag{6.14}$$

This demonstrates the nondegeneracy and associativity of the form that makes $\mathbb{C}(Q^2)$ a Frobenius algebra [36, 9.5].

The group G acts on $\mathbb{C}(Q^2)$ via (6.5). The group G is also embedded in the group of units of $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ via (6.9), and thus acts on $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ by conjugation. For θ in $\mathbb{C}(Q^2)$, x in Q, and g in G, the image of x under $\widetilde{\theta^g}$ is

$$\sum_{y\in Q} \theta^g(x,y) y = \sum_{y\in Q} \theta(xg^{-1}, yg^{-1}) y = \sum_{z\in Q} \theta(xg^{-1}, z) zg = xg^{-1}\widetilde{\theta} g\,.$$

Thus (6.13) is also an isomorphism of G-modules. An element of $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ is fixed by G if and only if it commutes with all elements of G, i.e. is an element of $V(G,Q)$. This proves almost all of the following.

THEOREM 6.2

The mapping (6.13) *restricts to an isomorphism of* $\mathbb{C}\mathrm{Cl}(Q)$ *with* $V(G,Q)$*, under which the characteristic function* κ_i *of the conjugacy class* C_i *corresponds to the basic element* α_i *of* $V(G,Q)$*. In particular, convolution on* $\mathbb{C}\mathrm{Cl}(Q)$ *is commutative.*

PROOF For each x in Q,

$$\begin{aligned} x\widetilde{\kappa_i} = \sum_{y\in Q} \kappa_i(x,y) y = \sum_{y\in C_i(x)} y &= \sum_{q\in C_i(e)} q\rho(e,x) \\ &= e\alpha_i\rho(e,x) = e\rho(e,x)\alpha_i = x\alpha_i\,, \end{aligned}$$

whence $\widetilde{\kappa_i} = \alpha_i$, as required. ∎

COROLLARY 6.1
For any two elements x, y of Q,

$$\alpha_i = \sum_{x' \in C_i(x)} \rho(x, x') = \sum_{y' \in C_i(y)} \rho(y, y') \tag{6.15}$$

and

$$\tau := \sum_{q \in Q} \rho(x, q) = \sum_{q \in Q} \rho(y, q) = \sum_{i=1}^{s} \alpha_i \tag{6.16}$$

in $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$.

DEFINITION 6.1 *The $\mathbb{C}Q$-endomorphism τ of* (6.16) *is called the* total endomorphism.

6.5 Bose-Mesner and Hecke algebras

Theorem 6.2 gives two interpretations of the centralizer ring $V(G, Q)$ or algebra $\mathbb{C}\mathrm{Cl}(Q)$ of class functions. Two other interpretations are available, and prove useful in certain circumstances. The first involves a concept from algebraic combinatorics [6, II.2.2] [37, §2.1].

DEFINITION 6.2 *Let Q be a finite, nonempty set. A* (commutative) association scheme (Q, Γ) *on Q is a disjoint union partition*

$$Q^2 = C_1 + \cdots + C_s$$

or $\Gamma = \{C_1, \ldots, C_s\}$ of Q^2 such that the following axioms are satisfied:

(A1) $C_1 = \{(x, x) \mid x \in Q\}$;

(A2) *The converse of each relation in Γ belongs to Γ;*

(A3) $\forall\, C_i \in \Gamma\,, \forall\, C_j \in \Gamma\,, \forall\, C_k \in \Gamma\,, \exists\, c_{ij}^k \in \mathbb{N}\,. \forall\, (x, y) \in C_k\,,$

$$\left|\{z \in Q \mid (x, z) \in C_i,\ (z, y) \in C_j\}\right| = c_{ij}^k\,.$$

(A4) $\forall\, 1 \le i, j, k \le s\,,\ c_{ij}^k = c_{ji}^k$.

Axiom (A4) *is the* commutativity *of the scheme.*

THEOREM 6.3
The conjugacy class partition (6.10) *of a finite, nonempty quasigroup Q forms a commutative association scheme (Q, Γ).*

PROOF Satisfaction of the axioms (A1) and (A2) is clear from Section 6.1. For $1 \leq k \leq s$, let A_k be the incidence matrix of the quasigroup conjugacy class C_k. Thus the matrix A_k is the $(n \times n)$-matrix whose i,j-entry is 1 if $(q_i, q_j) \in C_k$, and 0 otherwise. By (6.15), each such matrix A_k may be construed as the matrix of the endomorphism α_k of $\mathbb{C}Q$ with respect to the basis Q. The scalars c_{ij}^k of (A3) then appear as the *structure constants*

$$A_i A_j = \sum_{k=1}^{s} c_{ij}^k A_k \,. \tag{6.17}$$

of the algebra $V(G,Q)$ with respect to its basis $\{\alpha_1, \ldots, \alpha_s\}$, while (A4) is satisfied since $V(G,Q)$ is commutative. □

In the context of association schemes, the algebra $V(G,Q)$ is known as the *Bose-Mesner algebra* of (Q,Γ). It is often very convenient to construe the centralizer ring $V(G,Q)$ as the complex linear span of the set

$$I_n = A_1, A_2, \ldots, A_s \tag{6.18}$$

of $(n \times n)$-matrices. By Corollary 6.1, the matrix of the total endomorphism τ with respect to the basis Q becomes the $n \times n$ all-ones matrix J or

$$J_n = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & 1 & \ldots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \ldots & 1 \end{bmatrix} . \tag{6.19}$$

Equation (6.16) then takes the matrix form $J_n = A_1 + \cdots + A_s$.

The fourth interpretation of the algebra considers $\mathbb{C}\mathrm{Cl}Q$ as the space of complex-valued functions constant on $C_1, \ldots, C_s$. Fixing e in Q, the algebra $\mathbb{C}\mathrm{Cl}Q$ is isomorphic (by restriction) to the space of complex-valued functions defined on Q that are constant on each of the orbits $C_1(e), \ldots, C_s(e)$ of the stabilizer G_e on Q. The permutation representation of G on Q is similar to the homogeneous space $G_e \backslash G$ of G on the right cosets $G_e \rho(e,q)$ of G_e, and the orbits of G_e on Q correspond under the similarity to the sets of right cosets contained in a single double G_e-coset $G_e \rho(e,q) G_e$. (These double cosets are the orbits of the relative multiplication group of the subquasigroup G_e of G.) Complex-valued functions on Q may be identified as complex-valued functions on G that are constant on right G_e-cosets. Then functions on Q that are constant on $C_1(e), \ldots, C_s(e)$ correspond to functions on G that are constant on double G_e-cosets. Under this interpretation, $\mathbb{C}\mathrm{Cl}Q$ becomes the *Hecke algebra* $H(G, G_e, 1_{G_e})$ [36, 11.22]. The feature of this interpretation is that an element e of Q has been chosen. There are occasions when this is appropriate and advantageous.

In summary, there are four sets naturally isomorphic to one another, all carrying isomorphic algebra structures, induced from one set to the other by natural isomorphisms:

$$\begin{cases} \text{(a)} & \text{the algebra } \mathbb{C}\mathrm{Cl}Q \text{ of class functions;} \\ \text{(b)} & \text{the centralizer ring } V(G,Q); \\ \text{(c)} & \text{the Bose-Mesner algebra of matrices of } V(G,Q); \\ \text{(d)} & \text{the Hecke algebra } H(G,G_e,1_{G_e}), \text{ subject to choice of } e. \end{cases} \tag{6.20}$$

The action of a group of permutations G on a set Q is said to be *multiplicity-free* if the G-module $\mathbb{C}Q$ decomposes as a direct sum

$$\mathbb{C}Q = \bigoplus_{i=1}^{s} X_i \tag{6.21}$$

of mutually inequivalent irreducible G-modules.

PROPOSITION 6.1
The action of the combinatorial multiplication group G on a finite quasigroup Q is multiplicity-free.

PROOF Suppose that the decomposition (6.21) of the G-module $\mathbb{C}Q$ into a direct sum of irreducible modules were to include summands X_i and X_j equivalent by a G-isomorphism $\theta : X_i \to X_j$, so that $x\theta g = xg\theta$ for all x in X_i and g in G. For each 2×2 complex matrix

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

define a linear endomorphism

$$\alpha_A : X_i \oplus X_j \to X_i \oplus X_j; [x,y] \mapsto [a_{11}x + a_{21}y\theta^{-1}, a_{12}x\theta + a_{22}y].$$

Note that $\alpha_A g = g\alpha_A$ for all g in G. Then

$$A \mapsto \alpha_A \oplus \bigoplus_{k \neq i,j} 1_{X_k}$$

would be an injective $\mathbb{C}G$-homomorphism from the noncommutative ring of 2×2 complex matrices to the centralizer ring $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q$, violating the commutativity of this latter ring. □

The fundamental theorem of the combinatorial character theory of quasigroups then has a number of essentially equivalent formulations in various terms as follows.

THEOREM 6.4
Let G be the combinatorial multiplication group of a finite quasigroup Q of positive order n.

(a) *The action of G on Q is multiplicity-free.*

(b) *The set Q with the conjugacy class partition Γ forms a (commutative) association scheme (Q, Γ).*

(c) *For any q in Q, the multiplication group G and the stabilizer G_q of q in G form a Gel'fand pair (G, G_q).*

(d) $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q = V(G, Q)$ *is commutative, with vector space basis* (6.18).

For current purposes, Theorem 6.4(d) is the most convenient formulation. For Theorem 6.4(c) and the terminology of Gel'fand pairs, see [40, Ch. 3], [79, Defn. 4.1].

6.6 Quasigroup character tables

By Theorem 6.1, $V_{\mathbb{C}}(G, Q)$ is a commutative algebra with basis $\{\alpha_1, \ldots, \alpha_s\}$. Since the endomorphisms α_i of $\mathbb{C}Q$ commute mutually, an eigenspace of one is stable under the action of the others. One may thus decompose $\mathbb{C}Q$ as a direct sum of eigenspaces $\mathbb{C}Q_j$ such that

$$\begin{cases} \text{(a)} & \forall\, 1 \le i \le s,\ \exists\, \xi_{ij} \in \mathbb{C}\,.\, \mathbb{C}Q_j(\alpha_i - \xi_{ij}) = \{0\}\,; \\ \text{(b)} & \forall\, j \ne k,\ \exists\, i\,.\, \xi_{ij} \ne \xi_{ik}\,; \\ \text{(c)} & \mathbb{C}Q_1 = \mathbb{C}(q_1 + \cdots + q_n)\,. \end{cases} \tag{6.22}$$

For (a) and (b), decompose $\mathbb{C}Q$ into α_1-eigenspaces, then decompose each of these into α_2-eigenspaces, then each of these into α_3-eigenspaces, and so on. Note that each $\mathbb{C}Q_j$ must be an eigenspace for each linear combination of $\alpha_1, \ldots, \alpha_s$. In particular, one of them, say $\mathbb{C}Q_1$, must be an eigenspace of the total endomorphism τ corresponding to its eigenvalue n. But since the trace of τ is n, this eigenspace has dimension 1, and is thus as claimed in (6.22)(c). For $1 \le i \le s$, set

$$|C_i| = nn_i\,. \tag{6.23}$$

The numbers n_i are known as the *valencies*. Corollary 6.1 shows that $\xi_{i1} = n_i$ for $1 \le i \le s$.

The complex space $\mathbb{C}Q$ may be equipped with an Hermitian form $(\ |\ )$ defined by declaring Q to be an orthonormal basis. If C_{i^*} is the converse C_i^{-1} of C_i, then the incidence matrix of C_{i^*} is the (conjugate) transpose A_i^* of the

incidence matrix A_i of C_i, the matrix of the endomorphism α_i with respect to the orthonormal basis Q. Thus α_{i^*} is α_i^*, the adjoint endomorphism to α_i given by

$$(x\alpha_i|y) = (x|y\alpha_i^*)$$

for x, y in $\mathbb{C}Q$.

THEOREM 6.5

The vector space $\mathbb{C}Q$ decomposes as a direct sum

$$\mathbb{C}Q = \mathbb{C}Q_1 \oplus \mathbb{C}Q_2 \oplus \cdots \oplus \mathbb{C}Q_s \tag{6.24}$$

of mutually orthogonal subspaces $\mathbb{C}Q_j$ subject to (6.22). *If $\epsilon_j : \mathbb{C}Q \to \mathbb{C}Q_j$ is the projection onto $\mathbb{C}Q_j$, then*

$$\left\{\epsilon_1 = \frac{\tau}{n}, \epsilon_2, \ldots, \epsilon_s\right\} \tag{6.25}$$

is a basis for $V(G,Q)$ with $\epsilon_i^* = \epsilon_i$ for $1 \le i \le s$.

PROOF Suppose $j \neq k$, with $x_j \in \mathbb{C}Q_j$, $x_k \in \mathbb{C}Q_k$. Then for i given by (6.22)(b), one has

$$(x_j|x_k)\xi_{ij} = (\xi_{ij}x_j|x_k) = (x_j\alpha_i|x_k) = (x_j|x_k\alpha_i^*) = (x_j|\overline{\xi}_{ik}x_k) = (x_j|x_k)\xi_{ik}\,,$$

whence $(x_j|x_k)(\xi_{ij} - \xi_{jk}) = 0$. But $\xi_{ij} \neq \xi_{jk}$, so $(x_j|x_k) = 0$. This shows that $\mathbb{C}Q_i$ and $\mathbb{C}Q_j$ are orthogonal.

Consider a fixed $\mathbb{C}Q_k$. For each $j \neq k$, (6.22)(b) gives $i = i(j)$ such that $\xi_{i(j)j} \neq \xi_{i(j)k}$. Then $(\alpha_{i(j)} - \xi_{i(j)j})/(\xi_{i(j)k} - \xi_{i(j)j})$ is defined. By (6.22)(a) it restricts to 1 on $\mathbb{C}Q_k$ and to 0 on $\mathbb{C}Q_j$. Thus

$$\epsilon_k = \prod_{j\neq k} \frac{\alpha_{i(j)} - \xi_{i(j)j}}{\xi_{i(j)k} - \xi_{i(j)j}}\,,$$

whence ϵ_k lies in $V(G,Q)$. By definition the set $\{\epsilon_1, \epsilon_2, \ldots\}$ is linearly independent. Now (6.22)(a) yields $\alpha_i = \sum_j \xi_{ij}\epsilon_j$, so $\{\epsilon_1, \epsilon_2, \ldots\}$ spans $V(G,Q)$. It follows that there are s of the $\mathbb{C}Q_j$, and that $\{\epsilon_1, \ldots, \epsilon_s\}$ is a basis of $V(G,Q)$. With respect to a union of bases of $\mathbb{C}Q_j$, the matrix of ϵ_i is a diagonal 0-1-matrix, so $\epsilon_i^* = \epsilon_i$. □

COROLLARY 6.2

The set $\{\epsilon_1, \ldots, \epsilon_s\}$ is uniquely determined as the set of atoms of the finite Boolean algebra of idempotents of $V(G,Q)$.

COROLLARY 6.3

The decomposition (6.24) *coincides with the decomposition* (6.21).

PROOF Since the projection operators ϵ_i of the decomposition (6.24) lie in the centralizer ring $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q$, (6.24) is a G-module decomposition. The summands are irreducible by the minimality of the idempotents ϵ_i in $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q$, □

With respect to the basis Q, the matrix version of (6.25) is the set

$$\left\{E_1 = \frac{J_n}{n}, E_2, \ldots, E_s\right\} \tag{6.26}$$

of idempotent matrices, with J_n as the $n \times n$ all-ones matrix. Set

$$f_i = \mathrm{Tr}\, E_i = \mathrm{Tr}\, \epsilon_i = \dim \mathbb{C}Q_i \tag{6.27}$$

for $1 \leq i \leq s$. Note $f_1 = 1$. The f_i are known as the *multiplicities*. Suppose

$$A_i = \sum_{j=1}^{s} \xi_{ij} E_j \tag{6.28}$$

and

$$E_i = \sum_{j=1}^{s} \eta_{ij} A_j \tag{6.29}$$

for $1 \leq i \leq s$. In Delsarte's terminology [37], the $s \times s$ matrices $\Xi = [\xi_{ij}]$ and $nH = [n\eta_{ij}]$ are known respectively as the *first* and *second eigenmatrices* of G on Q. The ξ_{ij} are the values of the $V(G,Q)$-*characters* of G according to Tamaschke [170].

LEMMA 6.2
For $1 \leq i, j \leq s$ *:*

(a) $\eta_{i1} = f_i/n$, $\xi_{1j} = 1$, *and* $\eta_{1j} = 1/n$;

(b) $\mathrm{Tr}(\alpha_i \alpha_j) = |C_i|\delta_{i^* j}$ *and* $c_{ij}^1 = n_i \delta_{i^* j}$;

(c) $\eta_{ij} = \overline{\eta}_{ij^*}$;

(d) $\sum_{k=1}^{s} \eta_{ik}\overline{\eta}_{jk} n_k = \delta_{ij} f_i/n$.

PROOF (a) By Theorem 6.2, $\mathrm{Tr}\, \alpha_1 = n$ and $\mathrm{Tr}\, \alpha_i = 0$ for $i > 1$. The first result follows on taking the trace of (6.29). The second result holds since

$$\alpha_1 = 1 = \epsilon_1 + \cdots + \epsilon_s \,.$$

Finally, $\tau = \alpha_1 + \cdots + \alpha_s$ implies

$$\epsilon_1 = n^{-1}\tau = n^{-1}\alpha_1 + \cdots + n^{-1}\epsilon_s \,.$$

(b) For each x in Q, $(x\alpha_i\alpha_j|x) = (x\alpha_i|x\alpha_j^*) = \delta_{ij^*}n_i = \delta_{i^*j}n_i$. Thus $\mathrm{Tr}(\alpha_i\alpha_j) = nn_i\delta_{i^*j}$ and $c_{ij}^1 = n^{-1}\mathrm{Tr}(\alpha_i\alpha_j) = n_i\delta_{i^*j}$.

(c) The result follows by equating coefficients of α_j in

$$\sum_{j=1}^{s}\eta_{ij}\alpha_j = \epsilon_i = \epsilon_i^* = \sum_{j=1}^{s}\overline{\eta}_{ij}\alpha_j^* = \sum_{j=1}^{s}\overline{\eta}_{ij}\alpha_{j^*} = \sum_{j=1}^{s}\overline{\eta}_{ij^*}\alpha_j\,.$$

(d) Consider

$$\begin{aligned}\delta_{ij}\Big(\sum_{m=1}^{s}\eta_{im}\alpha_m\Big) &= \delta_{ij}\epsilon_i = \epsilon_i\epsilon_j\\ &= \Big(\sum_{k=1}^{s}\eta_{ik}\alpha_k\Big)\Big(\sum_{l=1}^{s}\eta_{il}\alpha_l\Big)\\ &= \sum_{m=1}^{s}\sum_{k=1}^{s}\sum_{l=1}^{s}\eta_{ik}\eta_{jl}c_{klm}\alpha_m\,.\end{aligned}$$

Equating coefficients of α_l (i.e. applying $n^{-1}\mathrm{Tr}$),

$$\delta_{ij}\eta_{i1} = \sum_{k=1}^{s}\sum_{l=1}^{s}\eta_{ik}\eta_{jl}c_{kl1}\,.$$

Then by (a) through (c), one obtains

$$\delta_{ij}f_i/n = \sum_{k=1}^{s}\eta_{ik}\overline{\eta}_{jk}n_k\,,$$

which is (d). □

By (6.28) and (6.29), the matrices Ξ and H are mutually inverse: $\Xi H = I$. Thus $H^*\Xi^* = I$, i.e.

$$\sum_{j=1}^{s}\overline{\eta}_{jk}\xi_{lj} = \delta_{kl}\,.$$

From Lemma 6.2(d) it follows that

$$\begin{aligned}f_i\overline{\xi}_{li}/n &= \sum_{j=1}^{s}\delta_{ij}f_i\overline{\xi}_{li}/n\\ &= \sum_{j=1}^{s}\sum_{k=1}^{s}\eta_{ik}n_k\overline{\eta}_{jk}\overline{\xi}_{lj}\\ &= \sum_{k=1}^{s}\eta_{ik}n_k\delta_{kl} = \eta_{il}n_l\,,\end{aligned}$$

whence $(f_i)^{1/2}\xi_{li}n_l^{-1} = n(f_i)^{-1/2}\overline{\eta}_{il}$. This equation underlies the fundamental definition of the combinatorial character theory of quasigroups.

DEFINITION 6.3 *Let Q be a finite quasigroup.*

(a) *The* character table *of Q is defined to be the $s \times s$ matrix $\Psi(Q)$ or Ψ with entries*

$$\psi_{ij} = \frac{\sqrt{f_i}}{n_j}\,\xi_{ji} = \frac{n}{\sqrt{f_i}}\,\overline{\eta}_{ij} \tag{6.30}$$

for $1 \le i, j \le s$.

(b) *Each row ψ_i of the character table Ψ gives a class function ψ_i whose restriction to elements of C_j is ψ_{ij}. These functions $\psi_1, \ldots, \psi_s$ are known as the* basic (combinatorial) characters *of Q.*

(c) *The* degree *or* dimension *of a basic character ψ_i is the positive real number ψ_{i1}.*

The character table is often displayed with its columns labeled by the corresponding conjugacy classes, or by typical elements of these classes. By mild abuse of notation, the set $\{\psi_1, \psi_2, \ldots, \psi_s\}$ is also labeled Ψ. The zeta function $\zeta = \psi_1$ is sometimes called the *principal character*.

For a pique P, the i-th *irreducible character* is the complex-valued function χ_i on P with $\chi_i(p) = \psi_{ij}$ for $(e, p) \in C_j$. If P is a group, then this definition agrees with the usual group-theoretic concept. Indeed $\psi_i(x, y) = \chi_i(x\backslash y)$ in that case (Exercise 6). In the group case, each $\psi_{i1} = \chi_i(1)$ is the degree or dimension of the character χ_i, an integer. For general quasigroups, the dimensions ψ_{i1} need not be rational — compare Figure 6.1 on page 158. On the other hand, Section 9.8 shows how a nonassociative quasigroup (in that case $\mathbb{Z}/4\mathbb{Z}$ under subtraction) may have an irrational dimension that coincides with an irrational quantum-mechanical statistical dimension, and a centralizer ring that implements the corresponding quantum-mechanical fusion algebra. In some ways, the most natural normalization of the characters is obtained by considering the $(s \times s)$-matrix Υ whose i, j-entry is

$$\Upsilon_{ij} = \sqrt{\frac{f_i}{nn_j}}\xi_{ji} = \sqrt{\frac{nn_j}{f_i}}\overline{\eta}_{ij} \tag{6.31}$$

[41, (A.8)] [158, (4.7)].

6.7 Orthogonality relations

The inverse relationship between the matrices Ξ and H of Section 6.6 yields the following *orthogonality relations*.

THEOREM 6.6
The character table of a finite, nonempty quasigroup Q satisfies

$$\sum_{k=1}^{s} \varphi_{ki}\overline{\varphi}_{kj} = n\delta_{ij}/n_i \tag{6.32}$$

and

$$\sum_{k=1}^{s} \varphi_{ik}\overline{\varphi}_{jk} n_k = n\delta_{ij}\,. \tag{6.33}$$

The set Ψ forms an orthonormal basis for the space $\mathbb{C}\mathrm{Cl}(Q)$ of class functions under the inner product (6.7)*. In particular, this inner product is nondegenerate.*

PROOF Since $I = \Xi H$, one has that

$$\delta_{ij} = \sum_{k=1}^{s} \xi_{ik}\eta_{kj} = \sum_{k=1}^{s} n_i \psi_{ki}(f_k)^{-1/2}(f_k)^{1/2}\overline{\psi}_{kj} n^{-1}\,,$$

proving (6.32). By Lemma 6.2(d),

$$\delta_{ij} f_i/n = \sum_{k=1}^{s} \eta_{ik}\overline{\eta}_{jk} n_k = \sum_{k=1}^{s} n^{-1}\overline{\psi}_{ik}(f_i)^{1/2} n^{-1}\psi_{jk}(f_j)^{1/2} n_k\,,$$

from which (6.33) follows on taking the complex conjugate. Finally, for $x \in Q$,

$$\begin{aligned} n\langle \psi_i, \psi_j\rangle &= \sum_{y\in Q} \psi_i(x,y)\psi_j(y,x) \\ &= \sum_{k=1}^{s} \sum_{(x,y)\in C_k} \psi_i(x,y)\psi_j(y,x) \\ &= \sum_{k=1}^{s} n_k \psi_{ik}\psi_{jk^*} \\ &= \sum_{k=1}^{s} n_k \psi_{ik}\overline{\psi}_{jk} \\ &= n\delta_{ij} \end{aligned}$$

by (6.33), so that $\{\psi_1, \ldots, \psi_s\}$ is a linearly independent orthonormal set of class functions. Since the space of class functions has dimension s, it is also a basis. □

The relations (6.33) and (6.32) amount to the unitarity of the matrix (6.31), which is thus called the *unitary character table* Υ or $\Upsilon(Q)$ of the quasigroup Q.

As for groups, the character table $\Psi(Q)$ of a finite quasigroup Q encodes a large amount of information about the quasigroup.

COROLLARY 6.4

The character table of Q yields the following for $1 \leq i, j \leq s$:

(a)

$$n = \sum_{k=1}^{s} \psi_{k1}\overline{\psi}_{k1}\,;$$

(b)

$$n_i = \frac{\sum_{k=1}^{s} \psi_{k1}\overline{\psi}_{k1}}{\sum_{k=1}^{s} \psi_{ki}\overline{\psi}_{ki}}\,;$$

(c)

$$f_i = \psi_{i1}^2\,;$$

(d)

$$\eta_{ij} = \frac{\psi_{i1}\overline{\psi}_{ij}}{\sum_{k=1}^{s} \psi_{k1}\overline{\psi}_{k1}}\,;$$

(e)

$$\xi_{ij} = \frac{\psi_{ji}\sum_{k=1}^{s} \psi_{k1}\overline{\psi}_{k1}}{\psi_{j1}\sum_{k=1}^{s} \psi_{ki}\overline{\psi}_{ki}}\,.$$

THEOREM 6.7

The character table of Q determines the centralizer ring $V(G, Q)$.

PROOF By Corollary 6.4 and (6.28),

$$\alpha_i = n_i \sum_{k=1}^{s} \psi_{ki} f_k^{-1} \epsilon_k\,.$$

Then

$$\sum_{l=1}^{s} n_i n_j \psi_{li}\psi_{lj} f_l^{-1}\epsilon_l = \Big(n_i \sum_{k=1}^{s} \psi_{ki} f_k^{-1/2}\epsilon_k\Big)\Big(n_j \sum_{l=1}^{s} \psi_{lj} f_l^{-1/2}\epsilon_l\Big)$$
$$= \alpha_i\alpha_j = \sum_{m=1}^{s} c_{ij}^m \alpha_m = \sum_{l=1}^{s}\sum_{m=1}^{s} c_{ij}^m n_m \psi_{lm} f_l^{-1/2}\epsilon_l\,.$$

Equating coefficients of ϵ_l,

$$n_i n_j \psi_{li}\psi_{lj} f_l^{-1} = \sum_{m=1}^{s} c_{ij}^m n_m \psi_{lm} f_l^{-1/2}\,.$$

Multiplying by $f_l^{-1/2}\overline{\psi}_{lk}$ and summing over l,

$$\sum_{l=1}^{s} n_i n_j \psi_{li}\psi_{lj}\overline{\psi}_{lk} f_l^{-1} = \sum_{l=1}^{s}\sum_{m=1}^{s} c_{ij}^m n_m \psi_{lm}\overline{\psi}_{lk}$$
$$= \sum_{m=1}^{s} c_{ij}^m n_m n\delta_{mk} n_m^{-1} = n c_{ij}^k$$

by (6.32). Thus

$$c_{ij}^k = \frac{n_i n_j}{n}\sum_{l=1}^{s} \psi_{li}\psi_{lj}\overline{\psi}_{lk} f_l^{-1/2}\,. \tag{6.34}$$

By Corollary 6.4, the character table specifies all the terms on the right-hand side of (6.34). It thus specifies the structure constants of the centralizer ring, as required. □

PROPOSITION 6.2

The character table of Q determines the stability congruence of Q as

$$\sigma(Q) = \bigcup\{C_i \mid n_i = 1\}\,. \tag{6.35}$$

PROOF For fixed e in Q, the sets $C_i(e)$ are the orbits of the stabilizer G_e on Q. Thus

$$e^\sigma = \bigcup\{\{x\} \mid xG_e = x\} = \bigcup\{C_i(e) \mid n_i = 1\}\,,$$

from which (6.35) follows. Note that $\Psi(Q)$ determines the valencies n_i according to Corollary 6.4(b). □

6.8 Rank two quasigroups

A quasigroup Q has rank 2 if there are just two quasigroup conjugacy classes, the equality relation

$$C_1 = \{(x, y) \in Q^2 \mid x = y\}$$

and the diversity relation

$$C_2 = \{(x, y) \in Q^2 \mid x \neq y\}.$$

In other words, the multiplication group G acts 2-transitively on Q. (Compare Exercise 13 in Chapter 9.) For example, any nonabelian quasigroup of order 3 has rank 2, and indeed all the projective geometries of Section 1.6 yield rank 2 quasigroups. The only finite rank 2 group is the cyclic group of order 2. On the other hand, any countable torsion-free group has an HNN-extension group that is a rank 2 quasigroup [80], [103, §53].

The orthogonality relations immediately specify the character table of any finite rank 2 quasigroup Q of order n as shown in Figure 6.1. The top row is filled by the trivial character ψ_1. The entry $\psi_{21} = (n-1)^{1/2}$ is specified by (6.32) with $i = j = 1$. The remaining entry $\psi_{22} = -(n-1)^{-1/2}$ may then be specified by (6.33) with $i = 1$ and $j = 2$.

Q	C_1	C_2
ψ_1	1	1
ψ_2	$(n-1)^{1/2}$	$-(n-1)^{-1/2}$

FIGURE 6.1: The character table of a rank 2 quasigroup of order n.

Theorem 3.10 shows that the rank 2 quasigroups of a given prime order $p > 3$ include some quasigroups which are central, and some which are not (compare Exercise 10). Thus the character table of a finite quasigroup does not determine whether or not the quasigroup is central.

In a well-defined sense, almost all finite quasigroups have rank 2. For a positive integer n, let $l(n)$ denote the number of Latin squares of order n using the symbols $1, 2, \ldots, n$. Let $\mathcal{P}$ be a certain property which a finite quasigroup may or may not possess. Let $p(n)$ denote the number of Latin squares of order n that yield multiplication tables of quasigroups possessing

the property $\mathcal{P}$ when bordered on the left and on top with $1, 2, \ldots, n$ in order. Then *almost all finite quasigroups* are said to *have property* $\mathcal{P}$ if

$$\lim_{n\to\infty} \frac{p(n)}{l(n)} = 1, \tag{6.36}$$

while *hardly any finite quasigroups* are said to *have property* $\mathcal{P}$ if the limit in (6.36) is 0. (Thus in the latter case, almost all finite quasigroups have the complementary property $\neg\mathcal{P}$.)

THEOREM 6.8
Almost all finite quasigroups Q have the symmetric group $Q!$ as their multiplication group.

PROOF The smallest transitive permutation group containing a random permutation is almost always the symmetric or alternating group [108]. On the other hand, hardly any finite quasigroups have their multiplication group consisting entirely of even permutations [74]. □

COROLLARY 6.5
Almost all finite quasigroups are rank 2 *quasigroups.*

6.9 Entropy

The information-theoretic concept of entropy is a useful source of numerical invariants for the classification of finite quasigroups.

DEFINITION 6.4 *The* (conjugate) entropy *of a finite, nonempty quasigroup Q is defined to be*

$$H(Q) = \sum_{i=1}^{s} \frac{n_i}{n} \log \frac{n}{n_i}, \tag{6.37}$$

the logarithms being taken to a fixed base. If the base is taken to be 2*, the units of entropy are* bits.

Since the character table of Q determines n and each n_i, it determines the entropy of Q (compare Exercise 18). In turn, the entropy of Q suffices for the recognition of abelian and rank 2 quasigroups.

THEOREM 6.9
The entropy $H(Q)$ of a finite quasigroup Q of positive order n satisfies

$$\log n - (1 - n^{-1}) \log(n-1) \leq H(Q) \leq \log n \,.$$

Equality obtains on the left if and only if Q has rank 2. It obtains on the right if and only if Q is abelian.

PROOF Suppose that for some i, there are positive integers n_i' and n_i'' such that $n_i = n_i' + n_i''$. Now

$$0 < \frac{n_i'}{n_i} \log \frac{n_i}{n_i'} + \frac{n_i''}{n_i} \log \frac{n_i}{n_i''} \,,$$

since the right-hand side is a positive linear combination of the positive quantities $\log(n_i/n_i')$ and $\log(n_i/n_i'')$. In other words,

$$-n_i \log n_i < n_i' \log \frac{1}{n_i'} + n_i'' \log \frac{1}{n_i''} \,,$$

so that

$$\frac{1}{n}\Big(n_i \log n - n_i \log n_i\Big) < \frac{1}{n}\Big(n_i' \log n + n_i' \log \frac{1}{n_i'} + n_i'' \log n + n_i'' \log \frac{1}{n_i''}\Big)$$

or

$$\frac{n_i}{n} \log \frac{n}{n_i} < \frac{n_i'}{n} \log \frac{n}{n_i'} + \frac{n_i''}{n} \log \frac{n}{n_i''} \,.$$

Thus the entropy (6.37) is strictly increased when conjugacy classes are split, or strictly decreased when they are fused. It obtains its minimum if and only if Q has rank 2. It obtains its maximum of $\log n$ if and only if each multiplicity n_i is 1, or each conjugacy class has order $|Q|$. This means that for each element x of Q, the stabilizer G_x is trivial. According to Proposition 3.16, this latter condition is equivalent to Q being abelian. □

The entropy offers a more refined measure than the simple counts of conjugacy classes that have often been used in group theory (see [144], for example).

PROPOSITION 6.3
Suppose that a finite, nonempty quasigroup Q has s conjugacy classes. Then the entropy $H(Q)$ of Q is bounded above by $\log s$.

PROOF The natural logarithm function is concave, and thus its graph lies below its tangent line at the point $(1, 0)$. In other words, for any positive real number x,

$$\log x \leq x - 1 \,.$$

Setting $x = (n/n_i)(1/s)$, one obtains

$$\log \frac{n}{n_i} - \log s \leq \frac{n}{n_i s} - 1 \,. \tag{6.38}$$

Multiplying (6.38) by n_i/n and summing for $1 \leq i \leq s$ yields

$$\sum_{i=1}^{s} \frac{n_i}{n} \log \frac{n}{n_i} - \log s \leq 0 \,,$$

from which the upper bound follows. □

Since the entropy of a finite, nonempty quasigroup Q is determined by the character table of Q, it is apparent that the entropy cannot determine whether Q is central or not. One is thus led to the second numerical invariant.

DEFINITION 6.5 *The* asymptotic (conjugate) entropy $h(Q)$ *of a finite, nonempty quasigroup Q is defined to be*

$$h(Q) = \limsup_{m \to \infty} \frac{1}{m} H(Q^m) \,.$$

By Theorem 6.9, $0 < H(Q^m) \leq \log |Q^m|$, so the asymptotic entropy $h(Q)$ satisfies

$$0 \leq h(Q) \leq \log |Q| \,. \tag{6.39}$$

Note that $h(Q)$ is determined by the sequence $\Psi(Q^m)$ of character tables of powers of Q.

PROPOSITION 6.4
If two finite, nonempty quasigroups P and Q are centrally isotopic, then they have the same entropy and the same asymptotic entropy.

PROOF By Theorem 3.4 and (3.25), two finite quasigroups A and B are centrally isotopic if and only if there is a nonempty finite quasigroup Z such that $Z \times A$ and $Z \times B$ are isomorphic. Since P and Q are centrally isotopic, there is a finite nonempty quasigroup Z_1 with $Z_1 \times P$ and $Z_1 \times Q$ isomorphic. Suppose, as an induction hypothesis, that there is a finite nonempty quasigroup Z_r with $Z_r \times P^r \cong Z_r \times Q^r$. Then

$$\begin{aligned}(Z_r \times Z_1) \times P^{r+1} &\cong (Z_r \times P^r) \times (Z_1 \times P) \\ &\cong (Z_r \times Q^r) \times (Z_1 \times Q) \cong (Z_r \times Z_1) \times Q^{r+1} \,.\end{aligned}$$

It follows that P^m is centrally isotopic to Q^m for each positive integer m. By Proposition 3.10, centrally isotopic quasigroups have similar multiplication group actions, and accordingly have the same entropy. Thus $H(P^m) = H(Q^m)$ for each m (including $m = 1$, of course), whence $h(P) = h(Q)$. □

Just as abelian quasigroups maximize the entropy according to Theorem 6.9, central quasigroups maximize the asymptotic entropy.

PROPOSITION 6.5
Let Q be a finite, nonempty central quasigroup. Then $h(Q) = \log |Q|$.

PROOF By Proposition 6.4 and Theorem 3.7, it suffices to consider the case of a central pique $(P, 0)$ centrally isotopic to Q. Let q be the order of P, and let r be the order of the inner multiplication group F of P. The stabilizer of $(0, \dots, 0)$ in $\operatorname{Mlt} P^m$ is then $F_m = \{(f, \dots, f) \mid f \in F\}$, again of order r. For each positive integer j, let n_j be the number of orbits of size j in the action of F_m on P^m. Then the entropy of P^m is

$$\sum_{j=1}^{r} n_j \frac{j}{q^m} \log \frac{q^m}{j} \,. \tag{6.40}$$

The n_j satisfy

$$n_1 + 2n_2 + \dots rn_r = q^m \,.$$

For nonnegative real numbers $x_1, \dots, x_r$, consider the problem of minimizing

$$\sum_{j=1}^{r} \frac{x_j}{q^m} \log \frac{q^m}{j} = \frac{1}{q^m} \Bigg(\log q^m \Big(\sum_{j=1}^{r} x_j \Big) - \sum_{j=1}^{r} x_j \log j \Bigg) \tag{6.41}$$

subject to

$$x_1 + x_2 + \dots + x_r = q^m \,. \tag{6.42}$$

In view of (6.42), the problem reduces to maximizing

$$\sum_{j=1}^{r} x_j \log j$$

subject to (6.42). The desired extremum is attained at

$$x_r = q^m, \qquad x_{r-1} = \dots = x_1 = 0 \,,$$

which gives $\log q^m - \log r$ as the minimum value of (6.41). Setting $x_j = jn_j$ makes the value of (6.41) equal to (6.40). Thus

$$\log q^m \geq H(Q^m) \geq \log q^m - \log r \,,$$

whence

$$h(Q) = \lim_{m \to \infty} \frac{1}{m} H(Q^m) = \log q$$

as required. ∎

The asymptotic entropy of Q determines whether or not Q is central, according to the "asymptotic" analogue of Theorem 6.9.

THEOREM 6.10

The asymptotic entropy $h(Q)$ of a finite quasigroup Q of positive order n satisfies

$$0 \leq h(Q) \leq \log n\,.$$

Equality obtains on the right if and only if Q is central.

The inequalities just recall (6.39), while the "if" statement holds by Proposition 6.5. The remainder of this section is devoted to the proof of the "only if" statement. Let Q be a finite, nonempty, noncentral quasigroup. It must be shown that $h(Q) < \log |Q|$. In fact, it will be shown that there are positive constants w and c such that

$$\frac{1}{m} H(Q^m) \leq \log |Q| - w \log 2 + \frac{\log 2c}{m} \tag{6.43}$$

for all sufficiently large m.

Fix an element e of Q. For any positive integer m, set

$$x = (e, \ldots, e) \in Q^m\,.$$

Since Q is not central, the diagonal $\widehat{Q}$ is not a normal subquasigroup of Q^2. Then $\widehat{Q}$ is a proper subset of $\widehat{Q}F$ (compare Exercise 9 of Chapter 3). In particular,

$$\exists\, q \in Q\,.\, \exists\, (\alpha, \beta) \in \operatorname{Mlt} Q^2\,.\, e\alpha = e\beta = e\,, \quad q\alpha = s \neq t = q\beta\,. \tag{6.44}$$

Consider a random element

$$y = (y_1, \ldots, y_m)$$

of Q^m. The probability that its i-th component y_i coincides with q is $|Q|^{-1}$. Let $p = 1 - |Q|^{-1}$, the probability that y_i differs from q. The following lemma bounds the probability that y does not have even a certain small proportion u of its components coinciding with the element q.

LEMMA 6.3

For each p in the open unit interval $]0, 1[$, there are positive constants u, v, and c (with $c \geq 1$ and u irrational) such that

$$\sum_{k=0}^{\lfloor um \rfloor} \binom{m}{k} (1-p)^k p^{m-k} \leq c 2^{-vm}$$

for all nonnegative integers m.

PROOF For given $0 < r < 1$, let rT denote the circle of radius r centered on the origin in the complex plane. Then

$$\begin{aligned}
&\sum_{k=0}^{\lfloor um \rfloor} \binom{m}{k} (1-p)^k p^{m-k} \\
&\quad = \frac{1}{2\pi i} \int_{rT} \big(z(1-p)+p\big)^m \big(1 + z^{-1} + \cdots + z^{-\lfloor um \rfloor}\big) z^{-1} dz \\
&\quad = \frac{1}{2\pi i} \int_{rT} \frac{\big(z(1-p)+p\big)^m}{z^{\lfloor um \rfloor}} \cdot \frac{z^{1+\lfloor um \rfloor} - 1}{z(z-1)} dz \,.
\end{aligned}$$

For $z \in rT$, one has the estimates

$$\left| \frac{z^{1+\lfloor um \rfloor} - 1}{z(z-1)} \right| \leq \frac{r^{1+\lfloor um \rfloor} - 1}{r(r-1)} < \frac{2}{r(1-r)}$$

and

$$\left| \frac{\big(z(1-p)+p\big)^m}{z^{\lfloor um \rfloor}} \right| \leq \frac{\big(r(1-p)+p\big)^m}{r^{\lfloor um \rfloor}} \leq \left(\frac{r(1-p)+p}{r^u} \right)^m ,$$

whence

$$\sum_{k=0}^{\lfloor um \rfloor} \binom{m}{k} (1-p)^k p^{m-k} < \frac{2}{1-r} \left(\frac{r(1-p)+p}{r^u} \right)^m .$$

Now $r(1-p)+p < 1$, while $\lim_{u \to 0} r^u = 1$. The positive irrational constant u is thus chosen so small that

$$b = \frac{r^u}{r(1-p)+p} > 1 \,.$$

The lemma follows, with

$$c = \frac{2}{1-r} \geq 1$$

and $v = \log_2 b$. □

The irrationality of u in Lemma 6.3 is merely a technical convenience to separate the floor of um from its ceiling, regardless of the choice of the integer m.

An element

$$y = (y_1, \ldots . y_m)$$

of Q^m is called *good* if the number of its components coinciding with q exceeds um, the irrational constant u being associated by Lemma 6.3 with

$$p = \frac{|Q| - 1}{|Q|} \,.$$

A quasigroup conjugacy class of Q^m is called *good* if it contains a pair (x, y) with good y. If elements and classes are not good, they are called *bad*. By Lemma 6.3, there are at most $2^{-vm}c|Q|^m$ bad elements y. Each bad class contains at least one pair (x, y) with bad y. Thus the number of bad classes is at most

$$2^{-vm}c|Q|^m\,. \tag{6.45}$$

On the other hand, good classes are fairly large.

LEMMA 6.4
Each good quasigroup conjugacy class of Q^m contains at least $2^{um}|Q|^m$ elements, for all sufficiently large m.

PROOF Without loss of generality, one may consider the good class containing the pair (x, y) with

$$y = (q, \ldots, q, y_{r+1}, \ldots, y_m)\,,$$

where $r = \lceil um \rceil$. For each subset I of $\{1, \ldots, r\}$, there is a certain element γ_I of the stabilizer of x in $\mathrm{Mlt}\, Q^m$. This element γ_I is chosen to have the property that

$$y\gamma_I = (z_1, \ldots, z_r, y'_{r+1}, \ldots, y'_m)$$

for some y'_i in Q, where $z_i = s$ for i in I, but $z_j = t$ for j not in I. Thus the i-th components of γ_I may be taken as the α of (6.44), while the j-th components may be taken as β. As I ranges over the 2^r different subsets of $\{1, \ldots, r\}$, one obtains 2^r different elements $(x, y)\gamma_I = (x, y\gamma_I)$ in the conjugacy class, each having x in its first half. The result follows. □

Since $Q^m \times Q^m$ has $|Q|^{2m}$ elements, and each good conjugacy class has at least $2^{um}|Q|^m$ elements, there are at most

$$2^{-um}|Q|^m \tag{6.46}$$

good classes. Let w be the minimum of the two positive constants u and v. Recall $c \geq 1$. Since each class is either good or bad, (6.45) and (6.46) show that the total number of classes is at most

$$|Q|^m(2^{-vm}c + 2^{-um}) \leq 2c|Q|^m \cdot 2^{-wm}\,.$$

Proposition 6.3 then implies

$$H(Q^m) \leq \log|Q|^m - \log 2^{wm} + \log 2c\,,$$

from which the required inequality (6.43) follows.

6.10 Exercises

1. Show that a group is of real type if and only if each element is conjugate to its inverse.

2. For a group $(Q, \cdot, /, \backslash)$, show that the quasigroup $(Q, /)$ is of real type.

3. Verify directly that the convolution (6.3) is associative.

4. Let θ and φ be quasigroup class functions on a pique. Verify the equation $\theta'\varphi' = (\theta\varphi)'$.

5. Draw up a table of the various structures carried by (6.20)(a) through (d) in their various manifestations, e.g., zeta function on Q^2, identity endomorphism of $\mathbb{C}Q$, the $n \times n$ identity matrix, the function $G \to \{1\}$.

6. For a finite group P, verify the relation $\psi_i(x, y) = \chi_i(x\backslash y)$ between the basic quasigroup characters and the irreducible pique characters.

7. For a finite, nonempty quasigroup Q, show that each of the following determines the others:

   (a) The character table Ψ;

   (b) The unitary character table Υ;

   (c) The $V(G, Q)$-character table Ξ.

8. Show that centrally isotopic quasigroups have the same character table.

9. Give an example of isotopic quasigroups with different character tables.

10. Let p be a prime number larger than 3. and let $Q = \mathbb{Z}/p\mathbb{Z}$.

    (a) Let r be a nonzero element of $\mathbb{Z}/p\mathbb{Z}$. Show that $x \cdot y = xr + y$ defines a central rank 2 quasigroup structure $(Q, \cdot)$.

    (b) Let ρ be the transposition (12), and let λ be the cycle $(12 \dots p)$. Show that $x \circ y = x\rho + y\lambda$ defines a rank 2 quasigroup structure on Q. Invoke Theorem 3.10 (p. 81), or argue directly, to show that $(Q, \circ)$ is not central.

11. Show that almost all finite quasigroups are simple.

12. Let Q be a finite, nonempty quasigroup with character table Ψ. Show that

$$H(Q) = \sum_{j=1}^{s} \Big(\sum_{i=1}^{s} \big|\psi_{ij}\big|^2 \Big)^{-1} \log \Big(\sum_{i=1}^{s} \big|\psi_{ij}\big|^2 \Big) .$$

13. Using the strict concavity of the logarithm function, show that the upper bound $\log s$ for the entropy of a finite, nonempty quasigroup Q with s conjugacy classes is actually attained if and only if $s = |Q|$ and Q is abelian.

14. Exhibit finite piques P and Q for which $H(P \times Q) \neq H(P) + H(Q)$.

15. Let P and Q be finite loops. Show that $H(P \times Q) = H(P) + H(Q)$.

16. Show that for finite loops, the entropy and asymptotic entropy coincide.

6.11 Problems

1. For general finite nonempty quasigroups P and Q, what is the relationship between $h(P)$, $h(Q)$, and $h(P \times Q)$?

2. Let n be the order of a finite simple group. Is there a simple group S of order n such that $H(S) \leq H(Q)$ for all groups Q of order n?

3. For which quasigroup varieties $\mathbf{V}$ does there exist a function $b(s)$ such that a finite $\mathbf{V}$-quasigroup Q with s conjugacy classes has order at most $b(s)$? Note that the variety $\mathbf{G}$ of associative quasigroups has such a function [23, p. 461], while results such as Corollary 6.5 or Exercise 10 show that the variety $\mathbf{Q}$ of all quasigroups does not.

6.12 Notes

Section 6.1

If Q is a loop with identity element e, then the pique conjugacy classes of (Q, e) are the *loop conjugacy classes* considered by Bruck [21, p. 63].

Section 6.3

The concept of the centralizer ring of a permutation action is due to Wielandt [175]. The "V" in the notation $V(G, Q)$ stands for "Vertauschungsring." Theorem 6.1 was first proved in [146].

Section 6.5

Some sources use the term "association scheme" without the commutativity requirement (A4), and then describe schemes satisfying (A1) through (A4) as "commutative association schemes."

For the structure constants of $V(G, Q)$, compare [36, §9D]. In [6, Th. 2.1.4], the derivation of Theorem 6.4(a) from the commutativity axiom (A4) for association schemes is depicted as a consequence of "Schur's Lemma" [6, §1.3].

Section 6.7

Theorem 6.6 originally appeared in [91, (3.3)] and [148, 541(a)(b)]. Theorem 6.7 is a generalization of the group-theoretical result [36, 9.33]. Compare also [6, Th. II.3.6(ii)].

Section 6.8

Corollary 6.5 was initially conjectured in [152]. C.E. Praeger [132] attributes Theorem 6.8 to P.J. Cameron.

Section 6.9

See [159] for a quick introduction to some of the key information-theoretic aspects of entropy.

The full term "conjugate entropy" is used to make a distinction with the characteristic entropy concept introduced in Exercise 17 of Chapter 7.

Lemma 6.3 gives an appropriate and immediate version of the "Chernoff bound" of large deviation theory [29], [52, §3], [167, Lectures 4, 7].

Chapter 7

COMBINATORIAL CHARACTER THEORY

This chapter shows how more advanced aspects of the ordinary character theory of finite groups extend to finite quasigroups. At the same time, it becomes apparent that the theory is considerably enriched by the extension. The notation and conventions of the preceding chapter are used throughout. Section 7.1 shows that the congruence lattice of a finite quasigroup Q is determined by its character table. On the other hand, while the centrality of Q is decided by the character table of Q^2, it is not decided by the character table of Q itself. In particular, and in contrast to the situation in group theory, character tables of factors do not specify the character table of their product. Section 7.2 shows how character tables of homomorphic quasigroups are connected, while Section 7.3 deals with the dual situation where the multiplication groups are nested. Section 7.4 covers Frobenius reciprocity and induction, including the quasigroup analogue of Artin's Theorem. Section 7.5 studies the linear characters of a quasigroup.

7.1 Congruence lattices

The congruences on a quasigroup Q form a lattice under inclusion. The quasigroup Q is said to be *subdirectly irreducible* if this lattice has a unique minimal element, known as the *socle*. If Q is a group, then the congruence lattice is isomorphic to the lattice of normal subgroups under the map $V \mapsto 1^V$ taking a congruence V to the congruence class of the identity element. Since the normal subgroups of a finite group are just the kernels of the ordinary group characters, the character table of a finite group determines its lattice of congruences directly. This character table property extends to general finite quasigroups, but the proof is not as immediate.

THEOREM 7.1

The character table of a finite quasigroup Q determines its congruence lattice.

PROOF It will be shown that the matrix $H = [\eta_{ij}]$ of (6.29) determines the congruence lattice. The theorem then follows by Corollary 6.4(d) (p. 156).

Let V be a congruence relation on Q. Since V is a subquasigroup of Q^2 containing $\widehat{Q}$, it is invariant under the diagonal action (2.13) of G, and so is a union of conjugacy classes, including $C_1 = \widehat{Q}$. This means that the endomorphism α of $\mathbb{C}Q$ defined by

$$x\alpha = \sum_{(x,y)\in V} y$$

for x in Q can be written as

$$\alpha = \sum_{j\in V_1} \alpha_j$$

for a subset V_1 of $\{1,\dots,s\}$ containing 1. In particular, α lies in $V(G,Q)$. Let V_0 denote the complement of V_1 in $\{1,\dots,s\}$. Let $|V| = nv$, so $v = |x^V|$ for each x in Q. (Compare Exercise 7 in Chapter 3.) Then $\alpha^2 = v\alpha$, and the idempotent $v^{-1}\alpha$ of $V(G,Q)$ may be expressed as

$$v^{-1}\alpha = \sum_{i\in V'} \epsilon_i$$

for some subset V' of $\{1,\dots,s\}$. Now

$$\begin{aligned}
\frac{1}{v}\sum_{j\in V_1}\alpha_j &= v^{-1}\alpha \\
&= \sum_{i\in V'}\epsilon_i \\
&= \sum_{i\in V'}\sum_{j=1}^{s}\eta_{ij}\alpha_j \\
&= \sum_{i\in V'}\sum_{j\in V_1}\eta_{ij}\alpha_j + \sum_{i\in V'}\sum_{j\in V_0}\eta_{ij}\alpha_j\,.
\end{aligned}$$

Equating coefficients of α_j, one has

$$v\sum_{i\in V'}\eta_{ij} = \begin{cases} 1 & \text{for } j\in V_1 \supseteq \{1\}\,; \\ 0 & \text{for } j\in V_0\,. \end{cases} \tag{7.1}$$

For the congruence V on Q, let H_V be the submatrix of H consisting of the rows with indices in V'. Then the matrix vH_V has either 1 or 0 as its column sums. The congruence V is the union of those conjugacy classes C_j for which the j-th column sum of vH_V or H_V is nonzero.

Conversely, consider a subset V' of $\{1,\dots,s\}$. Let H' denote the submatrix of H consisting of the rows with indices in V'. Suppose that there are

complementary subsets V_0, V_1 of $\{1, \ldots, s\}$, the element 1 lying in V_1, and a positive integer v such that (7.1) is satisfied. Let

$$\alpha = \sum_{j \in V_1} \alpha_j \quad \text{and} \quad V = \bigcup_{j \in V_1} C_j \,.$$

Then

$$\begin{aligned} \frac{1}{v}\alpha &= \frac{1}{v} \sum_{j \in V_1} \alpha_j \\ &= \sum_{j=1}^{s} \sum_{i \in V'} \eta_{ij} \alpha_j \\ &= \sum_{i \in V'} \epsilon_i \end{aligned}$$

is idempotent, whence $\alpha^2 = v\alpha$, and V is transitive. Now V is reflexive since $1 \in V_1$. Also, V is invariant under the diagonal action of G. It follows by Proposition 2.1 (p. 39) that V is a congruence on Q.

Thus the congruence relations on Q are precisely the conjugacy class unions

$$V = \bigcup_{j \in V_1} C_j$$

for which there is a submatrix H_V of H consisting of rows with indices in a subset V' of $\{1, \ldots, s\}$ and a positive integer v such that (7.1) is satisfied. In particular, H specifies the congruence lattice of Q. □

COROLLARY 7.1

The character table of a finite quasigroup Q determines whether or not Q is subdirectly irreducible.

COROLLARY 7.2

The character table $\Psi(Q^2)$ of the direct square Q^2 of a finite quasigroup Q determines whether or not Q is central.

PROOF A quasigroup Q is central if and only if the congruence lattice of Q^2 contains a common complement to the kernels of the two projections

$$\pi_i : Q^2 \to Q; (q_1, q_2) \mapsto q_i$$

for $i = 1, 2$ [73] [78]. By Theorem 7.1, the congruence lattice of Q^2 is determined by $\Psi(Q^2)$. □

Since the character table of a finite quasigroup Q does not determine whether Q is central, Corollary 7.2 shows that the character table of Q does not determine the character table of the direct square Q^2 of Q.

7.2 Quotients

Suppose that $\theta : P \twoheadrightarrow Q$ is a quasigroup epimorphism. If P is a group, and $D : Q \to \mathrm{Aut}_{\mathbb{C}}V$ represents Q as a group of automorphisms of a complex vector space V, then the composite $\theta D : P \to \mathrm{Aut}_{\mathbb{C}}V$ represents P. Composing with the trace map $\mathrm{Tr} : \mathrm{Aut}_{\mathbb{C}}V \to \mathbb{C}$, it is a trivial matter to lift characters from the quotient Q up to P. For general finite quasigroups P, a comparable lifting result holds. The proof is much less direct, and will occupy the entire section.

THEOREM 7.2 (***Quotient Theorem***)
Let $\theta : P \twoheadrightarrow Q$ be a quasigroup epimorphism, with corresponding diagonal

$$\theta^{\mathsf{II}} : P^2 \to Q^2; (x, y) \mapsto (x\theta, y\theta). \tag{7.2}$$

Then for each basic character

$$\psi_k : Q^2 \to \mathbb{C}$$

of Q, the lift

$$\theta^{\mathsf{II}}\psi_k : P^2 \to \mathbb{C}$$

is a basic character of P.

Let $V(G, Q)$ be the centralizer ring of the multiplication group G of Q. Let $V(F, P)$ be the centralizer ring of the multiplication group F of P. Let $A_1, \ldots, A_s$ denote the respective incidence matrices of the conjugacy classes $C_1, \ldots, C_s$ of Q. The epimorphism $\theta : P \to Q$ induces the epimorphism $\mathrm{Mlt}\,\theta : F \to G$ according to (2.12). For each conjugacy class D of P, the subset

$$D\theta^{\mathsf{II}} = \{(x_1\theta, x_2\theta) \mid (x_1, x_2) \in D\}$$

of Q^2 is contained within a conjugacy class of Q, since for f in F one has

$$(x_1, x_2)f = (y_1, y_2) \quad \Rightarrow \quad (x_1\theta, x_2\theta)f\,\mathrm{Mlt}\,\theta = (y_1\theta, y_2\theta)\,.$$

For each $1 \leq i \leq s$, let

$$D_{i1}, \ldots, D_{ir_i}$$

be a complete list of all those conjugacy classes D with $D\theta^{\mathsf{II}} \subseteq C_i$. Take $D_{11} = \widehat{P}$. Note $D_{ij}\theta^{\mathsf{II}} = C_i$ for $1 \leq i \leq s$ and $1 \leq j \leq r_i$. Then $r_i > 0$ for $1 \leq i \leq s$, since given a typical element $(x\theta, y\theta)$ of C_i, one has (x, y) in D_{ij} for some j. Let B_{ij} be the incidence matrix of D_{ij} for $1 \leq i \leq s$ and $1 \leq j \leq r_i$. Let

$$\beta_{ij} : \mathbb{C}P \to \mathbb{C}P; x \mapsto \sum_{(x,y)\in B_ij} y$$

be the corresponding endomorphism of $\mathbb{C}P$. Then there are bases $\{\alpha_1, \ldots, \alpha_s\}$ or $\{A_1, \ldots, A_s\}$ for $V(G,Q)$ and $\{\beta_{11}, \ldots, \beta_{sr_s}\}$ or $\{B_{11}, \ldots, B_{sr_s}\}$ for $V(F,P)$. Define a linear map

$$\phi : V(G,Q) \to V(F,P); \alpha_i \mapsto \sum_{j=1}^{r_i} \beta_{ij} \tag{7.3}$$

and its matrix version

$$\sigma : V(G,Q) \to V(F,P); A_i \mapsto \sum_{j=1}^{r_i} B_{ij} \,. \tag{7.4}$$

In general, these maps are not algebra homomorphisms.

Consider a particular element (a,b) of a given conjugacy class D_{ij} of P. Let n_{ij} be the number of elements a' of P with $a\theta = a'\theta$ and (a',b) in D_{ij}. By homogeneity, this number only depends on the indices i, j, and not on the particular choice of (a,b). Indeed

$$a' \in a^{\ker\theta} \cap D_{ij}(b) \quad \Leftrightarrow \quad a'f \in af^{\ker\theta} \cap D_{ij}(bf)$$

for f in F. One also has that

$$n_{ij} = \frac{|Q| \cdot |D_{ij}|}{|P| \cdot |C_{i|}} \,, \tag{7.5}$$

since $|D_{ij}|/|P|$ and $n_{ij}|C_i|/|Q|$ both count the set of all a' in P with (a',b) in D_{ij}.

LEMMA 7.1

For given conjugacy classes D_{ij} of P and C_k of Q, the equation

$$B_{ij}A_k^\sigma = n_{ij}(A_jA_k)^\sigma \tag{7.6}$$

holds in the centralizer ring $V(F,P)$.

PROOF Let

$$B_{ij}A_k^\sigma = \sum_{l=1}^{s} \sum_{m=1}^{r_l} c_{ij,k}^{lm} B_{lm} \,.$$

Fix an element (a,b) of the conjugacy class D_{lm} of P. Then the coefficient $c_{ij,k}^{lm}$ represents the number of elements p of P with $(a\theta, b\theta)$ in C_k and $(p.b)$ in D_{ij}. Now by (6.17),

$$A_kA_i = \sum_{k=1}^{s} c_{ki}^{l} A_l$$

in $V(G,Q)$. Since $(a\theta, b\theta)$ lies in C_k, the structure constant c_{ki}^l represents the number of elements q of Q with $(a\theta, q)$ in C_k and $(q, b\theta)$ in C_i. Given $(q, b\theta)$ in C_i, there are precisely n_{ij} elements p of P with $p\theta = q$ and (p, b) in D_{ij}. For each such p, one has $(a\theta, p\theta) = (a\theta, q)$ lying in C_k. Thus $c_{ij,k}^{lm} = n_{ij}c_{ki}^l$. Since

$$\begin{aligned}(A_jA_k)^\sigma &= \sum_{l=1}^{s} c_{ki}^l A_l \\ &= \sum_{l=1}^{s}\sum_{m=1}^{r_l} c_{ki}^l B_{lm}\,,\end{aligned}$$

the relation (7.6) in $V(F,P)$ follows. □

The centralizer ring $V(G,Q)$ has the basis (6.26) of idempotents. Then for $1 \le i,k \le s$, (6.28) yields

$$E_kA_i = \xi_{ik}E_k\,. \tag{7.7}$$

LEMMA 7.2

For a given conjugacy class D_{ij} of P and basic idempotent E_k of $V(G,Q)$, the equation

$$B_{ij}E_k^\sigma = n_{ij}\xi_{ik}E_k^\sigma \tag{7.8}$$

holds in the centralizer ring $V(F,P)$.

PROOF Since

$$E_k = \sum_{l=1}^{s} \eta_{kl}A_l$$

by (6.29), one has

$$\begin{aligned}B_{ij}E_k^\sigma &= \sum_{l=1}^{s} \eta_{kl}B_{ij}A_l^\sigma \\ &= \sum_{l=1}^{s} \eta_{kl}n_{ij}(A_iA_l)^\sigma \\ &= n_{ij}\Big(\sum_{l=1}^{s} \eta_{kl}A_lA_i\Big)^\sigma \\ &= n_{ij}(E_kA_i)^\sigma \\ &= n_{ij}\xi_{ik}E_k^\sigma\,,\end{aligned}$$

the second equality holding by (7.6) and the last by (7.7). □

Lemma 7.2 shows that for each $1 \leq k \leq s$, the subspace $\mathbb{C}P\epsilon_k^\phi$ of $\mathbb{C}P$ is an eigenspace for each β_{ij}, with corresponding eigenvalue $n_{ij}\xi_{ik}$. It follows that the column vector

$$\begin{bmatrix} n_{11}\xi_{1k} \\ \vdots \\ n_{sr_s}\xi_{sk} \end{bmatrix}$$

is a column of the first eigenmatrix of F on P. Let the dimension of the subspace $\mathbb{C}P\epsilon_k^\phi$ be d_k. Then the row vector

$$\sqrt{d_k}\,|P|\Big[\,\frac{n_{11}\xi_{1k}}{|B_{11}|}\cdots\frac{n_{sr_s}\xi_{sk}}{|B_{sr_s}|}\,\Big] \tag{7.9}$$

is a row of the character table $\Psi(P)$ of P. It remains to calculate d_k.

LEMMA 7.3
For $1 \leq k \leq s$, the element

$$\frac{|Q|}{|P|}E_k^\sigma$$

is an idempotent of $V(F,P)$. Then d_k is the trace f_k of E_k.

PROOF Since each element of Q has $|P|/|Q|$ pre-images under θ, one has that

$$\sum_{j=1}^{r_i} n_{ij} = \frac{|P|}{|Q|}$$

for $1 \leq i \leq s$. Then

$$\begin{aligned} E_k^\sigma E_k^\sigma &= E_k^\sigma\Big(\sum_{i=1}^{s}\eta_{ki}A_i\Big)^\sigma \\ &= \sum_{i=1}^{s}\eta_{ki}E_k^\sigma\sum_{j=1}^{r_s}B_{ij} \\ &= \sum_{i=1}^{s}\eta_{ki}\xi_{ik}\sum_{j=1}^{r_s}n_{ij}E_k^\sigma \\ &= \frac{|P|}{|Q|}E_k^\sigma\sum_{i=1}^{s}\eta_{ki}\xi_{ik}\,, \end{aligned}$$

the penultimate equality following by Lemma 7.2. Now the matrices $[\eta_{ki}]$ and $[\xi_{ik}]$ are mutually orthogonal, so that

$$\sum_{i=1}^{s}\eta_{ki}\xi_{ik} = 1 \quad \text{and} \quad E_k^\sigma E_k^\sigma = \frac{|P|}{|Q|}E_k^\sigma\,.$$

The first statement of Lemma 7.3 follows. In particular, the idempotent

$$\frac{|Q|}{|P|}\epsilon_k^\phi$$

is the projection operator of $\mathbb{C}P$ onto the subspace $\mathbb{C}P\epsilon_k^\phi$. But

$$\begin{aligned}\operatorname{Tr}\epsilon_k^\phi &= \operatorname{Tr}\Big(\sum_{i=1}^{s}\eta_{ki}A_i^\sigma\Big)\\ &= \sum_{i=1}^{s}\eta_{ki}\sum_{j=1}^{r_i}\operatorname{Tr}B_{ij}\\ &= \eta_{k1}|P|\\ &= f_k\frac{|P|}{|Q|}\,,\end{aligned}$$

the last equality holding by Lemma 6.2(a). Thus $d_k = f_k$ as required. □

Using this value for d_k and (7.5) for each n_{ij}, the row vector (7.9) becomes

$$\sqrt{f_k}\,|Q|\Big[\,\frac{\xi_{1k}}{|C_1|}\cdots\frac{\xi_{sk}}{|C_s|}\,\Big]\,. \tag{7.10}$$

This vector is just the k-th row of the character table $\Psi(Q)$ of Q, expanded by having its i-th entry written r_i times for each $1 \le i \le s$. As a row of the character table of P, (7.10) represents the complex class function on P sending each element of B_{ij} to the value of ψ_k on C_i. This is precisely the function (7.2), which is thus a basic character of P. The proof of the Quotient Theorem 7.2 is completed.

7.3 Fusion

The Quotient Theorem 7.2 related the character tables $\Psi(Q)$ and $\Psi(P)$ for a quasigroup epimorphism $Q \twoheadrightarrow P$ inducing an epimorphism $\operatorname{Mlt}Q \twoheadrightarrow \operatorname{Mlt}P$ of the corresponding combinatorial multiplication groups. A dual situation arises when there are two quasigroup structures $(Q,+)$ and $(Q,\cdot)$ on the same underlying set Q, such that $\operatorname{Mlt}(Q,+)$ embeds as a subgroup of $\operatorname{Mlt}(Q,\cdot)$ with the group monomorphism $\operatorname{Mlt}(Q,+) \hookrightarrow \operatorname{Mlt}(Q,\cdot)$. Corollary 2.2 and Theorem 3.5 provide examples of this. A more general case is described as follows.

PROPOSITION 7.1
Suppose that a quasigroup $(Q,\cdot)$ *is principally isotopic to a loop* $(Q,+,e)$. *Then* $\mathrm{Mlt}(Q,+)$ *is a subgroup of* $\mathrm{Mlt}(Q,\cdot)$.

PROOF Let the principal isotopy be $(\alpha,\beta,1_Q):(Q,+)\to(Q,\cdot)$, so that

$$x^\alpha\cdot y^\beta = x+y \tag{7.11}$$

for x,y in Q. By (7.11), it follows that

$$L_+(x)=\beta L_\cdot(x^\alpha) \quad \text{and} \quad R_+(y)=\alpha R_\cdot(y^\beta)\,.$$

Since $R_+(e)=L_+(e)=1_Q$, one has $\alpha=R_\cdot(e^\beta)^{-1}$ and $\beta=L_\cdot(e^\alpha)^{-1}$. Then

$$\begin{aligned}\mathrm{Mlt}(Q,+) &= \langle L_+(q),R_+(q)\mid q\in Q\rangle\\ &= \langle L_\cdot(e^\alpha)^{-1}L_\cdot(q^\alpha),R_\cdot(e^\beta)^{-1}R_\cdot(q^\beta)\mid q\in Q\rangle\\ &\le \langle L_\cdot(x),R_\cdot(x)\mid x\in Q\rangle=\mathrm{Mlt}(Q,\cdot)\,,\end{aligned}$$

as required. □

REMARK 7.1 In Proposition 7.1, the requirement that $(Q,+,e)$ be a loop is essential (Exercise 1). □

The topic of fusion investigates how the character theory of $(Q,\cdot)$ depends on the character theory of $(Q,+)$ when $H=\mathrm{Mlt}(Q,+)$ is a subgroup of $G=\mathrm{Mlt}(Q,\cdot)$. Because H is a subgroup of G, an endomorphism of the $\mathbb{C}G$-module $\mathbb{C}Q$ is automatically an endomorphism of the $\mathbb{C}H$-module $\mathbb{C}Q$. Thus the centralizer ring $V(G,Q)$ is a subring of the centralizer ring $V(H,Q)$. Suppose that (6.10) is the conjugacy class partition of $(Q,\cdot)$, and that the corresponding conjugacy class partition of $(Q,+)$ is

$$Q^2=\sum_{i=1}^{s}\sum_{j=1}^{r_i}D_{ij} \tag{7.12}$$

with $C_i=D_{i1}+\cdots+D_{ir_i}$ for $1\le i\le s$. Note that $r_1=1$ and $D_{11}=\widehat{Q}$. Let B_{ij} be the incidence matrix of D_{ij} for $1\le i\le s$ and $1\le j\le r_i$. Thus

$$A_i=\sum_{j=1}^{r_i}B_{ij} \tag{7.13}$$

for $1\le i\le s$.

The partition (7.12) and the corresponding partition of the columns of the character table $\Psi(Q,+)$ of $(Q,+)$ are called the $(Q,\cdot)$-*fusion of* $(Q,+)$-*classes*

or the *G-fusion of H-classes*. Since $V(G,Q)$ is a subring of $V(H,Q)$, each idempotent ϵ_i from (6.25) is a sum

$$\epsilon_i = \sum_{j=1}^{t_i} \epsilon_{ij} \tag{7.14}$$

of t_i distinct minimal idempotents of $V(H,Q)$. The matrix version of (7.14) is

$$E_i = \sum_{j=1}^{t_i} E_{ij}\,.$$

Since

$$\mathbb{C}Q = \bigoplus_{i=1}^{s} \mathbb{C}Q\epsilon_i = \bigoplus_{i=1}^{s}\bigoplus_{j=1}^{t_i} \mathbb{C}\epsilon_{ij}\,,$$

the set $\{\{\epsilon_{ij} \mid 1 \le j \le t_i\} \mid 1 \le i \le s\}$ forms a basis of $V(H,Q)$ with

$$\sum_{i=1}^{s} t_i = \sum_{i=1}^{s} r_i \tag{7.15}$$

elements. Taking

$$\mathbb{C}\Big(\sum_{q\in Q} q\Big) = \mathbb{C}Q\epsilon_1 = \mathbb{C}Q\epsilon_{11}\,,$$

one has

$$t_1 = r_1 = 1\,. \tag{7.16}$$

The matrix bases $\{A_1,\dots,A_s\}$ and $\{E_1,\dots,E_s\}$ of $V(G,Q)$ are connected by the relation

$$E_i = \sum_{j=1}^{s} \eta_{ij}^G A_j \tag{7.17}$$

for $1 \le i \le s$ — compare (6.29). Similarly, the matrix bases

$$\{B_{11},\dots,B_{sr_s}\} \quad \text{and} \quad \{E_{11},\dots,E_{st_s}\}$$

of $V(G,Q)$ are connected by the relation

$$E_{kl} = \sum_{i=1}^{s}\sum_{j=1}^{r_i} \eta_{kl,ij}^H B_{ij} \tag{7.18}$$

for $1 \le k \le s$ and $1 \le l \le t_k$. The character table $\Psi(Q,\cdot)$ of $(Q,\cdot)$ is the matrix $[\psi_{ik}^G]$ with

$$\psi_{ik}^G = \frac{|Q|}{\sqrt{\operatorname{Tr} E_i}}\overline{\eta}_{ik}^G\,, \tag{7.19}$$

and the character table $\Psi(Q,+)$ of $(Q,+)$ is the matrix $[\psi^H_{ij,kl}]$ with

$$\psi^H_{ij,kl} = \frac{|Q|}{\sqrt{\mathrm{Tr}\, E_{ij}}}\overline{\eta}^H_{ij,kl}\,. \tag{7.20}$$

The quasigroup $(Q,\cdot)$, or more precisely its multiplication group G, determines the partition

$$\{\{\epsilon_{ij} \mid 1 \le j \le t_i\} \mid 1 \le i \le s\} \tag{7.21}$$

of the basis

$$\{\epsilon_{ij} \mid 1 \le i \le s, 1 \le j \le t_i\}$$

of $V(H,Q)$, and a corresponding partition

$$\{\{\psi^H_{ij} \mid 1 \le j \le t_i\} \mid 1 \le i \le s\}. \tag{7.22}$$

of the set of basic characters of $(Q,+)$, i.e., of the set of rows of $\Psi(Q,+)$. The partitions (7.21) and (7.22) are called the *G-fusion of H-characters* or the *$(Q,\cdot)$-fusion of $(Q,+)$-characters*. The dual of the Quotient Theorem 7.2 may then be formulated as follows.

THEOREM 7.3 (***Fusion Theorem***)
Let $(Q,+)$ and $(Q,\cdot)$ be two quasigroup structures on the set Q. Suppose that $\mathrm{Mlt}(Q,+)$ is a subgroup of $\mathrm{Mlt}(Q,\cdot)$. Then the character table $\Psi(Q,\cdot)$ of $(Q,\cdot)$ is determined by the character table $\Psi(Q,+)$ of $(Q,+)$ together with the $(Q,\cdot)$-fusion of the $(Q,+)$-classes and $(Q,+)$-characters.

PROOF By (7.14) and (7.18) for each $1 \le i \le s$, one has

$$E_i = \sum_{j=1}^{t_i} E_{ij} = \sum_{j=1}^{t_i}\sum_{k=1}^{s}\sum_{l=1}^{r_k} \eta^H_{ij,kl} B_{kl} = \sum_{k=1}^{s}\sum_{l=1}^{r_k}\Big(\sum_{j=1}^{t_i}\eta^H_{ij,kl}\Big)B_{kl}\,.$$

But by (7.17) and (7.13), one also has

$$E_i = \sum_{k=1}^{s}\eta^G_{ik}A_k = \sum_{k=1}^{s}\eta^G_{ik}\sum_{l=1}^{r_k}B_{kl} = \sum_{k=1}^{s}\sum_{l=1}^{r_k}\eta^G_{ik}B_{kl}\,.$$

Equating coefficients of B_{kl} gives

$$\eta^G_{ik} = \sum_{j=1}^{t_i}\eta^H_{ij,kl} \tag{7.23}$$

for each $1 \le i \le s$ and $1 \le l \le r_k$. (Note the equality of the various right-hand sides of (7.23) obtained for $1 \le l \le r_k$.) The theorem now follows from

(7.19), (7.20), and (7.23), provided that $\operatorname{Tr} E_i$ is determined by the data. But by (7.14) and Corollary 6.4(c),

$$\operatorname{Tr} E_i = \sum_{j=1}^{t_i} \operatorname{Tr} E_{ij} = \sum_{j=1}^{t_i} \left(\psi^H_{ij,11}\right)^2, \tag{7.24}$$

so the proof of the theorem is complete. □

The explicit determination of the character table of $(Q,\cdot)$ from the character table of $(Q,+)$ and the $(Q,\cdot)$-fusions, promised by the Fusion Theorem 7.3, is best described geometrically. Consider the specification of the i-th basic character ψ^Q_i of $(Q,\cdot)$. In the fusion data, this character corresponds to the fusion of the t_i basic characters

$$\psi^H_{i1}, \ldots, \psi^H_{it_i}$$

of $(Q,+)$. For each conjugacy class D_{kl} of $(Q,+)$, there is a t_i-dimensional complex vector

$$\mathbf{w}_{kl} = \left[\psi^H_{i1,kl}, \ldots, \psi^H_{it_i,kl}\right]. \tag{7.25}$$

In particular, for $(k,l) = (1,1)$ one obtains the *leading vector*

$$\mathbf{w}_{11} = \left[(\operatorname{Tr} E_{i1})^{1/2}, \ldots, (\operatorname{Tr} E_{it_i})^{1/2}\right] \tag{7.26}$$

with positive real components. These vectors $\mathbf{w}_{kl}$ may be taken to lie in the t_i-dimensional complex vector space $W = \mathbb{C}^{t_i}$. The subspace $W_0 = \mathbb{C}\mathbf{w}_{11}$ is called the *principal subspace*; its elements are called *principal vectors*. An inner product $(\mathbf{x}|\mathbf{y}) = \mathbf{x}\mathbf{y}^*$ is given on W, where * denotes the conjugate transpose. The corresponding norm is $\|\mathbf{x}\|$ with $\|\mathbf{x}\|^2 = (\mathbf{x}|\mathbf{x})$. The character ψ^Q_i is then specified by least squares approximations as follows.

THEOREM 7.4

The value ψ^G_{ik} of a basic character ψ_i of $(Q,\cdot)$ on the k-th conjugacy class C_k of $(Q,\cdot)$ is given as

$$\psi^G_{ik} = (\mathbf{w}_{kl}|\mathbf{w}_{11})/\|\mathbf{w}_{11}\| \tag{7.27}$$

for each $1 \le l \le r_i$.

PROOF By (7.24) and (7.26), $\left(\operatorname{Tr} E_i\right)^{1/2} = \|\mathbf{w}_{11}\|$. Then by (7.19), (7.23) and (7.20), one has

$$\|\mathbf{w}_{11}\|\psi^G_{ik} = |Q|\overline{\eta}^G_{ik} = |Q|\sum_{j=1}^{t_i} \overline{\eta}^H_{ij,kl} = \sum_{j=1}^{t_i} \psi^H_{ij,kl}(\operatorname{Tr} E_{ij})^{1/2} = (\mathbf{w}_{kl}|\mathbf{w}_{11}).$$

The result follows. □

The geometrical significance of Theorem 7.4 is that the vectors $\mathbf{w}_{k1}, \ldots, \mathbf{w}_{kr_k}$ all lie in a hyperplane orthogonal to the principal subspace. The intersection of this hyperplane with the principal subspace is a single point, the principal vector that is closest to each of the vectors $\mathbf{w}_{k1}, \ldots, \mathbf{w}_{kr_k}$. As a principal vector, this point is a scalar multiple of the unit vector $\mathbf{w}_{11}/\|\mathbf{w}_{11}\|$ pointing in the direction of the leading vector. The scalar is the character value ψ^G_{ik}. In other words, the character value is the unique scalar λ that minimizes the expression

$$\|\mathbf{w}_{kl} - \lambda(\mathbf{w}_{11}/\|\mathbf{w}_{11}\|)\|$$

for each $1 \leq i \leq r_k$, picking a unique value to assign to each class C_k in place of the vectors $\mathbf{w}_{k1}, \ldots, \mathbf{w}_{kr_k}$ of possible values. One thus picks the unique best approximation to these vectors in the one-dimensional subspace of principal vectors, and then takes the character value to be the component of this best approximation with respect to an orthonormal basis of the principal subspace.

Another condition, very useful for the completion of partial fusion data, is the *Magic Rectangle Condition*, (7.28) below.

THEOREM 7.5

Fix $i, k \in \{1, \ldots, s\}$. Then for each $l \in \{1, \ldots, l_i\}$ and $l' \in \{1, \ldots, r_k\}$, the relation

$$\frac{\sum_{j=1}^{r_k} |D_{kj}| \psi^H_{il,kj}}{\sum_{j=1}^{r_k} |D_{kj}| \psi^H_{il,11}} = \frac{\sum_{j'=1}^{t_l} \psi^H_{ij',11} \psi^H_{ij',kl'}}{\sum_{j'=1}^{t_l} \psi^H_{ij',11} \psi^H_{ij',11}} \tag{7.28}$$

holds.

PROOF The matrix bases

$$\{E_1, \ldots, E_s\} \quad \text{and} \quad \{A_1, \ldots, A_s\}$$

of $V(G, Q)$ are connected by the relation

$$A_k = \sum_{i=1}^{s} \xi^G_{ki} E_i \tag{7.29}$$

for $1 \leq k \leq s$ — compare (6.28). Similarly, the matrix bases

$$\{E_{11}, \ldots, E_{st_s}\} \quad \text{and} \quad \{B_{11}, \ldots, B_{sr_s}\}$$

of $V(G, Q)$ are connected by the relation

$$B_{kl} = \sum_{i=1}^{s} \sum_{j=1}^{r_i} \xi^H_{kl,ij} E_{ij} \tag{7.30}$$

for $1 \leq k \leq s$ and $1 \leq l \leq t_k$. Now by (7.13) and (7.30), one has

$$A_k = \sum_{l=1}^{rk} B_{kl} = \sum_{l=1}^{rk} \sum_{i=1}^{s} \sum_{j=1}^{r_i} \xi^H_{kl,ij} E_{ij} = \sum_{i=1}^{s} \sum_{j=1}^{r_i} \Big(\sum_{l=1}^{r_k} \xi^H_{kl,ij} \Big) E_{ij} \,.$$

But by (7.29) and (7.14), one also has

$$A_k = \sum_{i=1}^{s} \xi_{ki}^G E_i = \sum_{i=1}^{s} \xi_{ki}^G \sum_{j=1}^{t_i} E_{ij} = \sum_{i=1}^{s} \sum_{j=1}^{t_i} \xi_{ki}^G E_{ij} \,.$$

Equating coefficients of E_{ij} gives

$$\xi_{ki}^G = \sum_{l=1}^{r_k} \xi_{kl,ij}^H \tag{7.31}$$

for each $1 \le i \le s$ and $1 \le j \le t_i$. Recalling

$$\psi_{ik}^G = \frac{\sqrt{\operatorname{Tr} E_i}}{|C_k|} |Q| \cdot \xi_{ki}^G$$

and

$$\psi_{ij,kl}^H = \frac{\sqrt{\operatorname{Tr} E_{ij}}}{|D_{kl}|} |Q| \cdot \xi_{kl,ij}^H \,,$$

(7.31) yields

$$\psi_{ik}^G = \frac{\sqrt{\operatorname{Tr} E_i}}{\sqrt{\operatorname{Tr} E_{ij}}} \sum_{l=1}^{r_k} \frac{|D_{kl}|}{|C_k|} \psi_{ij,kl}^H \,.$$

But by Theorem 7.4,

$$\psi_{ik}^G = \frac{1}{\sqrt{\operatorname{Tr} E_i}} \sum_{j'=1}^{t_i} \psi_{ij',kl'}^H \sqrt{\operatorname{Tr} E_{ij}} \,.$$

The Magic Rectangle Condition follows on equating these two expressions for ψ_{ik}^G and cross-multiplying. □

In cases such as the bottom right-hand part of Exercise 3(f) at the end of this chapter, the condition (7.28) explicitly yields magic rectangles, in which all the (unweighted) row sums and column sums are equal.

7.4 Induction

Let P be a nonempty subquasigroup of the finite quasigroup Q. Now the relative multiplication group of P in Q is a subgroup of the multiplication group of Q. It follows that the quasigroup conjugacy class partition of P may be written in such a form

$$P^2 = \sum_{i=1}^{s} \sum_{j=1}^{r_i} D_{ij} \tag{7.32}$$

that each part D_{ij} is a subset of a corresponding quasigroup conjugacy class C_i of Q. (If P^2 does not intersect C_i, then $r_i = 0$.) For $1 \le i \le s$, define

$$D_i = \sum_{j=1}^{r_i} D_{ij}.$$

Then the *induction* map

$$\uparrow_P^Q : \mathbb{C}\mathrm{Cl}(P) \to \mathbb{C}\mathrm{Cl}(Q); f \mapsto f^Q$$

is given by

$$|Q|^{-2} \sum_{(x,y)\in C_i} f^Q(x,y) = |P|^{-2} \sum_{(x,y)\in D_i} f(x,y)\,. \tag{7.33}$$

Using the convention of (6.6), this may be written in the form

$$f^Q(C_i) = \frac{|Q^2|}{|P^2|} f(D_i) = \frac{|Q|^2}{|P|^2} \sum_{j=1}^{r_i} f(D_{ij})\,. \tag{7.34}$$

These simple formulas subsume the more complicated induction formulas used for group class functions (Exercise 4).

Along with the induction map $\uparrow_P^Q : \mathbb{C}\mathrm{Cl}(P) \to \mathbb{C}\mathrm{Cl}(Q)$ given by (7.33), there is also a *restriction* map

$$\downarrow_P^Q : \mathbb{C}\mathrm{Cl}(Q) \to \mathbb{C}\mathrm{Cl}(P); f \mapsto f\big|_{P^2}.$$

Under the inner products (6.7), namely $\langle\ ,\ \rangle_P$ on $\mathbb{C}\mathrm{Cl}(P)$ and $\langle\ ,\ \rangle_Q$ on $\mathbb{C}\mathrm{Cl}(Q)$, these linear mappings are mutually adjoint.

THEOREM 7.6 (***Frobenius Reciprocity***)

For class functions f in $\mathbb{C}\mathrm{Cl}(Q)$ and g in $\mathbb{C}\mathrm{Cl}(P)$,

$$\langle f, g\uparrow_P^Q\rangle_Q = \langle f\downarrow_P^Q, g\rangle_P\,. \tag{7.35}$$

PROOF

$$\begin{aligned}
\langle f, g\uparrow_P^Q\rangle_Q &= \frac{1}{|Q|^2}\sum_{i=1}^{s}\sum_{(z,t)\in C_i} f(t,z)g\uparrow_P^Q(z,t)\\
&= \frac{1}{|Q|^2}\sum_{i=1}^{s}\sum_{(z,t)\in C_i} f(t,z)\frac{|Q|^2}{|C_i|\cdot|P|^2}g(D_i)\\
&= \frac{1}{|P|^2}\sum_{i=1}^{s}|C_i|^{-1}f(C_i^{-1})g(D_i)\\
&= \frac{1}{|P|^2}\sum_{i=1}^{s}|C_i|^{-1}f(C_i^{-1})\sum_{j=1}^{r_i}g(D_{ij})\\
&= \frac{1}{|P|^2}\sum_{i=1}^{s}\sum_{j=1}^{r_i}\sum_{(x,y)\in B_{ij}} f\downarrow_P^Q(y,x)g(x,y) = \langle f\downarrow_P^Q, g\rangle_P\,.
\end{aligned}$$

□

The set of integral combinations of irreducible characters of a group forms a ring under Hadamard multiplication. For a general nonempty finite quasigroup Q, the *coefficient ring* $\mathbb{Z}[Q]$ is defined to be the ring

$$\mathbb{Z}[\langle\psi_i\psi_j,\psi_k\rangle_Q \mid 1\le i,j,k\le s\,]\,.$$

The *character ring* $R[Q]$ is then defined to be the ring of $\mathbb{Z}[Q]$-linear combinations of basic characters under Hadamard multiplication. If Q is associative, this agrees with the usual group-theoretic definition [142, 9.1]. If Q is a rank 2 quasigroup, with character table as presented in Figure 6.1, then the relation

$$\psi_2\psi_2 = \psi_1 + (n-2)(n-1)^{-1/2}\psi_2.$$

implies that the coefficient ring $\mathbb{Z}[Q]$ is

$$\mathbb{Z}[(n-1)^{-1/2}] = \mathbb{Z}[X]/\langle(n-1)X^2-1\rangle.$$

Now let P be a nonempty subquasigroup of a finite quasigroup Q. If Q is associative, the induction map $\uparrow_P^Q\colon \mathbb{C}\mathrm{Cl}(P)\to\mathbb{C}\mathrm{Cl}(Q)$ restricts to an abelian group homomorphism $\uparrow_P^Q\colon (R[P],+)\to(R[Q],+)$. If Q is not associative, this need no longer be true. Let P be the Steiner triple system $\mathsf{PG}(1,2)$ embedded in Q, the Steiner triple system $\mathsf{PG}(2,2)$. Then the nontrivial basic character of P induces up to $7\sqrt{3}/9$ times the nontrivial basic character of Q, although $7\sqrt{3}/9$ does not lie in the coefficient ring $\mathbb{Z}[Q]=\mathbb{Z}[6^{-1/2}]$. To study rings of quasigroup characters under induction, it appears to be necessary to admit at least the full ring $\mathbb{A}$ of algebraic numbers as the ring of coefficients. Let $\mathbb{A}\mathrm{Cl}(Q)$ denote the ring of quasigroup class functions on the quasigroup Q taking values in the ring $\mathbb{A}$.

PROPOSITION 7.2
Let Q be a finite, nonempty quasigroup.

(a) *The set Ψ of basic characters of Q forms an $\mathbb{A}$-basis for $\mathbb{A}\mathrm{Cl}(Q)$.*

(b) *The induction map*

$$\uparrow_P^Q : \mathbb{C}\mathrm{Cl}(P) \to \mathbb{C}\mathrm{Cl}(Q)$$

restricts to

$$\uparrow_P^Q : \mathbb{A}\mathrm{Cl}(P) \to \mathbb{A}\mathrm{Cl}(Q)\,.$$

(c) *For class functions f in $\mathbb{A}\mathrm{Cl}(P)$ and g in $\mathbb{A}\mathrm{Cl}(Q)$, one has*

$$f \uparrow_P^Q \cdot g = (f \cdot g \downarrow_P^Q) \uparrow_P^Q \,.$$

(d) *$\mathbb{A}\mathrm{Cl}(P) \uparrow_P^Q$ is an ideal of $\mathbb{A}\mathrm{Cl}(Q)$, and $\mathbb{C}\mathrm{Cl}(P) \uparrow_P^Q$ is an ideal of $\mathbb{C}\mathrm{Cl}(Q)$.*

PROOF (a): For g in $\mathbb{A}\mathrm{Cl}(Q)$, Theorem 6.6 shows that

$$g = \sum_{i=1}^{s} \langle g, \psi_i \rangle \psi_i \,. \tag{7.36}$$

Each coefficient

$$\langle g, \psi_i \rangle = \frac{1}{|Q|} \sum_{(x,y)\in Q^2} g(y,x)\psi_i(x,y) = n^{-1} \sum_{j=1}^{s} \overline{\psi}_{ij} \sum_{(x,y)\in C_j} g(x,y)$$

in (7.36) is an algebraic number.

(b): If f lies in $\mathbb{A}\mathrm{Cl}(P)$, then $f \uparrow_P^Q$ lies in $\mathbb{A}\mathrm{Cl}(Q)$ by (7.33).

(c): For (z,t) in C_i, one has that

$$\begin{aligned}(f^Q \cdot g)(z,t) &= \frac{|Q|^2}{|C_i| \cdot |P|^2} f(B_i) g(z,t) \\ &= \frac{|Q|^2}{|C_i| \cdot |P|^2} \sum_{(x,y)\in B_i} f(x,y) g_P(x,y) = (f \cdot g_P)^Q(z,t)\,.\end{aligned}$$

(d): This follows directly from (c). ∎

A set $\{P_j \mid 1 \le j \le N\}$ of nonempty subquasigroups of a quasigroup Q is said to be *protrusive* if $\bigcup\{P_j^2 \mid 1 \le j \le N\}$ contains a member of each quasigroup conjugacy class C_i of Q (so that some P_j^2 "protrudes" into each C_i). For example, the set of cyclic subgroups of a group is protrusive, since an element $(1,x)$ of C_i is contained in $\langle x \rangle^2$. If Q is associative, Artin's Theorem [142, 9.2] shows that each character of Q is a rational linear combination of characters induced from characters of members of any protrusive set of

subquasigroups of Q. These results do not apply verbatim to nonassociative quasigroups. Taking Q to be the Steiner triple system $\mathsf{PG}(2,2)$, the covering set $\{\langle x\rangle \mid x \in Q\} = \{\{x\} \mid x \in Q\}$ of (1.17), the set of "cyclic" or singly-generated subquasigroups, is not protrusive, since the equality relation $\bigcup\{\{x\}^2 \mid x \in Q\}$ does not intersect the conjugacy class C_2. As for Artin's Theorem, the singleton containing one copy of $\mathsf{PG}(1,2)$ is protrusive. However, denoting the basic characters of this subquasigroup by φ_1 and φ_2, the trivial character of Q is $\varphi_1^Q - (2\sqrt{2}/7)\varphi_2^Q$, while the nontrivial character is $(3\sqrt{3}/7)\varphi_2^Q$, so the characters of Q are not obtained as rational linear combinations of characters induced from characters of the protrusive subquasigroup. The closest analogue of Artin's Theorem holding for general quasigroups appears to be the following.

THEOREM 7.7

Let $\{P_j \mid 1 \le j \le N\}$ be a protrusive set of nonempty subquasigroups of a finite quasigroup Q. Then the direct sum maps

$$\bigoplus_{j=1}^{N} \uparrow_{P_j}^{Q} : \bigoplus_{j=1}^{N} \mathbb{A}\mathrm{Cl}(P_j) \to \mathbb{A}\mathrm{Cl}(Q)$$

and

$$\bigoplus_{j=1}^{N} \uparrow_{P_j}^{Q} : \bigoplus_{j=1}^{N} \mathbb{C}\mathrm{Cl}(P_j) \to \mathbb{C}\mathrm{Cl}(Q)$$

are surjective.

PROOF The algebraic case will be treated: the complex case follows similarly. Since the inner product of algebraic-valued class functions is algebraic, the Frobenius Reciprocity Theorem 7.6 shows that

$$\bigoplus_{j=1}^{N} \downarrow_{P_j}^{Q} : \mathbb{A}\mathrm{Cl}(Q) \to \bigoplus_{j=1}^{N} \mathbb{A}\mathrm{Cl}(P_j)$$

is adjoint to

$$\bigoplus_{j=1}^{N} \uparrow_{P_j}^{Q} : \bigoplus_{j=1}^{N} \mathbb{A}\mathrm{Cl}(P_j) \to \mathbb{A}\mathrm{Cl}(Q)\,.$$

Now $\bigoplus_{j=1}^{N} \downarrow_{P_j}^{Q}$ injects, since a class function restricting to zero on each P_j is zero on each C_i, and hence is zero altogether. It follows that the adjoint map surjects, as required. □

7.5 Linear characters

A basic character ψ_i of Q is said to be *linear* if its degree ψ_{i1} is 1. The significance of linear characters is indicated by the following.

PROPOSITION 7.3
A finite, nonempty quasigroup Q is abelian if and only if all its basic characters are linear.

PROOF If Q is nonempty and abelian, it is an abelian group. Then $\mathbb{C}G \cong \mathbb{C}Q \cong V(G,Q)$, and all the character degrees $\sqrt{\operatorname{Tr} E_i}$ equal 1. Conversely, suppose that $\psi_{i1} = 1$ for $1 \leq i \leq s$. Then by the orthogonality relation (6.32),

$$|Q| = \sum_{i=1}^{s} \psi_{i1}\overline{\psi}_{i1} = s\,.$$

Since there are $s = |Q|$ conjugacy classes, each has order $|Q|$. Thus for each element x of Q, the stabilizer G_x is trivial. By Proposition 3.16, it follows that Q is abelian. □

A general quasigroup Q has a smallest congruence γ or $\gamma(Q)$, its *abelian replica congruence*, for which the quotient Q^γ is abelian (see Appendix B.2). If Q is nonempty, then the abelian group Q^γ has a unique idempotent element, the normal *derived subquasigroup* Q' of Q. The replica Q^γ may be written as the quotient Q/Q', From now on, assume that Q has positive finite order n. Then the order m of Q' divides n. Since Q/Q' is an abelian group, its n/m basic characters $\chi_1, \ldots, \chi_{n/m}$ are all linear. By the Quotient Theorem 7.2, it follows that for $1 \leq i \leq n/m$, the lifts

$$\psi_i = (\operatorname{nat}\gamma)^{\mathsf{ll}}\chi_i : Q^2 \to \mathbb{C}; (x,y) \mapsto \chi_i(x^\gamma, y^\gamma) \tag{7.37}$$

of the basic characters χ_i of Q/Q' are linear basic characters of Q. The following result shows that the set $\Lambda(Q)$ or

$$\Lambda = \{\psi_1, \ldots, \psi_{n/m}\} \tag{7.38}$$

of basic characters (7.37) forms the complete set of linear basic characters of Q.

THEOREM 7.8
For a finite, nonempty quasigroup Q, a basic character is linear if and only if it is the lift of a basic character of the abelian replica Q/Q'.

PROOF Let ψ_i be a linear basic character of Q. It must be shown that ψ_i factors through $(\mathrm{nat}\,\gamma)^{\shortparallel} : Q \times Q \to Q^\gamma \times Q^\gamma$. In other words, let C_j and C_k be quasigroup conjugacy classes for which $C_j(\mathrm{nat}\,\gamma)^{\shortparallel} = C_k(\mathrm{nat}\,\gamma^{\shortparallel}$. It must then be shown that $\psi_{ij} = \psi_{ik}$.

Since ψ_i is linear, the multiplicity f_i is 1, so (6.27) implies that $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q_i$ is commutative. Consider elements p, q, r of Q. Now since the projection $\epsilon_i : \mathbb{C}Q \to \mathbb{C}Q_i$ onto the G-submodule $\mathbb{C}Q_i$ of $\mathbb{C}Q$ is an element of the centralizer ring $V(G, Q)$, one has

$$\begin{aligned}(p\epsilon_i)R(qr)\epsilon_i &= (p \cdot qr)\epsilon_i = qR(r)L(p)\epsilon_i \\ &= q\epsilon_i R(r)L(p) = q\epsilon_i L(p)R(r) \\ &= qL(p)R(r)\epsilon_i = (pq \cdot r)\epsilon_i = (p\epsilon_i)R(q)\epsilon_i R(r)\epsilon_i\,.\end{aligned}$$

Thus the map

$$Q \to Aut_{\mathbb{C}}\mathbb{C}Q_i; q \mapsto R(q)\epsilon_i \tag{7.39}$$

is a quasigroup homomorphism. Since $Aut_{\mathbb{C}}\mathbb{C}Q_i$ is an abelian group, the homomorphism (7.39) factors through the natural projection $\mathrm{nat}\,\gamma$. Thus

$$q^\gamma = r^\gamma \quad \Rightarrow \quad R(q)\epsilon_i = R(r)\epsilon_i\,. \tag{7.40}$$

Fix an element e of Q. Then fix elements q_0 of $C_j(e)$ and r_0 of $C_k(e)$. For all q in $C_j(e)$ and r in $C_k(e)$, one has $q^\gamma = q_0^\gamma = r_0^\gamma = r^\gamma$, so that $(e\backslash q)^\gamma = (e\backslash q_0)^\gamma = (e\backslash r_0)^\gamma = (e\backslash r)^\gamma$. By (6.15),

$$\alpha_j = \sum_{q \in C_j(e)} R(e\backslash e)^{-1} R(e\backslash q)\,.$$

Also, $\alpha_j\epsilon_i = \xi_{ji}\epsilon_i = n_j\psi_{ij}\epsilon_i$. Thus

$$\begin{aligned}\psi_{ij}\epsilon_i &= n_j^{-1}\alpha_j\epsilon_i \\ &= n_j^{-1} \sum_{q \in C_j(e)} R(e\backslash e)^{-1} R(e\backslash q)\epsilon_i \\ &= R(e\backslash e)^{-1} R(e\backslash q_0)\epsilon_i \\ &= R(e\backslash e)^{-1} R(e\backslash r_0)\epsilon_i \\ &= n_k^{-1} \sum_{r \in C_k(e)} R(e\backslash e)^{-1} R(e\backslash r)\epsilon_i \\ &= n_k^{-1}\alpha_k\epsilon_i = \psi_{ik}\epsilon_i\,,\end{aligned}$$

so that $\psi_{ij} = \psi_{ik}$ as required. ∎

COROLLARY 7.3

The number of linear basic characters of Q divides the order of Q.

It will now be shown that the set Λ of linear basic characters of Q carries the structure of an abelian group which acts by Hadamard multiplication on the full set Ψ of characters.

LEMMA 7.4
For φ, χ in $\mathbb{C}\mathrm{Cl}(Q)$ and ψ in Ψ,

$$\langle \varphi\psi, \chi\rangle = \langle \varphi, \overline{\psi}\chi\rangle .$$

PROOF For (x, y) in C_j and $\psi = \psi_i$,

$$\begin{aligned}\psi(x,y) &= \psi_{ij}\\ &= n f_i^{-1/2}\overline{\eta}_{ij}\\ &= n f_i^{-1/2}\eta_{ij^*}\\ &= \overline{\psi}_{ij^*} = \overline{\psi}(y,x)\end{aligned}$$

by Lemma 6.2(c). Then

$$\begin{aligned}|Q|^2\langle \varphi\psi, \chi\rangle &= (\varphi\psi) * \chi(\widehat{Q})\\ &= \sum_{x\in Q}\sum_{y\in Q}\varphi(x,y)\psi(x,y)\chi(y,x)\\ &= \sum_{x\in Q}\sum_{y\in Q}\varphi(x,y)\overline{\psi}(y,x)\chi(y,x)\\ &= \varphi * (\overline{\psi}\chi)(\widehat{Q})\\ &= |Q|^2\langle \varphi, \overline{\psi}\chi\rangle .\end{aligned}$$

□

PROPOSITION 7.4
For a linear basic character λ of Q, Hadamard multiplication by λ gives an isometry of $\mathbb{C}\mathrm{Cl}(Q)$.

PROOF For φ, χ in $\mathbb{C}\mathrm{Cl}(Q)$, use of Lemma 7.4 shows that

$$\langle \varphi\lambda, \chi\lambda\rangle = \langle \varphi, \overline{\lambda}\chi\lambda\rangle = \langle \varphi, \chi\overline{\lambda}\lambda\rangle = \langle \varphi, \chi\rangle .$$

□

Let k be a natural number. Then a basic character ψ of Q is said to *appear with multiplicity k* in a class function χ if $\langle \psi, \chi\rangle = k$, so that k is the coefficient of ψ in the unique expression of χ as a linear combination from Ψ.

THEOREM 7.9
Let Λ or $\Lambda(Q)$ be the set (7.38) of linear basic characters of Q.

(a) *Λ acts as an abelian group on the full set Ψ of basic characters under Hadamard multiplication.*

(b) *In the product of two basic characters, each linear character appears with multiplicity 0 or 1.*

(c) *Fix a linear basic character λ and a general basic character ψ. Then there is a unique basic character χ such that λ appears in $\chi\psi$ with a positive multiplicity. This multiplicity is 1.*

PROOF (a): For $1 \le i, j, k \le s$, the Krein parameter q_{ij}^k [6, Th. 2.3.6(i)] is given as

$$\begin{aligned} q_{ij}^k &= n^{-1} f_i f_j \sum_{l=1}^{s} n_l^{-2} \xi_{li} \xi_{lj} \overline{\xi}_{lk} \\ &= n^{-1} (f_i f_j f_k^{-1})^{1/2} \sum_{l=1}^{s} n \psi_{il} \psi_{jl} \overline{\psi}_{kl} \\ &= (f_i f_j f_k^{-1})^{1/2} n^{-2} \sum_{x \in Q} \sum_{y \in Q} \psi_i(x,y) \psi_j(x,y) \psi_k(y,x) \\ &= (f_i f_j f_k^{-1})^{1/2} \langle \psi_i \psi_j, \psi_k \rangle \,. \end{aligned}$$

By the Krein condition [6, Th. 2.3.8], q_{ij}^k is real and nonnegative. Then

$$\langle \psi_i \psi_j, \psi_k \rangle \ge 0 \,. \tag{7.41}$$

Now suppose that ψ_i is a linear basic character of Q. By Proposition 7.4, the matrix of Hadamard multiplication by ψ_i with respect to the orthonormal basis Ψ is orthogonal. By (7.41), the coefficients of this matrix are nonnegative. But an orthogonal matrix with nonnegative entries is a permutation matrix, so Hadamard multiplication by ψ_i permutes the elements of Ψ.

(b): Let the two basic characters be ψ_j and ψ_k. Let ψ_i again be linear. Then by Lemma 7.4, $\langle \psi_i, \psi_j \psi_k \rangle = \langle \psi_i \overline{\psi}_j, \psi_k \rangle = \langle \psi_i \psi_{j^*}, \psi_k \rangle$. By (a) and the orthonormality of Ψ, these products take the value 0, unless ψ_{j^*} is permuted under Hadamard multiplication by ψ_i to ψ_k, in which case the products take the value 1.

(c): By Lemma 7.4, $\langle \lambda, \chi\psi \rangle = \langle \lambda\overline{\chi}, \psi \rangle = \langle \overline{\chi}, \overline{\lambda}\psi \rangle$. This product takes a nonzero value, namely 1, if and only if $\overline{\chi} = \overline{\lambda}\psi$, i.e., if and only if $\chi = \lambda\overline{\psi}$. □

As shown by the following results, linear characters often play a key role in relating the structure and character tables of certain quasigroups.

THEOREM 7.10

Let Q be a quasigroup of finite order $n > 2$. Then the following conditions on Q are equivalent:

(a) *Q has a unique nonlinear basic character, the square of which is the sum of all the linear characters of Q;*

(b) *The character table $\Psi(Q)$ of Q has the form*

Q	C_1	C_2	C_3	$\dots$	C_s
ψ_1	1	1	1	$\dots$	1
$\vdots$	$\vdots$	$\vdots$	$\Psi(Q/Q')$		$\vdots$
$\psi_{n/2}$	1	1		$\dots$	
ψ_s	$\sqrt{n/2}$	$-\sqrt{n/2}$	0	$\dots$	0

(c) *On Q, the abelian replica congruence $\gamma(Q)$ and stability congruence $\sigma(Q)$ coincide, each having order $2n$.*

PROOF (a) $\Rightarrow$ (b): Let ψ_s be the unique nonlinear character of Q, so that $\psi_1, \dots, \psi_{s-1}$ form the complete set $\Lambda(Q)$ of linear characters of Q. By assumption, $\psi_s^2 = \psi_1 + \cdots + \psi_{s-1}$. Then

$$\begin{aligned} n &= \psi_{11}^2 + \cdots + \psi_{(s-1)1}^2 + \psi_{s1}^2 \\ &= (s-1) + \psi_{11} + \cdots + \psi_{(s-1)1} = 2(s-1)\,, \end{aligned}$$

whence $\psi_{s1}^2 = s - 1 = n/2$. Since there are $n/2$ linear characters, Theorem 7.8 shows that $|Q/Q'| = n/2$. Let $C_3, \dots, C_s$ respectively contain representatives for each of the $s-2$ γ-classes distinct from Q'. By the orthogonality of later columns to the first in the character table $\Psi(Q/Q')$ of Q/Q', the sums

$$\psi_{si}^2 = \psi_{1i} + \cdots + \psi_{(s-1),i}$$

are zero for $3 \le i \le s$, whence $\psi_{si} = 0$. This completes all but the second column of the character table $\Psi(Q)$ of Q. The second column may then be completed using the orthogonality of the final row to the first row in this table.

(b) $\Rightarrow$ (c): If $\Psi(Q)$ is as shown in (b), then by Theorem 7.8 $|Q/Q'| = n/2$, whence $|Q'| = 2$ and $|\gamma| = 2n$. Use of Corollary 6.4(b) (p. 156) on $\Psi(Q)$ yields $n_1 = n_2 = 1$ and $n_3 = \cdots = n_s = 2$. Proposition 6.2 (p. 157) now shows that $\sigma(Q) = C_1 \cup C_2 = \gamma(Q)$.

(c) $\Rightarrow$ (a): Suppose $|\gamma(Q)| = |\sigma(Q)| = 2n$. Since $|Q'| = 2$, there are precisely $n/2$ linear basic characters by Theorem 7.8. By Proposition 6.2, without loss of generality one has $n_1 = n_2 = 1$ and $n_i > 1$ for $i > 2$. (Since $n > 2$, there are conjugacy classes other than C_1 and C_2.) For $i > 2$, Corollary 6.4(b) gives

$$2 \le n_i \le n \Big/ \sum_{k=1}^{s} |\psi_{ki}|^2 \le n \Big/ \sum_{k=1}^{n/2} |\psi_{ki}|^2 = 2\,,$$

whence equality holds throughout, and $\psi_{ki} = 0$ for $k > n/2$. The orthogonality relation (6.33) yields

$$|\psi_{s1}|^2 + |\psi_{s2}|^2 = n$$

on setting $i = j = s$, and

$$\psi_{s1} + \psi_{s2} = 0$$

on setting $i = s$, $j = 1$. Thus $\psi_{s1} = \sqrt{n/2}$, and ψ_s is the unique nonlinear basic character, the square of which is the sum of all the linear basic characters. □

The quaternion group and octonion loop (compare Exercise 19 in Chapter 1) both satisfy the conditions of Theorem 7.10. Another example is furnished by Parker's Moufang loop used in Conway's construction of the Fischer-Griess monster group [32]. For an immediate example, see Section 9.8 below.

There is a more general (and correspondingly weaker) version of Theorem 7.10.

THEOREM 7.11

Let Q be a quasigroup of positive finite order n, with derived subquasigroup Q' of order m. Suppose that Q has a unique nonlinear basic character.

(a) *The character table $\Psi(Q)$ of Q has the form*

Q	C_1	C_2	C_3	$\dots$	$C_{1+n/m}$
ψ_1	1	1	1	$\dots$	1
$\vdots$	$\vdots$	$\vdots$	$\Psi(Q/Q')$		$\vdots$
$\psi_{n/m}$	1	1		$\dots$	
$\psi_{1+n/m}$	$\sqrt{\frac{n(m-1)}{m}}$	$-\sqrt{\frac{n}{m(m-1)}}$	0	$\dots$	0

(b) *Q is subdirectly irreducible.*

(c) *Q has an integral coefficient ring if and only if one of the following (mutually exclusive) conditions holds:*

(i) *Q satisfies the conditions of Theorem 7.10;*

(ii) *The Diophantine equation*

$$p^2m(m-1) = n(m-2)^2 \tag{7.42}$$

has a positive integral solution p.

PROOF By Theorem 7.9(c),

$$\psi_s^2 = \psi_1 + \cdots + \psi_{n/m} + \alpha\psi_s \tag{7.43}$$

for a certain coefficient α, making $\mathbb{Z}[\alpha]$ the coefficient ring of Q. Applying (7.43) to C_1 gives

$$\alpha = (m-2)(n/m)^{1/2}(m-1)^{-1/2}\,.$$

If $\mathbb{Z}[\alpha] = \mathbb{Z}$, then either $\alpha = 0$ and the conditions of Theorem 7.10 apply, or else α is a positive integer, in which case (7.42) has a solution. Conversely, if (7.42) has a solution, then α is integral and $m > 2$. On the other hand, condition (a) of Theorem 7.10 makes $\alpha = 0$ and $\mathbb{Z}[\alpha] = \mathbb{Z}$. This completes the proof of (c). The form (a) of the character table follows on filling in $\Psi(Q/Q')$ as shown, making $\gamma = C_1 \cup C_2$, and completing ψ_s with the orthogonality for columns of $\Psi(Q)$. By Theorem 7.1, the congruence lattice of Q is the ordinal sum of the singleton $\{\widehat{Q}\}$ and a copy of the congruence lattice of Q/Q'. The copy of the trivial congruence on Q/Q' becomes γ. Thus Q, having γ as a socle, is subdirectly irreducible. □

7.6 Exercises

1. Give an example of two principally isotopic quasigroup structures $(Q,\cdot)$ and $(Q,+)$ on a set Q such that the multiplication groups $\mathrm{Mlt}(Q,\cdot)$ and $\mathrm{Mlt}(Q,+)$ are incomparable.

2. (a) Show that the $(\mathbb{Z}/5\mathbb{Z},-,0)$-fusion of $(\mathbb{Z}/5\mathbb{Z},+,0)$ pique classes is $\{\{0\},\{\pm1\},\{\pm2\}\}$.

   (b) Use condition (7.28) to fix the $(\mathbb{Z}/5\mathbb{Z},-)$-fusion of $(\mathbb{Z}/5\mathbb{Z},+)$ pique characters.

   (c) Show that the character table of $(\mathbb{Z}/5\mathbb{Z},-)$ is

$$\begin{bmatrix} 1 & 1 & 1 \\ \sqrt{2} & \sqrt{2}\cos(2\pi/5) & -\sqrt{2}\cos(\pi/5) \\ \sqrt{2} & -\sqrt{2}\cos(\pi/5) & \sqrt{2}\cos(2\pi/5) \end{bmatrix} \tag{7.44}$$

(d) Use Theorem 3.10 (p. 81) to show that loops of prime order are either abelian or have rank 2.

(e) Conclude that (7.44) is a quasigroup character table which is not a loop character table.

(f) Show that (7.44) is the character table of any nonabelian quasigroup of order 5 that is not a rank 2 quasigroup.

3. Consider the loop $(Q, \cdot, 0)$ with multiplication table:

	0	3	4	1	2	5
0	0	3	4	1	2	5
3	3	0	1	4	5	2
4	4	1	2	5	0	3
1	1	4	5	2	3	0
2	2	5	0	3	1	4
5	5	2	3	0	4	1

[The table is obtained from the table for the integers $(Q, +) = (\mathbb{Z}/6\mathbb{Z}, +)$ modulo 6 under addition by interchanging the columns of the 2×2 square whose rows and columns are indexed by 2 and 5.]

(a) Show that the center of $(Q, \cdot, 0)$ is $\{0, 3\}$.

(b) Show that the loop conjugacy classes of $(Q, \cdot, 0)$ are $\{0\}$, $\{3\}$, $\{1, 4\}$, and $\{2, 5\}$.

(c) Show that the quotient of $(Q, \cdot, 0)$ by its center is the cyclic group of order 3.

(d) Use the Quotient Theorem 7.2 to compute the first three basic characters ψ_1, ψ_2, ψ_3 of the loop $(Q, \cdot, 0)$.

(e) Use the orthogonality relations to compute the fourth basic character ψ_4 of $(Q, \cdot, 0)$.

(f) Using $0 \le j \le 5$ to label the row corresponding to the group character $k \mapsto \exp(2\pi ijk/6)$, show that the character table of $(Q, +)$, partitioned according to the $(Q, \cdot)$-fusion, is

	0	3	4	1	2	5
0	1	1	1	1	1	1
2	1	1	ω	ω	ω^2	ω^2
4	1	1	ω^2	ω^2	ω	ω
1	1	-1	ω^2	$-\omega^2$	ω	$-\omega$
3	1	-1	1	-1	1	-1
5	1	-1	ω	$-\omega$	ω^2	$-\omega^2$

(g) Use (7.27) to compute the fourth basic character ψ_4 of $(Q, \cdot, 0)$.

4. [92] Let P be a subgroup of a finite group Q. If g is a group class function on P, the induced group class function g^Q on Q is defined by the formula

$$g^Q(s) = \frac{1}{|P|} \sum_{u \in Q, u^{-1}su \in P} g(u^{-1}su) \tag{7.45}$$

for s in Q (compare [142, 7.2]). Defining a quasigroup class function f on P by $f(x, y) = g(x\backslash y)$, show that $f^Q(z, t) = g^Q(z\backslash t)$ for z, t in Q.

5. [92] Let N be a nonempty subquasigroup of a subquasigroup P of a finite quasigroup Q. Let f be a class function on N. Prove the *transitivity of induction*, namely $f \uparrow_N^P \uparrow_P^Q = f \uparrow_N^Q$.

6. [150] Let Q be a finite quasigroup with congruence class partition Γ.

   (a) Set $\Omega = Q \times Q$, and let

   $$\mu : 2^\Omega \to [0, 1]; A \mapsto \frac{|A|}{|Q \times Q|}$$

   be the normalized counting measure on Ω. Let F be the smallest Boolean subalgebra or σ-field of 2^Ω containing Γ. Show that the complex F-measurable random variables on the measure space $(\Omega, 2^\Omega, \mu)$ are precisely the quasigroup class functions on Q.

   (b) For a function $f : P \times P \to \mathbb{C}$ on the square of a nonempty subquasigroup P of Q, define a random variable $X_f : \Omega \to \mathbb{C}$ by

   $$X_f(x, y) = \begin{cases} f(x, y) \cdot |Q^2|/|P^2|, & (x, y) \in P \times P\,; \\ 0, & (x, y) \notin P \times P\,. \end{cases}$$

   If f is a quasigroup class function on P, show that the induced class function $f \uparrow_P^Q$ is the conditional expectation $E(X_f|F)$.

   (c) Derive Proposition 7.2(d) from the relation $E(XY|F) = XE(Y|F)$ for an F-measurable random variable X [14, Th.34.2].

   (d) Derive the transitivity of induction (Exercise 5) from the relation $E(E(X|F_2)|F_1) = E(X|F_1)$ for nested σ-subfields $F_1 \subseteq F_2$ [14, Th. 34.4].

7. Let Q be an abelian group. Let T be the quotient of the abelian group $(\mathbb{R}, +, 0)$ of reals by the subgroup $\mathbb{Z}$ of integers. Recall that a *character* κ of Q is a group homomorphism $\kappa : Q \to T$. Let Q^* be the set of characters of Q.

   (a) Define the sum $\kappa + \kappa'$ of two characters κ and κ' by

   $$q(\kappa + \kappa') = q\kappa + q\kappa' \tag{7.46}$$

   for q in Q. Show that the sum of two characters is a character.

(b) Show that the set Q^* of characters forms an abelian group under the operation (7.46).

(c) Show that the identity element of the group Q^* is formed by the *trivial character* with constant value $\mathbb{Z}$.

(d) If Q is finite, consider the abelian group Q^* as given by (b) above, and the abelian group $\Lambda(Q)$ of linear basic characters of Q given by Theorem 7.9(a). Show that Q^* and $\Lambda(Q)$ are isomorphic.

8. For a finite nonempty quasigroup Q, show that the abelian group $\Lambda(Q)$ of linear basic characters of Q is isomorphic to the abelian group replica Q/Q' of Q.

9. Let Q be a central pique with inner multiplication group I. Let J be the augmentation ideal of the integral group algebra $\mathbb{Z}I$ of I, namely the ideal of $\mathbb{Z}I$ generated by the set $\{h - 1 \mid h \in I\}$. Show that the derived subquasigroup Q' of Q is the submodule QJ of the $\mathbb{Z}I$-module Q. [Compare the proof of Theorem 3.9 (p. 79).]

10. [163] Let Q be a finite central pique with pointed idempotent e and inner multiplication group I. Let Q^* be the group of characters of the abelian cloop $(Q, +, e)$ of Q (compare Exercise 7 above).

(a) Show that the specification

$$q(\alpha\kappa) = (q\alpha)\kappa$$

(for $q \in Q$, $\alpha \in I$, $\kappa \in Q^*$) yields a left action of I on Q^*.

(b) Show that Q^* forms a central pique under the operation

$$\kappa \cdot \lambda = R\kappa + L\lambda$$

with the trivial character ϵ as the pointed idempotent.

(c) Show that I is the inner multiplication group of the pique Q^*.

(d) Show that Q and Q^* have the same number s of pique conjugacy classes.

(e) Let $D_1, \ldots, D_s$ be the pique conjugacy classes of Q, and let $\Delta_1, \ldots, \Delta_s$ be the pique conjugacy classes of Q^*. Show that the character table $\Psi(Q)$ of Q is given by

$$\psi_{ij} = \frac{1}{n_j\sqrt{f_i}} \sum_{q \in D_j} \sum_{\kappa \in \Delta_i} q\kappa$$

for $1 \leq i, j \leq s$.

11. Show that Lemma 7.4 does not extend to the more general case of ψ in $\mathbb{C}\mathrm{Cl}(Q)$.

12. Exhibit the full character tables of the quaternion group and octonion loop.

13. Show that the hypotheses of Theorem 7.10 are satisfied by the dihedral group D_4.

14. Show that a group satisfies the hypotheses of Theorem 7.10 if and only if it is an extraspecial 2-group (compare [4, §23] or [83, III §13]).

15. Show that each code loop (compare Exercise 20 in Chapter 2) satisfies the hypotheses of Theorem 7.10.

16. (a) Show that the hypotheses of Theorem 7.11 are satisfied by the symmetric group S_3.
    (b) Show that the hypotheses of Theorem 7.10 are not satisfied by the symmetric group S_3.
    (c) Recalling that groups always have an integral coefficient ring, determine which of the two alternatives of Theorem 7.11(c) holds for the symmetric group S_3.

17. Define the *characteristic entropy* of a finite, nonempty quasigroup Q to be the quantity
$$\sum_{j=1}^{s} \frac{f_j}{n} \log \frac{n}{f_j} .$$
    (a) Use Proposition 7.3 to show that the analogue of Theorem 6.9 (p.160) holds for the characteristic entropy.
    (b) Conclude that for finite, nonempty abelian and rank 2 quasigroups, the conjugate entropy and characteristic entropy agree.

18. Let Q be a finite, nonempty quasigroup with character table Ψ. Show that the characteristic entropy of Q is given by
$$\log \Big(\sum_{i=1}^{s} |\psi_{i1}|^2 \Big) - \sum_{i=1}^{s} |\psi_{i1}|^2 \log |\psi_{i1}|^2 .$$

19. Let Q be a finite, nonempty central quasigroup. Show that the conjugate entropy and characteristic entropy of Q agree.

20. Use Theorem 7.10 to construct a series of finite quasigroups Q for which the ratio of the conjugate entropy to the characteristic entropy may be made arbitrarily close to 2.

21. Can you use Theorem 7.11 to construct a series of finite quasigroups Q for which the ratio of the conjugate entropy to the characteristic entropy may be made arbitrarily large?

7.7 Problems

1. Determine those varieties **J** of quasigroups with the property that each finite nonempty member Q of **J** has an integral coefficient ring $\mathbb{Z}[Q]$.

2. To what extent could the characteristic entropy of a finite, nonempty quasigroup exceed its conjugate entropy? (Compare Exercise 21.)

3. (Compare Problem 2 in Chapter 6.) Let n be the order of a finite simple group. Is there a simple group S of order n such that the characteristic entropy of S is no greater than the characteristic entropy of Q for all groups Q of order n?

7.8 Notes

Section 7.1

Theorem 7.1 first appeared in [91, Th. 3.6], [148, 545]. Its proof relies on the idea of [25, Prop. 3.1].

Section 7.2

The material of this section, including the Quotient Theorem 7.2 first appeared in [93].

Section 7.3

The material of this section, including the Fusion Theorem 7.3 and the Magic Rectangle Condition, first appeared in [93].

Section 7.4

The material of this section first appeared in [92] and [148].

Section 7.5

The material of this section first appeared in [95].

Chapter 8

SCHEMES AND SUPERSCHEMES

The previous chapter covered those more advanced parts of combinatorial character theory that extend the character theory of groups. The background for the current chapter is the theory of association schemes, examining some topics in quasigroup character theory that do not have close counterparts in group character theory. Section 8.2 considers more "no-go theorems" in the spirit of Section 3.9, this time asking for examples of association schemes and scheme character tables that cannot arise from a finite quasigroup. The theorems rely on the concept of sharp transitivity discussed in Section 8.1. Sharp transitivity gives an intrinsic, local characterization of (unnormalized) loop transversals.

The remainder of the chapter is motivated by the facts that the character table Ψ of a general finite quasigroup Q does not determine the character table of $Q \times Q$, and in particular that the tensor square $\Psi \otimes \Psi$ is not the character table of $Q \times Q$. Section 8.3 introduces superschemes, which extend association schemes from binary relations on Q to relations of arbitrary finite length. Section 8.4 introduces the corresponding Bose-Mesner superalgebras, which are graded analogues of the Bose-Mesner algebra of an association scheme. Section 8.5 then interprets the tensor square $\Psi \otimes \Psi$ of a quasigroup character table Ψ within the context of superalgebras. The final two sections show how the superscheme of a finite quasigroup Q, and more especially its superalgebra, encode enough information to enable one to reconstruct the multiplication group G of Q along with its permutation action on Q.

8.1 Sharp transitivity

DEFINITION 8.1 *Let S be a set of permutations on a set Q. Then S is said to be* sharply transitive *if Q and S are empty, or otherwise if there is a function*

$$\sigma : Q \times Q \to S; (q, r) \mapsto \sigma(q, r)$$

such that, for each element (q, r) of $Q \times Q$, the permutation $\sigma(q, r)$ is the unique element of S with $q\sigma(q, r) = r$.

PROPOSITION 8.1
Let G be the multiplication group of a quasigroup Q. Then the set

$$R(Q) = \{R(x) \mid x \in Q\}$$

of right multiplications is a sharply transitive subset of G.

PROOF The sharp transitivity of the subset $R(Q)$, with

$$\sigma : Q \times Q \to S; (q, r) \mapsto R(q\backslash r)\,,$$

follows directly from the combinatorial definition of a quasigroup. □

COROLLARY 8.1
Let e be an element of a quasigroup Q with multiplication group G. Then the loop transversal

$$\{\rho(e, q) \mid q \in Q\}$$

of (2.29) *is a sharply transitive subset of G.*

PROOF The subset (2.29) of G is the set of right multiplications in the loop structure (2.30) on Q. □

REMARK 8.1 The converse of Proposition 8.1 is false: The existence of a sharply transitive subset of a permutation group does not imply that the action is the multiplication group action of a quasigroup. For a simple example, consider the right regular permutation representation of a nonabelian group. (Compare Exercise 2.) Some more subtle examples are considered in Section 8.2 below. □

Sharply transitive sets have a graph-theoretical characterization. If G is a group of permutations on a finite set Q, two permutations g and h are said to be *compatible* precisely when $qg \neq qh$ for all q in Q. In other words, the quotient g/h has no fixed points. Thus two permutations are compatible if they could potentially appear together in a sharply transitive set. One then defines the *compatibility graph* of G on Q as the undirected graph on the vertex set G in which an edge joins two permutations if and only if they are compatible. Sharply transitive subsets of G correspond to the $|Q|$-cliques in the compatibility graph, sets of vertices of size $|Q|$ inducing a complete subgraph.

Figure 8.1 displays the compatibility graph of the symmetric group S_3 in its natural action on the set $\{1, 2, 3\}$. As illustrations of Proposition 8.1, the clique on the right represents the right multiplications in the 3-element idempotent quasigroup, while the clique on the left represents all the right multiplications in the 3-element abelian group under subtraction.

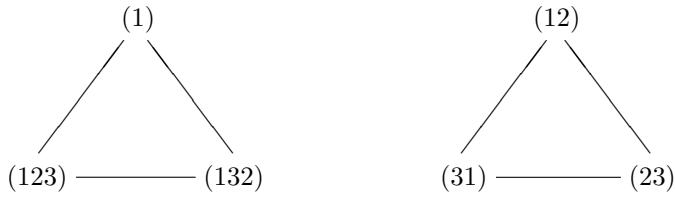


FIGURE 8.1: The compatibility graph of S_3.

PROPOSITION 8.2

Let G be a group of permutations of a finite set Q. Then the multiplication group $\mathrm{Mlt}\, G$ *of the group G is a group of automorphisms of the compatibility graph of G on Q.*

PROOF Let g_1, g_2 be a pair of elements of G. For an element g of G, one has

$$\begin{aligned} & \forall\, q \in Q\,,\ qgg_1 \neq qgg_2 \\ \Leftrightarrow\ & \forall\, q \in Q\,,\ qg_1 \neq qg_2 \\ \Leftrightarrow\ & \forall\, q \in Q\,,\ qg_1g \neq qg_2g\,. \end{aligned}$$

Thus the following three statements are equivalent:

(a) $\{g_1, g_2\}L(g)$ is an edge of the compatibility graph;

(b) $\{g_1, g_2\}$ is an edge of the compatibility graph;

(c) $\{g_1, g_2\}R(g)$ is an edge of the compatibility graph.

The claim of the proposition follows. □

As an illustration of Proposition 8.2, note that the conjugations in the group S_3 permute the elements within the 3-cliques of the compatibility graph displayed in Figure 8.1, while multiplication (on the left or the right) by a transposition interchanges the cliques.

COROLLARY 8.2

Let γ be an element of $\mathrm{Mlt}\, G$*, and let S be a subset of G. Then S is sharply transitive if and only if $S\gamma$ is sharply transitive.*

8.2 More no-go theorems

The no-go theorems of Section 3.9 exhibited abstract groups that could not be multiplication groups of quasigroups, or permutation actions that could not be multiplication group actions on a quasigroup. The goal of this section is to exhibit association schemes which cannot be the association scheme of a quasigroup, and association scheme character tables, like table (8.2) below, which cannot be quasigroup character tables. The main tool to be used is sharp transitivity. Its crudest application produces schemes or tables which cannot come from a multiplicity-free permutation group containing any sharply transitive subset.

PROPOSITION 8.3
For integral $r > 2$, let $X^{[2]}$ denote the set of 2-element subsets of an r-element set X. Let S_r be the symmetric group on X. Let $S_r^{[2]}$ denote the image of S_r under the monomorphic permutation representation

$$S_r \to X^{[2]}!; g \mapsto \left(g^{[2]} : \{x, y\} \mapsto \{xg, yg\}\right)$$

of S_r on $X^{[2]}$. Then if r is even, the permutation group $S_r^{[2]}$ contains no sharply transitive subset.

PROOF Let T be a set of permutations of X such that $T^{[2]} = \{t^{[2]} \mid t \in T\}$ is a compatible subset of the permutation group $S_r^{[2]}$. For even r, it will be shown that $|T| < |X^{[2]}|$, so that $T^{[2]}$ cannot be a sharply transitive subset of the permutation group $S_r^{[2]}$.

For elements x, y of X, set

$$T_x^y = \{t \in T \mid xt = y\}.$$

Let a, c, d be distinct elements of X. Consider the functions

$$\delta : T_a^c \to X \setminus \{a\}; t \mapsto dt^{-1}$$

and

$$\gamma : T_a^d \to X \setminus \{a\}; t \mapsto ct^{-1}.$$

Note that the union $T_a^c \cup T_a^d$ is disjoint. Let

$$\beta : T_a^c \cup T_a^d \to X \setminus \{a\}$$

be the disjoint union of the functions δ and γ. Then

$$\{a, t\beta\}t^{[2]} = \{c, d\}$$

for all t in $T_a^c \cup T_a^d$. Now the function β is injective. Indeed, suppose $t_1\beta = t_2\beta$. Then

$$\{a, t_1\beta\}t_1^{[2]} = \{c, d\} = \{a, t_2\beta\}t_2^{[2]} = \{a, t_1\beta\}t_2^{[2]}\,,$$

whence $t_1^{[2]} = t_2^{[2]}$ or $t_1 = t_2$ follows by the compatibility of $T^{[2]}$. Thus

$$|T_a^c| + |T_a^d| \le r - 1\,. \tag{8.1}$$

Set $m = \max\left\{|T_a^x| \,\middle|\, x \in X\right\}$.

Case (a): $m \ge r/2$.
In this case (8.1) shows that there is a unique element y of X such that $|T_a^y| = m$. For $y \ne x \in X$, one has $|T_a^x| \le r - 1 - m$. Thus

$$|T| = \sum_{z \in X} T_a^z \le m + (r-1)(r-1-m) = (r-1)^2 - (r-2)m\,.$$

Now $m \ge r/2$, so

$$|T| \le (r-1)^2 - (r-2)\frac{r}{2} < |X^{[2]}|\,,$$

completing the proof for this case.

Case (b): $m < r/2$.
Here $m \le (r-2)/2$, so

$$|T| \le (r-1)m \le \frac{(r-1)(r-2)}{2} < |X^{[2]}|\,,$$

completing the proof in this case as well. □

The permutation representation of $S_r^{[2]}$ on $X^{[2]}$ is multiplicity-free, so the orbits of the diagonal action of $S_r^{[2]}$ on $X^{[2]} \times X^{[2]}$ give an association scheme, the *Johnson scheme* $J(r, 2)$ [6, III.2] [37, §4.2] or "triangular" association scheme [17], [145]. The character tables of these schemes may be computed from the Eberlein polynomials [6, Th. III.2.10], [37, Th. 4.6]. For example,

$$\begin{bmatrix} 1 & 1 & 1 \\ \sqrt{7} & \frac{1}{3}\sqrt{7} & -\frac{1}{3}\sqrt{7} \\ 2\sqrt{5} & -\frac{1}{3}\sqrt{5} & \frac{2}{15}\sqrt{5} \end{bmatrix} \tag{8.2}$$

is the character table for the scheme $J(8, 2)$.

THEOREM 8.1

Let r be an even integer greater than 4. Then the character table of the Johnson scheme $J(r, 2)$ is not a quasigroup character table.

PROOF Suppose that Q is a quasigroup whose character table is the character table of the scheme $J(r,2)$, for even r greater than 4. Let G be the multiplication group of Q, and let (Q,Γ) be the association scheme given by the orbits of G on $Q \times Q$. For the values of r under consideration, the Johnson scheme $J(r,2)$ is uniquely determined by its character table unless $r = 8$ [31] [145] [171]. If $r = 8$, there are three exceptional association schemes with the same character table. They are described in [174, pp. 184–185]. Their relations are distance relations in strongly regular graphs. However, the automorphism groups of these graphs are not transitive on the 28 vertices: one has an orbit of length 8, while the other two have orbits of length 4. Since the transitive group G is a subgroup of the group of automorphisms of the relational structure (Q,Γ), it follows that (Q,Γ) cannot coincide with any of these exceptional schemes. Thus (Q,Γ) coincides with the Johnson scheme $J(r,2)$ in each case.

Now by the hypothesis on r, the permutation representation $S_r^{[2]}$ is 2-closed [100, p. 134], so the permutation representation of G on Q is similar to the permutation representation of a subgroup H of $S_r^{[2]}$. By Proposition 8.1, G contains a sharply transitive subset. By the similarity, the subgroup H of $S_2^{[2]}$ would also contain a sharply transitive subset. But this contradicts Proposition 8.3. □

A more refined use of sharp transitivity in proving no-go theorems considers multiplicity-free permutation group actions which may well contain sharply transitive subsets, but where none of them can be a loop transversal of the form given by Corollary 8.1. Let F be a field of odd prime power order r. Let F^* denote the cyclic group of nonzero elements of F. Let L_r denote the group

$$\{\mathsf{F} \to \mathsf{F}; x \mapsto mx + c \mid m \in \mathsf{F}^*, c \in \mathsf{F}\}$$

of linear permutation polynomial actions on F. Let $L_r^{[2]}$ denote the corresponding subgroup of the permutation group $S_r^{[2]}$ of Proposition 8.3, taking $X = \mathsf{F}$. The following theorem classifies the sharply transitive subsets of $L_r^{[2]}$.

THEOREM 8.2

(a) *Let T be a transversal to $\{\pm 1\}$ in F^*. Then*

$$S = S(T) = \{x \mapsto tx + c \mid t \in T, c \in \mathsf{F}\} \tag{8.3}$$

is a sharply transitive subset of the permutation group $L_r^{[2]}$ on the set $\mathsf{F}^{[2]}$ of 2-element subsets of F.

(b) *Conversely, each sharply transitive subset S of $L_r^{[2]}$ is of the form $S = S(T)$ for some transversal T to $\{\pm 1\}$ in F^*. In particular, there are $2^{(r-1)/2}$ distinct sharply transitive subsets of $L_r^{[2]}$.*

PROOF Define the *moment map*

$$\mathsf{F}^{[2]} \to \mathsf{F} \times \mathsf{F}^{*2}; \{a, b\} \mapsto \left(\frac{1}{2}(a+b), \frac{1}{4}(a-b)^2\right).$$

The moment map bijects, having

$$\mathsf{F} \times \mathsf{F}^{*2} \to \mathsf{F}^{[2]}; (\mu, \sigma^2) \mapsto \{\mu - \sigma, \mu + \sigma\}$$

as its two-sided inverse. Intuitively one may regard $\{a, b\}$ as a probability distribution on F, assigning weight $\frac{1}{2}$ to each of a and b. The element μ is then considered as the mean of the distribution, while σ^2 is its variance. Rather than studying the action of $L_r^{[2]}$ on $\mathsf{F}^{[2]}$, it is computationally more convenient to study the action of $L_r^{[2]}$ on $\mathsf{F} \times \mathsf{F}^{*2}$. These actions are similar via the moment map and its inverse. In particular, a familiar calculation from elementary probability theory shows that an element

$$x \mapsto mx + c$$

of $L_r^{[2]}$ acts on $\mathsf{F} \times \mathsf{F}^{*2}$ as

$$(\mu, \sigma^2) \mapsto (m\mu + c, m^2\sigma^2). \tag{8.4}$$

Now suppose that T and $S(T)$ are given as in (8.3). For an ordered pair $\big((\mu, \sigma^2), (\nu, \tau^2)\big)$ of elements of $\mathsf{F} \times \mathsf{F}^{*2}$, there is a unique element $x \mapsto tx + c$ of $S(T)$ taking (μ, σ^2) to (ν, τ^2). By the second component of (8.4), one must have $t^2\sigma^2 = \tau^2$, whence t is determined as the unique element of T which squares to τ^2/σ^2. The first component of (8.4) then yields the equation $t\mu + c = \nu$, having the unique solution $c = \nu - t\mu$. This shows that the subsets $S(T)$ are sharply transitive, as claimed.

Conversely, suppose given a sharply transitive subset S of $L_r^{[2]}$. Now (8.4) specializes to

$$(0, 1) \mapsto (c, m^2).$$

As $x \mapsto mx + c$ ranges through the $r(r-1)/2$ elements of S, the pair (c, m^2) must range over the $r(r-1)/2$ elements of $\mathsf{F} \times \mathsf{F}^{*2}$, It thus remains to check that $f : x \mapsto mx + c$ and $g : x \mapsto -mx + d$ cannot both lie in S. Write $f : x \mapsto m(x - a)$ and $g : x \mapsto m(b - x)$. Then f and g both map $\left(\frac{1}{2}(a+b), 1\right)$ in $\mathsf{F} \times \mathsf{F}^{*2}$ to $\left(\frac{1}{2}m(b-a), m^2\right)$, a contradiction to the sharp transitivity. □

PROPOSITION 8.4

Let $r > 3$ be an odd prime power. Let $(Q, \cdot)$ be a quasigroup structure on the set $\mathsf{F}^{[2]}$ with the character table of the Johnson scheme $J(r, 2)$. Then for no element e of Q can the sharply transitive set $\{\rho(e, y) \mid y \in Q\}$ be of the form $S(T)$ as in (8.3).

PROOF For the values of r being considered, the Johnson scheme $J(r,2)$ is uniquely determined by its character table [31], [145], [171]. Thus the nondiagonal orbits of the multiplication group G of $(Q,\cdot)$ on Q^2 are

$$C_2 = \{(A,B) \mid 1 = |A \cap B|\}$$

and

$$C_3 = \{(A,B) \mid \varnothing = A \cap B\}\,.$$

Suppose that for some e in Q, the set $S = \{\rho(e,y) \mid y \in Q\}$ is of the form $S(T)$. Corollary 8.2 shows that without loss of generality one may take $e = \{\pm 1\}$. In F^* one has $T \cap \{\pm 1\} = 1$, since $\rho(e,e) = 1$.

Let $(Q,+_e,e)$ be the loop with $x +_e y = x\rho(e,y)$ for x,y in Q. Recall the isomorphism

$$(Q,+_e,e) \to (S,*,1); y \mapsto \rho(e,y) \tag{8.5}$$

from $(Q,+_e,e)$ to the loop defined by the loop transversal S. By Section 7.3, the scheme of the quasigroup $(Q,\cdot)$ is obtained by fusion from the scheme of the loop $(Q,+_e,e)$. Thus the $(Q,\cdot)$-classes C_2 and C_3 are obtained as unions of $(Q,+_e)$-classes.

For a nonzero element a of F, define $\overline{a}$ in T by $a \in \{\pm 1\}\overline{a}$. Consider an element $ax+b$ of L_r. Its representative in $S = S(T)$ is

$$\overline{ax+b} = \overline{a}x + b\,.$$

For elements $vx+c$, $wx+d$ of S, it follows that

$$(vx+c) * (wx+d) = (\overline{vw})x + (wc+d)$$

in the loop $(S,*,1)$. Then

$$(vx+c)R_*(wx+d)L_*(wx+d)^{-1} = vx + \big(wc + (1-v)d\big)\,. \tag{8.6}$$

Now $R_*(wx+d)L_*(wx+d)^{-1}$ is an element of the inner multiplication group of the loop $(S,*,1)$. For elements s, t of S, the pairs $(1,t)$ and $(1,tR_*(s)L_*(s)^{-1})$ share the same $(S,*)$-class. Take $t = vx + (u-1)$ for some element u of T distinct from 1. Take $s = ux+u$. Using (8.6), one obtains the pairs

$$(1, ux + (u-1)) \quad \text{and} \quad (1, ux)$$

lying in the same $(S,*)$-class. Mapping via the inverse of the isomorphism (8.5), one obtains the pairs

$$(\{\pm 1\}, \{-1, 2u-1\}) \quad \text{and} \quad (\{\pm 1\}, \{\pm u\})$$

lying in the same $(Q,+_e)$-class. However, the first pair lies in the $(Q,\cdot)$-class C_2, while the second pair lies in the $(Q,\cdot)$-class C_3, This is a contradiction, since C_2 is a union of $(Q,+_e)$-classes. ∎

COROLLARY 8.3
The character table of the Johnson scheme $J(5,2)$ is not a quasigroup character table.

PROOF A computer search shows that the only sharply transitive subsets of $S_5^{[2]}$ that contain 1 are those lying entirely within $L_5^{[2]}$, and thus of the form $S(T)$. Proposition 8.4 then shows that there can be no quasigroup with the character table of $J(5,2)$. □

8.3 Superschemes

Definition 6.2 (p. 147) for a (commutative) association scheme may be restated with a slight change of notation as follows.

DEFINITION 8.2 *Let Q be a finite, nonempty set. Then an* association scheme (Q, Γ^0) *on Q is a disjoint union partition*

$$Q^{0+2} = C_1^0 + \cdots + C_{s_0}^0$$

or $\Gamma^0 = \{C_1^0, \ldots, C_{s_0}^0\}$ of the direct square of Q such that:

(A1) $C_1^0 = \{(x,x) \mid x \in Q\}$;

(A2) $\forall\, C_j^0 \in \Gamma^0$,

$$\{(x_1,x_2) \mid \exists\, (y_1,y_2) \in C_j^0 \,.\, x_1 = y_2, x_2 = y_1\} \in \Gamma^0\,;$$

(A3) $\forall\, C_i^0 \in \Gamma^0$, $\forall\, C_j^0 \in \Gamma^0$, $\forall\, C_k^0 \in \Gamma^0$,

$$\begin{aligned}
&\exists\, c(i,j,k;0,0) \in \mathbb{N}\,.\\
&\forall\, (x_0,y_0) \in C_k^0\,,\\
&\left|\{z \in Q \mid (x_0,z) \in C_i^0,\ (z,y_0) \in C_j^0\}\right| = c(i,j,k;0,0)\,;
\end{aligned}$$

(A4) $\forall\, 1 \le i,j,k \le s_0$, $c(i,j,k;0,0) = c(j,i,k;0,0)$.

The Bose-Mesner algebra of the association scheme (Q, Γ^0) is the complex vector space $\mathbb{C}\Gamma^0$ with basis Γ^0, equipped with the associative and commutative multiplication induced from

$$C_i^0 \cdot C_j^0 = \sum_{k=1}^{s_0} c(i,j,k;0,0) C_k^0 \tag{8.7}$$

by linearity. The algebra has a semilinear involution * extending the conversion $(C_i^0)^* = (C_i^0)^{-1}$.

According to Definition 8.2, an association scheme structure (Q, Γ^0) on a set Q is a collection Γ^0 of binary relations on Q satisfying the axioms (A1)–(A4). The concept of a superscheme describes a comparable collection of relations on Q, but with an arbitrary (finite) number of arguments. Now relations on Q are subsets of powers of Q. For a function $f : I \to J$ between index sets, there is a contravariantly induced function

$$f^* : Q^J \to Q^I; (j : J \to Q) \mapsto (fj : I \to Q)$$

between the corresponding powers of Q. For the transposition

$$\tau : \{1,2\} \to \{1,2\}; 1 \mapsto 2, 2 \mapsto 1\,,$$

the conversion axiom (A2) of Definition 8.2 may be rewritten in the form $\tau^*(C_j^0) \in \Gamma^0$. Thus the following definition gives a natural extension of the definition of an association scheme.

DEFINITION 8.3 *Let Q be a finite, nonempty set. Then a* superscheme *(Q, Γ^*) on Q is a disjoint union partition*

$$Q^{2+n} = C_1^n + \cdots + C_{s_n}^n$$

or $\Gamma^n = \{C_1^n, \ldots, C_{s_n}^n\}$ of the $(2+n)$-th power of Q, for each natural number n, such that:

(S1) $\forall\, n \in \mathbb{N}\,,\ C_1^n = \{(x, \ldots, x) \mid x \in Q\}\,;$

(S2) $\forall\, m, n \in \mathbb{N}\,,\ \forall\, f : \{1, \ldots, 2+m\} \to \{1, \ldots, 2+n\}\,,\ \forall\, C_j^n \in \Gamma^n\,,$

$$f^*(C_j^n) \in \Gamma^m\,;$$

(S3) $\forall\, m, n \in \mathbb{N}\,,\ \forall\, C_i^m \in \Gamma^m\,,\ \forall\, C_j^n \in \Gamma^n\,,\ \forall\, C_k^{m+n} \in \Gamma^{m+n}\,,$

$$\begin{aligned}
&\exists\, c(i,j,k;m,n) \in \mathbb{N}\,.\\
&\forall\, (x_0, \ldots, x_m, y_0, \ldots, y_n) \in C_k^{m+n}\,,\\
&\left|\{z \in Q \mid (x_0, \ldots, x_m, z) \in C_i^m,\ (z, y_0, \ldots, y_n) \in C_j^n\}\right| = c(i,j,k;m,n)\,;
\end{aligned}$$

(S4) $\forall\, 1 \le i, j, k \le s_0\,,\ c(i,j,k;0,0) = c(j,i,k;0,0).$

Note that the set $f^*(C_j^n)$ appearing in the axiom (S2) may be written in the form

$$\{(x_1, \ldots, x_{2+m}) \in Q^{2+m} \mid \exists\, (y_1, \ldots, y_{2+n}) \in C_j^n\,.\, \forall\, 1 \le i \le 2+m\,,\ x_i = y_{if}\}\,.$$

The following observation is a direct consequence of Definitions 8.2 and 8.3.

LEMMA 8.1
Let (Q, Γ^*) be a superscheme on a finite, nonempty set Q. Then the binary reduct (Q, Γ^0) of (Q, Γ^*) is an association scheme on Q.

Examples of superschemes are furnished by multiplicity-free group actions.

PROPOSITION 8.5
Let G be a group of permutations having a multiplicity-free action on a finite, nonempty set Q. For each natural number n, let Γ^n be the set of orbits of G on Q^{2+n}. Then (Q, Γ^*) is a superscheme.

PROOF Since (Q, Γ^0) is an association scheme, the existence of the numbers $c(i, j, k; 0, 0)$ is immediate, as is the satisfaction of the axiom (S4). For natural numbers m, n and a function

$$f : \{1, \ldots, 2 + m\} \to \{1, \ldots, 2 + n\},$$

the set $f^*(C_j^n)$ is an orbit of G on Q^{2+m} if C_j^n is an orbit of G on Q^{2+n}. Thus (S2) is satisfied. For each natural number n, the subset $\{(x, \ldots, x) \mid x \in Q\}$ of Q^{2+n} is an orbit, so (S1) is satisfied.

Finally, consider orbits $C_i^m \in \Gamma^m$, $C_j^n \in \Gamma^n$ and $C_k^{m+n} \in \Gamma^{m+n}$ for natural numbers m and n. Consider two elements

$$(x_0, \ldots, x_m, y_0, \ldots, y_n) \quad \text{and} \quad (x'_0, \ldots, x'_m, y'_0, \ldots, y'_n)$$

of C_k^{m+n}. Define

$$A = \{z \in Q \mid (x_0, \ldots, x_m, z) \in C_i^m,\ (z, y_0, \ldots, y_n) \in C_j^n\}$$

and

$$A' = \{z' \in Q \mid (x'_0, \ldots, x'_m, z') \in C_i^m,\ (z', y'_0, \ldots, y'_n) \in C_j^n\}.$$

Since C_k^{m+n} is an orbit of G, there is an element g of G such that

$$(x_0, \ldots, x_m, y_0, \ldots, y_n)g = (x'_0, \ldots, x'_m, y'_0, \ldots, y'_n).$$

Since C_i^m and C_j^n are orbits of G, the containment $z \in A$ implies $zg \in A'$. Thus $|A| \leq |A'|$, whence $|A'| \leq |A|$ by symmetry. The natural number $c(i, j, k; m, n)$ is obtained as the common value of the cardinalities $|A|$, $|A'|$, and the axiom (S3) is satisfied. □

An immediate consequence of Proposition 8.5 is the following analogue of Theorem 6.3.

COROLLARY 8.4
Each finite, nonempty quasigroup Q determines a superscheme (Q, Γ^*) given according to Proposition 8.5 by the action of the combinatorial multiplication group.

There are some ancillary concepts connected with each superscheme.

DEFINITION 8.4 *Let (Q, Γ^*) be a superscheme on a finite, nonempty set Q.*

(a) *The association scheme (Q, Γ^0) of Lemma 8.1 is called the* associated scheme *of the superscheme (Q, Γ^*);*

(b) *The sequence $s : \mathbb{N} \to \mathbb{Z}^+; n \mapsto s_n$ is called the* dimension sequence *of the superscheme (Q, Γ^*);*

(c) *The complex function $p(z)$ obtained by analytic continuation of*

$$\sum_{n=0}^{\infty} s_n z^n$$

is called the Poincaré series *of the superscheme (Q, Γ^*).*

The set of superschemes on a given finite, nonempty set Q is partially ordered, with $(Q, \Gamma^*) \leq (Q, \Delta^*)$ if and only if each Δ^n-class is a union of Γ^n-classes, for each natural number n. Formally,

$$(Q, \Gamma^*) \leq (Q, \Delta^*) \Leftrightarrow$$
$$\forall\, n \in \mathbb{N}\,, \forall\, D_j^n \in \Delta^n\,, \exists\, C_{j_1}^n, \ldots, C_{j_r}^n \in \Gamma^n\,.\, D_j^n = C_{j_1}^n \cup \cdots \cup C_{j_r}^n\,.$$

8.4 Superalgebras

Let (Q, Γ^*) be a superscheme on a given finite, nonempty set Q. For each natural number n, form the complex vector space $\mathbb{C}\Gamma^n$ with basis Γ^n. Then the *Bose-Mesner superalgebra* of the superscheme (Q, Γ) is the direct sum

$$\mathbb{C}\Gamma^* = \bigoplus_{n=0}^{\infty} \mathbb{C}\Gamma^n$$

of the spaces $\mathbb{C}\Gamma^n$. A product is defined on $\mathbb{C}\Gamma$ as the bilinear extension of

$$C_i^m \cdot C_j^n = \sum_{k=1}^{s_{m+n}} c(i, j, k; m, n) C_k^{m+n}\,. \tag{8.8}$$

Comparison with (8.7) shows that the Bose-Mesner superalgebra of a superscheme is analogous to the Bose-Mesner algebra of an association scheme. The Bose-Mesner superalgebra is graded over the monoid $\mathbb{N}$ of natural numbers by assigning degree n to $\mathbb{C}\Gamma^n$, since (8.8) yields

$$\mathbb{C}\Gamma^m \cdot \mathbb{C}\Gamma^n \subseteq \mathbb{C}\Gamma^{m+n} \tag{8.9}$$

for natural numbers m and n. For each natural number n, the subspace $\mathbb{C}\Gamma^n$ of $\mathbb{C}\Gamma^*$ is called the *homogeneous component* of *degree* n. In particular, the homogeneous component of degree 0 is the Bose-Mesner algebra of the associated scheme. There is a linear *trace function* defined on the homogeneous component of degree n by

$$\mathrm{Tr}\Big(\sum_{j=1}^{s_n} c_j C_j^n\Big) = |Q|^{n+1} c_1 \tag{8.10}$$

for each natural number n. For $n = 0$, the trace function (8.10) agrees with the the usual trace function on the Bose-Mesner algebra of the associated scheme.

PROPOSITION 8.6
The Bose-Mesner superalgebra of a superscheme (Q, Γ^*) *is associative.*

PROOF It suffices to prove that

$$(C_i^m C_j^n) C_k^p = C_i^m (C_j^n C_k^p) \tag{8.11}$$

for natural numbers m, n, p and $1 \le i \le s_m$, $1 \le j \le s_n$, $1 \le k \le s_p$. The coefficient of an element C_l^{m+n+p} of Γ^{m+n+p} in the left-hand side of (8.11) is

$$\sum_{q=1}^{s_{m+n}} c(i,j,q;m,n)c(q,k,l;m+n,p)\,. \tag{8.12}$$

The coefficient of C_l^{m+n+p} in the right hand side of (8.11) is

$$\sum_{r=1}^{s_{n+p}} c(i,r,l;m,n+p)c(j,k,r;n,p)\,. \tag{8.13}$$

Fix an element

$$(x_0, \ldots, x_m, y_1, \ldots, y_n, z_0, \ldots, z_p)$$

of C_l^{m+n+p}. Then by (S3), both (8.12) and (8.13) count the number of elements (t, u) of Q^2 such that $(x_0, \ldots, x_m, t)$ lies in C_i^m, $(t, y_1, \ldots, y_n, u)$ lies in C_j^n, and $(u, z_0, \ldots, z_p)$ lies in C_k^p. □

COROLLARY 8.5

Each homogeneous component of the Bose-Mesner superalgebra of a superscheme is a two-sided module over the commutative Bose-Mesner algebra of the associated scheme.

PROOF The left and right actions of $\mathbb{C}\Gamma^0$ on the homogeneous component $\mathbb{C}\Gamma^n$ of degree n are given by

$$L_n : \mathbb{C}\Gamma^0 \to \mathrm{End}_{\mathbb{C}}\mathbb{C}\Gamma^n; x \mapsto (y \mapsto xy) \tag{8.14}$$

and

$$R_n : \mathbb{C}\Gamma^0 \to \mathrm{End}_{\mathbb{C}}\mathbb{C}\Gamma^n; x \mapsto (y \mapsto yx) \tag{8.15}$$

respectively. Note that (8.14) and (8.15) are well-defined by (8.9). □

COROLLARY 8.6

The Bose-Mesner superalgebra of a superscheme is a two-sided module over the commutative Bose-Mesner algebra of the associated scheme.

PROOF The left and right actions of $\mathbb{C}\Gamma^0$ on $\mathbb{C}\Gamma^*$ are given by the respective sums

$$L = \bigoplus_{n=0}^{\infty} L_n \quad \text{and} \quad R = \bigoplus_{n=0}^{\infty} R_n$$

of the maps (8.14) and (8.15). □

By Definition 8.3(S2), for each pair m, n of natural numbers, each function

$$f : \{1, \ldots, 2+m\} \to \{1, \ldots, 2+n\}$$

determines a function $f^* : \Gamma^n \to \Gamma^m$. This latter function has a linear extension

$$f^* : \mathbb{C}\Gamma^n \to \mathbb{C}\Gamma^m$$

mapping from degree n to degree m. Finally, for each natural number n, consider the converse

$$(C_j^n)^* = \{(x_{m+1}, \ldots, x_0) \mid (x_0, \ldots, x_{m+1}) \in C_j^n\}$$

of a relation C_j^n in Γ^n. This conversion extends to a semilinear, anti-isomorphic involution * on the Bose-Mesner superalgebra (Exercise 7).

8.5 Tensor squares

In this section, it will be shown how the tensor square $\Psi \otimes \Psi$ of the character table Ψ of a finite quasigroup Q may be interpreted in the context of superalgebras. The first part of the section considers a general superscheme (Q, Γ^*).

The Bose-Mesner algebra $\mathbb{C}\Gamma^0$ of the associated scheme is commutative. The tensor square $\mathbb{C}\Gamma^0 \otimes \mathbb{C}\Gamma^0$ of the complex vector space $\mathbb{C}\Gamma^0$ with itself is (the underlying space of) the coproduct of $\mathbb{C}\Gamma^0$ with itself in the category of commutative $\mathbb{C}$-algebras (compare [165, Ch. IV, Exercise 2.2H]). Now the images of the $\mathbb{C}$-algebra homomorphisms (8.14) and (8.15) are respective commutative subalgebras $L_n(\mathbb{C}\Gamma^0)$ and $R_n(\mathbb{C}\Gamma^0)$ of $\mathrm{End}_{\mathbb{C}}\mathbb{C}\Gamma^n$. Since $\mathbb{C}\Gamma^*$ is associative, these commutative subalgebras commute mutually, and thus generate a commutative subalgebra K_n of $\mathrm{End}_{\mathbb{C}}\mathbb{C}\Gamma^n$. Let

$$L_n \otimes R_n : \mathbb{C}\Gamma^0 \otimes \mathbb{C}\Gamma^0 \to K_n \tag{8.16}$$

be the coproduct of the commutative $\mathbb{C}$-algebra homomorphisms

$$L_n : \mathbb{C}\Gamma^0 \to K_n \quad \text{and} \quad R_n : \mathbb{C}\Gamma^0 \to K_n\,.$$

The codomain of the $\mathbb{C}$-algebra homomorphism (8.16) may also be taken as the full (noncommutative) $\mathbb{C}$-algebra $\mathrm{End}_{\mathbb{C}}\mathbb{C}\Gamma^n$. Similarly, one may define a $\mathbb{C}$-algebra homomorphism

$$L \otimes R : \mathbb{C}\Gamma^0 \otimes \mathbb{C}\Gamma^0 \to \mathrm{End}_{\mathbb{C}}\mathbb{C}\Gamma^*; x_1 \otimes x_2 \mapsto \big(L \otimes R(x_1 \otimes x_2) : y \mapsto x_1 y x_2\big)\,.$$

For each natural number n, define

$$\lambda : \{1,2,3\} \to \{1,2\}; 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 2$$

and

$$\rho : \{1,2,3\} \to \{1,2\}; 1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 2\,.$$

LEMMA 8.2
Let a, b be elements of $\mathbb{C}\Gamma^0$.

(a) *The equation*

$$\lambda^*(a) \cdot b = a \cdot \rho^*(b) \tag{8.17}$$

holds in $\mathbb{C}\Gamma^1$.

(b) *The equation*

$$\mathrm{Tr}\big(\lambda^*(a) \cdot b\big) = \mathrm{Tr}\,(a) \cdot \mathrm{Tr}\,(b) = \mathrm{Tr}\big(a \cdot \rho^*(b)\big) \tag{8.18}$$

holds in $\mathbb{C}$.

PROOF For (8.17), it suffices to prove that

$$\lambda^*(C_i^0) \cdot C_j^0 = C_i^0 \cdot \rho^*(C_j^0) \tag{8.19}$$

for given C_i^0, C_j^0 in Γ^0. Fix C_k^1 in Γ^1. Suppose $(x, y, z) \in C_k^1$. Then in the expansion of each side of (8.19) as a complex linear combination of elements of Γ^1, the coefficient of C_k^1 is

$$\left|\{y \in Q \mid (x, y) \in C_i^0\,,\, (y, z) \in C_j^0\}\right|,$$

which is zero unless both $(x, y) \in C_i^0$ and $(y, z) \in C_j^0$, in which case it is 1. Setting $k = 1$ shows $\mathrm{Tr}\big(\lambda^*(a) \cdot b\big) = \delta_{1i}\delta_{1j}$. Then (8.18) follows by linearity. □

THEOREM 8.3
The algebra homomorphisms

$$L_1 \otimes R_1 : \mathbb{C}\Gamma^0 \otimes \mathbb{C}\Gamma^0 \to \mathrm{End}_{\mathbb{C}}\mathbb{C}\Gamma^1$$

and

$$L \otimes R : \mathbb{C}\Gamma^0 \otimes \mathbb{C}\Gamma^0 \to \mathrm{End}_{\mathbb{C}}\mathbb{C}\Gamma^*$$

embed the tensor square $\mathbb{C}\Gamma^0 \otimes \mathbb{C}\Gamma^0$ as a commutative subalgebra of the two respective endomorphism rings.

PROOF For each element α of $\mathbb{C}\Gamma^0 \otimes \mathbb{C}\Gamma^0$, the endomorphism $L \otimes R(\alpha)$ of $\mathbb{C}\Gamma^*$ restricts to the endomorphism $L_1 \otimes R_1(\alpha)$ of $\mathbb{C}\Gamma^1$. It thus suffices to show that $L_1 \otimes R_1$ embeds.

Now (to within isomorphism) the commutative algebra $\mathbb{C}\Gamma^0$ has one basis (6.18) consisting of the incidence matrices $A_1, \ldots, A_s$ of the respective relations $C_1^0, \ldots, C_s^0$ (taking $s = s_0$), and another (6.26) consisting of idempotent matrices $E_1, \ldots, E_s$, with

$$E_i = \sum \eta_{ij} A_j \quad \text{and} \quad \mathrm{Tr}\, E_i = \frac{f_i}{|Q|} \neq 0$$

for $1 \leq i \leq s$. Suppose that

$$\alpha = \sum_{1 \leq i,j \leq s} c_{ij} E_i \otimes E_j$$

lies in the kernel of $L_1 \otimes R_1$. Then for each element a of $\mathbb{C}\Gamma^1$,

$$0 = aL_1 \otimes R_1(\alpha) = \sum_{1 \leq i,j \leq s} c_{ij} E_i \cdot a \cdot E_j\,.$$

Given $1 \leq i, j \leq s$, use (8.17) to take

$$a_{ij} = \lambda^*(E_i) \cdot E_j = E_i \cdot \rho^*(E_j) \in \mathbb{C}\Gamma^1\,.$$

For $k \neq i$ or $l \neq j$, one has $E_k \cdot a_{ij} \cdot E_l = 0$. Thus

$$\begin{aligned} 0 &= a_{ij} L_1 \otimes R_1(\alpha) \\ &= c_{ij} E_i \cdot a_{ij} \cdot E_j \\ &= c_{ij} E_i \cdot E_i \cdot \rho^*(E_j) \cdot E_j \\ &= c_{ij} E_i \cdot \rho^*(E_j) \cdot E_j \\ &= c_{ij} a_{ij} \cdot E_j \\ &= c_{ij} \lambda^*(E_i) \cdot E_j \cdot E_j \\ &= c_{ij} \lambda^*(E_i) \cdot E_j = c_{ij} a_{ij} \,. \end{aligned}$$

But $a_{ij} \neq 0$, since (8.18) gives

$$\mathrm{Tr}(a_{ij}) = \mathrm{Tr}(E_i) \cdot \mathrm{Tr}(E_j) \neq 0 \,.$$

Thus $c_{ij} = 0$ for all $1 \leq i, j \leq s$. In other words, $\alpha = 0$ and $L_1 \otimes R_1$ injects. □

Now let Q be a finite, nonempty quasigroup with character table Ψ. Let (Q, Γ^*) be the superscheme on Q furnished by Corollary 8.4. Recall that the Bose-Mesner algebra $\mathbb{C}\Gamma^0$ of the associated scheme of the superscheme (Q, Γ) is the centralizer ring $V(G, Q)$ of the combinatorial multiplication group G on Q. The tensor square $V(G, Q) \otimes V(G, Q)$ has bases

$$\{\alpha_i \otimes \alpha_j \mid 1 \leq i, j \leq s\} \quad \text{and} \quad \{\epsilon_l \otimes \epsilon_m \mid 1 \leq l, m \leq s\} \,,$$

related by

$$\alpha_i \otimes \alpha_j = \sum_{l=1}^{s} \sum_{m=1}^{s} \xi_{il} \xi_{jm} \epsilon_l \otimes \epsilon_m \,.$$

The entries $\psi_{il}\psi_{jm}$ of the tensor square $\Psi \otimes \Psi$ are then given as the normalized coefficients

$$\psi_{il}\psi_{jm} = \frac{\sqrt{f_i f_j}}{n_l n_m} \xi_{il} \xi_{jm} \,.$$

The combinatorial interpretation of the tensor square $\Psi \otimes \Psi$ may be summarized as follows.

COROLLARY 8.7

Let Q be a finite, nonempty quasigroup with combinatorial multiplication group G and character table Ψ. Then the tensor square $\Psi \otimes \Psi$ is determined by the two-sided action of the centralizer ring $V(G, Q)$ on the set of orbits of G on Q^3.

8.6 Relation algebras

Proposition 8.5 showed that if G is a multiplicity-free permutation group acting on a finite, nonempty set Q, then the orbits of G on powers of Q give a superscheme (Q, Γ^*). The aim of the current section is to prove the converse of Proposition 8.5: If (Q, Γ^*) is a superscheme on a finite, nonempty set Q, then there is a permutation group G acting on Q such that the relations C_i^m of the superscheme are precisely the orbits of G on the powers of Q. For this purpose, multiplicity-freeness is irrelevant. It is then convenient to define a *noncommutative superscheme* (Q, Γ^*) exactly as in Definition 8.3, but without the commutativity axiom (S4). Thus the main theorem of this section, Theorem 8.5 below, gives the converse to the following reformulated version of Proposition 8.5.

PROPOSITION 8.7

Let G be a transitive group of permutations acting on a finite, nonempty set Q. For each natural number n, let Γ^n be the set of orbits of G on Q^{2+n}. Then (Q, Γ^*) is a noncommutative superscheme on Q.

The converse depends on a relational-algebraic characterization of full sets of group orbits due to Krasner [102]. Consider an m-ary relation R on a set Q, i.e. a subset of the m-th direct power Q^m. For $m > 1$, new relations are defined as follows:

$$R^\zeta = \{(x_1, x_2, \ldots, x_m) \mid (x_2, \ldots, x_m, x_1) \in R\} \tag{8.20}$$

$$R^\tau = \{(x_1, x_2, \ldots, x_m) \mid (x_2, x_1, x_3 \ldots, x_m) \in R\} \tag{8.21}$$

$$R^\Delta = \{(x_1, x_2, \ldots, x_{m-1}) \mid (x_1, x_1, x_2 \ldots, x_{m-1}) \in R\}\,. \tag{8.22}$$

Note that R^ζ and R^τ are m-ary, while R^Δ is $(m-1)$-ary, and may be empty even when R itself is nonempty. For $m \geq 1$, a new relation

$$R^\nabla = Q \times R = \{(x_0, x_1, \ldots, x_m) \mid x_0 \in Q,\ (x_1, \ldots, x_m) \in R\} \tag{8.23}$$

is defined. Given an $(2+m)$-ary relation R and an $(2+n)$-ary relation S, a $(2+m+n)$-ary relation $R \circ S$ is defined as the *relation product*

$$\{(x_0, \ldots, x_m, y_0, \ldots, y_n) \mid \exists\, z \in Q\,.\,(x_0, \ldots, x_m, z) \in R, (z, y_0, \ldots, y_n) \in S\}$$

generalizing the binary relation product (3.2). Finally, considering m-ary relations as subsets of the direct power Q^m, it is apparent that the set of m-ary relations carries the Boolean algebra structure (intersection, complementation, etc.) of the power set of Q^m.

DEFINITION 8.5 *Let Q be a set. Then a* Krasner algebra *on Q is a set of relations on Q, containing the equality relation $\{(x,x) \mid x \in Q\}$, that is closed under the operations of* (8.20) *through* (8.23)*, intersection, complementation, and relation product.*

Krasner's characterization of permutation group actions may now be stated.

THEOREM 8.4 (***Krasner's Theorem***)
Let Q be a finite, nonempty set. If K is a Krasner algebra on Q, then K is the set of relations on Q that are invariant under the action of a permutation group G on Q.

The proofs of Krasner's Theorem 8.4 in the literature [16, Th. 4] [102] [130, §1.3.5] are not very constructive, the group G appearing only as the group of permutations of Q preserving K.

Now suppose that (Q, Γ^*) is a noncommutative superscheme on a finite, nonempty set Q. A Krasner algebra K on Q will be constructed from (Q, Γ^*). For each natural number n, let

$$B_{2+n} = \{C^n_{i_1} \cup \cdots \cup C^n_{i_r} \mid 0 \le r \le s_n,\ 1 \le i_j \le s_n\} \tag{8.24}$$

be the σ-field or Boolean subalgebra of the power set of Q^{2+n} that is generated by the partition Γ^n of Q^{2+n}. Define

$$B_1 = \{\varnothing, Q\} \tag{8.25}$$

and

$$K = \bigcup_{m=1}^{\infty} B_m\,. \tag{8.26}$$

LEMMA 8.3
The set K of relations on Q is closed under the operation Δ of (8.22)*.*

PROOF For $m > 1$, consider

$$R = C^{m-2}_{i_1} \cup \cdots \cup C^{m-2}_{i_r} \in B_m\,.$$

If $(x_1, x_1, x_2, \ldots, x_{m-1})$ is an element of R, then there is an index $1 \le j \le r$ such that $(x_1, x_1, x_2, \ldots, x_{m-1}) \in C^{m-2}_{i_j}$. Now Γ^{m-3} is a partition of Q^{m-1}, so there is an index $1 \le k \le s_{m-3}$ such that $(x_1, x_2, \ldots, x_{m-1}) \in C^{m-3}_k$. Define the *predecessor function*

$$p : \{1, \ldots, m\} \to \{1, \ldots, m-1\}; i \mapsto \max\{1, i-1\}\,.$$

Then

$$(x_1, x_1, x_2, \ldots, x_{m-1}) \in p^*\big(C^{m-3}_k\big) \in \Gamma^{m-2}$$

by Axiom (S2) of Definition 8.3. Since Γ^{m-2} is a partition of Q^m, it follows that $C_{i_j}^{m-2} = p^*\big(C_k^{m-3}\big)$. Thus

$$R^{\Delta} = \bigcup \Big\{ C_k^{m-3} \in \Gamma^{m-3} \,\Big|\, \exists\, 1 \le j \le r \,.\, C_{i_j}^{m-2} = p^*\big(C_k^{m-3}\big) \Big\} \in B_{m-1}\,,$$

as required. □

LEMMA 8.4
The set K of relations on Q is closed under the operation ∇ of (8.23).

PROOF First note that $B_1^{\nabla} = \{\varnothing, Q^2\} \subset B_2$. Now for $m > 1$, consider

$$R = C_{i_1}^{m-2} \cup \cdots \cup C_{i_r}^{m-2} \in B_m\,.$$

If $(x_0, x_1, \ldots, x_m)$ is an element of R^{∇}, then there is an index $1 \le j \le r$ such that $(x_1, \ldots, x_m) \in C_{i_j}^{m-2}$. Now Γ^{m-1} is a partition of Q^{m+1}, so there is an index $1 \le k \le s_{m-1}$ such that $(x_0, x_1, \ldots, x_m) \in C_k^{m-1}$. Define the *successor function*

$$s : \{1, \ldots, m\} \to \{1, \ldots, m+1\}; i \mapsto i+1\,.$$

Then

$$(x_1, \ldots, x_m) \in s^*\big(C_k^{m-1}\big) \in \Gamma^{m-2}$$

by Axiom (S2) of Definition 8.3. Since Γ^{m-2} is a partition of Q^m, it follows that $C_{i_j}^{m-2} = s^*\big(C_k^{m-1}\big)$. Thus

$$R^{\nabla} = \bigcup \Big\{ C_k^{m-1} \in \Gamma^{m-1} \,\Big|\, \exists\, 1 \le j \le r \,.\, C_{i_j}^{m-2} = s^*\big(C_k^{m-1}\big) \Big\} \in B_{m+1}\,,$$

as required. □

It is interesting to observe the duality between the statements and proofs of Lemmas 8.3 and 8.4.

LEMMA 8.5
The set K of relations on Q is a Krasner algebra on Q.

PROOF By Axiom (S1) of Definition 8.3, K contains the binary equality relation $\widehat{Q}$ on Q. Since each uniand B_m in (8.26) is a Boolean subalgebra of the power set of the corresponding direct power Q^m, the set K is closed under intersection and complementation. For fixed $m > 1$, define the permutations

$$z = (1\ 2\ \ldots\ m) \quad \text{and} \quad t = (1\ 2)$$

on $\{1, 2, \ldots, m\}$. Then for $0 \le r \le s_{m-2}$ and $1 \le i_j \le s_{m-2}$, one has

$$\left(C_{i_1}^{m-2} \cup \cdots \cup C_{i_r}^{m-2}\right)^{\zeta} = z^*\left(C_{i_1}^{m-2}\right) \cup \cdots \cup z^*\left(C_{i_r}^{m-2}\right) \in B_m$$

and

$$\left(C_{i_1}^{m-2} \cup \cdots \cup C_{i_r}^{m-2}\right)^{\tau} = t^*\left(C_{i_1}^{m-2}\right) \cup \cdots \cup t^*\left(C_{i_r}^{m-2}\right) \in B_m$$

by Axiom (S2) of Definition 8.3, Along with Lemmas 8.3 and 8.4, these memberships show that K is closed under the operations (8.20) through (8.23). Finally, for

$$R = C_{i_1}^m \cup \cdots \cup C_{i_q}^m \quad \text{and} \quad S = C_{j_1}^n \cup \cdots \cup C_{j_r}^n ,$$

the relation product $R \circ S$ may be expressed as the element

$$\bigcup \left\{ C_k \in \Gamma^{m+n} \,\middle|\, \exists\, 1 \le t \le q \,.\, \exists\, 1 \le u \le r \,.\, c(i_t, j_u, k; m, n) > 0 \right\}$$

of B_{2+m+n}, so that K is also closed under the relation product. □

THEOREM 8.5

Let Q be a finite, nonempty set. Suppose that (Q, Γ^*) is a noncommutative superscheme on Q. Then there is a transitive permutation group G acting on Q such that for each natural number n, the partition Γ^n of the superscheme is the set of orbits of G on Q^{2+n}.

PROOF Let K be the Krasner algebra on Q given from (Q, Γ^*) by Lemma 8.5. By Krasner's Theorem 8.4, there is a group G acting on Q such that K is the set of relations on Q that are invariant under the action. In particular each Γ^n, as the set of atoms in the Boolean algebra B_{2+n}, is the set of orbits under the componentwise action of G on Q^{2+n}. By (8.25), the action of G on Q is transitive. □

COROLLARY 8.8

An association scheme is the associated scheme of a superscheme if and only if it consists of the orbitals of a multiplicity-free permutation group action.

Wojdyło [177] investigated association schemes which cannot be extended to superschemes beyond a certain level. The association schemes are based on graphs, and the extent to which the association scheme can be extended is related to the satisfaction of so-called *vertex conditions* in the graph.

8.7 The Reconstruction Theorem

Let (Q, Γ^*) be a noncommutative superscheme on a finite, nonempty set Q. By Theorem 8.5, the classes of Γ^* are the orbits of a transitive permutation group G of Q acting on the powers of Q. In this section, it will be shown how the Bose-Mesner superalgebra $\mathbb{C}\Gamma^*$ of (Q, Γ^*) may be used to recover the set Q and the group G to within similarity. Note that the order n of Q is the trace of the identity element C_1^0 of $\mathbb{C}\Gamma^*$.

DEFINITION 8.6 *In a Bose-Mesner superalgebra* $\mathbb{C}\Gamma^*$*, a* principal basis element *is an element* $P = C_p^{n-2}$ *of the homogeneous* $(n-2)$*-th degree basis* Γ^{n-2} *which is not an element of* $f^*(\Gamma^{m-2})$ *for any function*

$$f : \{1, \ldots, n\} \to \{1, \ldots, m\}$$

with $m < n$.

Definition 8.6 means that for each element $(x_1, \ldots, x_n)$ of P, no two coordinates x_i and x_j coincide if $i \neq j$. From now on, fix one particular principal basis element P of $\mathbb{C}\Gamma^*$.

For the successor function

$$s : \{1, \ldots, n\} \to \{1, \ldots, n+1\}; i \mapsto i+1\,,$$

define

$$Q' = (s^*)^{-1}\{P\} \subset \Gamma^{n-1}\,. \tag{8.27}$$

Note that $C_i^{n-1} \in Q'$ if and only if $C_i^{n-1} \leq P^\nabla$ in the Boolean algebra B_{n+1}. The set Q' will serve as a proxy for Q.

For positive integers m and h, define the *left insertion*

$$l_{mh} : \{1, \ldots, m+1\} \to \{1, \ldots, 2m+h+1\}; i \mapsto i$$

and the *right insertion*

$$r_{mh} : \{1, \ldots, m+h\} \to \{1, \ldots, 2m+h+1\}; i \mapsto m+1+i\,.$$

Then define the *split*

$$\sigma : \Gamma^{2m} \to \Gamma^{m-1} \times \Gamma^{m-1}; C_i^{2m} \mapsto \left(l_{m1}^*(C_i^{2m}), r_{m1}^*(C_i^{2m})\right).$$

In analogy with (8.27), define

$$G' = \sigma^{-1}\{(P^*, P)\} \subset \Gamma^{2n-2}\,. \tag{8.28}$$

The set G' will serve as a proxy for G.

Identifying each (C_j^{m-1}, C_k^{m-1}) with $C_j^{m-1} \otimes C_k^{m-1}$, the split σ extends to a linear map

$$\sigma : \mathbb{C}\Gamma^{2m} \to \mathbb{C}\Gamma^{m-1} \otimes \mathbb{C}\Gamma^{m-1}$$

for each positive integer m. This map is also called the *split*. On the other hand, the bilinear multiplication in $\mathbb{C}\Gamma^*$ gives a linear map

$$\mu : \mathbb{C}\Gamma^* \otimes \mathbb{C}\Gamma^* \to \mathbb{C}\Gamma^*$$

that restricts to maps

$$\mu : \mathbb{C}\Gamma^{m-1} \otimes \mathbb{C}\Gamma^{m-1} \to \mathbb{C}\Gamma^{2m-2} \quad \text{and} \quad \mu : \mathbb{C}\Gamma^{m-1} \otimes \mathbb{C}\Gamma^{m+n-2} \to \mathbb{C}\Gamma^{2m+n-3}$$

for each positive integer m. Finally, define

$$\alpha : \Gamma^{2m+n-1} \to \Gamma^{m-1} \times \Gamma^{m+n-2}; C_i^{2m+n-1} \mapsto \left(l_{mn}^*(C_i^{2m+n-1}), r_{mn}^*(C_i^{2m+n-1})\right)$$

Identifying each (C_j^{m-1}, C_k^{m+n-2}) with $C_j^{m-1} \otimes C_k^{m+n-2}$, the map α extends to a linear transformation

$$\alpha : \mathbb{C}\Gamma^{2m+n-1} \to \mathbb{C}\Gamma^{m-1} \otimes \mathbb{C}\Gamma^{m+n-2}.$$

THEOREM 8.6 (***Reconstruction Theorem***)
Let $\mathbb{C}\Gamma^*$ be the Bose-Mesner superalgebra of the (noncommutative) superscheme given by a transitive permutation group G on a finite, nonempty set Q of order n. Let P be a fixed principal basis element of $\mathbb{C}\Gamma^*$. Let Q' be given by (8.27) *and G' by* (8.28). *Then there is a group multiplication*

$$(\mu\sigma)^{n-1}\mu : G' \times G' \to G'$$

and an action

$$(\mu\alpha)^{n-1}\mu : Q' \times G' \to Q'$$

that is similar to the action of G on Q.

PROOF Fix an element

$$\overrightarrow{p} = (x_1, \ldots, x_n)$$

in P. Set

$$\overleftarrow{p} = (x_n, \ldots, x_1)$$

in P^*. Then $P = \overrightarrow{p}\,G$ and $P^* = \overleftarrow{p}\,G$. The map

$$G \to G'; g \mapsto \left(\overleftarrow{p}\,g, \overrightarrow{p}\right)G \tag{8.29}$$

gives a bijection from G to G'. This bijection is an isomorphism, since for g, h in G one has

$$\begin{aligned}&\big(\overleftarrow{p}\,g, \overrightarrow{p}\big)G \otimes \big(\overleftarrow{p}\,h, \overrightarrow{p}\big)G(\mu\sigma)^{n-1}\mu\\ &\quad= \big(\overleftarrow{p}\,gh, \overrightarrow{p}\,h\big)G \otimes \big(\overleftarrow{p}\,h, \overrightarrow{p}\big)G(\mu\sigma)^{n-1}\mu\\ &\quad= \big(\overleftarrow{p}\,gh, \overrightarrow{p}\big)G\,.\end{aligned}$$

The map

$$Q \to Q'; q \mapsto \big(q, \overrightarrow{p}\big)G \tag{8.30}$$

gives a bijection from Q to Q'. The maps (8.29) and (8.30) give a similarity from G on Q to G' on Q', since for g in G and q in Q, one has

$$\begin{aligned}&\big(q, \overrightarrow{p}\big)G \otimes \big(\overleftarrow{p}\,g, \overrightarrow{p}\big)G(\mu\alpha)^{n-1}\mu\\ &\quad= \big(qg, \overrightarrow{p}\,g\big)G \otimes \big(\overleftarrow{p}\,g, \overrightarrow{p}\big)G(\mu\alpha)^{n-1}\mu\\ &\quad= \big(qg, \overrightarrow{p}\big)G\,.\end{aligned}$$

□

COROLLARY 8.9

Let Q be a finite, nonempty quasigroup. Then the permutation group action of the combinatorial multiplication group G on Q may be recovered from the Bose-Mesner superalgebra of the superscheme associated with Q according to Corollary 8.4.

8.8 Exercises

1. Let S be a set of permutations on a nonempty set Q.

   (a) Show that S is transitive if and only if the map

   $$Q \times S \to Q \times Q; (q, g) \mapsto (q, qg)$$

   is surjective.

   (b) Show that S is sharply transitive if and only if the map

   $$Q \times S \to Q \times Q; (q, g) \mapsto (q, qg)$$

   is bijective.

2. Consider the right regular permutation action of a finite group G on itself.

(a) Show that the compatibility graph of this action is complete on the vertex set G.

(b) Using Proposition 7.3 (p. 187) or otherwise, show that the action is similar to the action of a multiplication group on a quasigroup if and only if G is abelian.

3. Compute the compatibility graph of the dihedral group D_4 in its natural action. (Compare Example 2.2.)

4. Let G be a permutation group on a nonempty set Q. Let e be an element of Q, and let S be a sharply transitive subset of G. Show that $S\sigma(e,e)^{-1}$ is a loop transversal to the stabilizer G_e in G.

5. Verify that (8.2) is the character table of the Johnson scheme $J(8,2)$.

6. Let Q be a set of finite positive order n. Determine the dimension sequence and the Poincaré series of the minimal and maximal superschemes on Q.

7. For elements x, y of a Bose-Mesner superalgebra, show that $(xy)^* = x^*y^*$.

8. Let Q be a finite, nonempty set. Let (Q, Γ^*) be the superscheme given by the permutation action of a group G on Q with group permutation character π (compare Chapter 9).

(a) Show that the Poincaré series of (Q, Γ^*) is given by

$$p(z) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{1 - z\pi(g)} .$$

(b) By considering the smallest real pole of $p(z)$, and the corresponding residue, show how to obtain $|Q|$ and $|G|$ from $p(z)$.

9. Let Q be a quasigroup, with corresponding superscheme (Q, Γ^*) given by Corollary 8.4. For which Krasner algebra operations does the set of congruences of Q form a subreduct of K?

8.9 Problems

1. To what extent is it possible to characterize those association schemes that are the association schemes of finite quasigroups?

2. To what extent is it possible to characterize those scheme character tables that are the character tables of finite quasigroups?

8.10 Notes

Section 8.1

Baer [5] used the term *simply transitive* instead of "sharply transitive." The latter term was used by O'Nan [121].

Section 8.2

The main results of this section appeared in [97]. The proof of Proposition 8.3 is due to K.W. Johnson [88]. For a character-theoretic proof, see [121, p. 66] (compare Exercises 17 and 18 in Chapter 9). Theorem 8.2 was presented in [88] with a different proof.

Section 8.3

Superschemes were introduced in [94].

Section 8.6

The results of Sections 8.6 and 8.7 appeared in [155]. Krasner algebras were described as "Post coalgebras" in [16], and as "Krasner algebras of the second kind" in [130]. (The first kind characterizes monoid actions.)

Chapter 9

PERMUTATION CHARACTERS

In the first four sections of this chapter, properties of the permutation action of the multiplication group of a finite quasigroup are used to describe some of the algebra structure associated with a homogeneous space for that quasigroup. The remaining sections introduce the characters of a finite quasigroup that are associated with permutation actions of the quasigroup. These give a direct generalization of the permutation characters of a group. The fundamental tool for the chapter is the linear map (9.1).

Associated with each quasigroup homogeneous space is an algebra known as the enveloping algebra. This algebra is defined in Section 9.1 as a subspace of the domain of (9.1), equipped with an algebra structure that makes the restriction of (9.1) an algebra homomorphism, the so-called canonical representation of the enveloping algebra (Definition 9.1). Section 9.2 describes the structure of the enveloping algebra (Theorem 9.1), while Section 9.3 analyses the canonical representation. As an application of the enveloping algebra, Section 9.4 presents sufficient conditions for the commuting of the action matrices of a homogeneous space, as observed in the example of Section 4.2.

A different restriction of (9.1), namely (9.21), furnishes a representation of the centralizer ring of the quasigroup (Theorem 9.3). Definition 9.3 then defines a homogeneous space to be faithful when this restriction injects. The definition is consistent with the classical terminology in the group case. In Section 9.6, the restriction (9.21) is used to define quasigroup permutation characters for quasigroup homogeneous spaces, and the definition is extended to general permutation representations in Section 9.7. As an illustration, Section 9.8 computes the permutation characters of the quasigroup of integers modulo 4 under subtraction.

9.1 Enveloping algebras

For a subquasigroup P of a finite quasigroup Q, let L denote the relative left multiplication group $\mathrm{LMlt}_Q P$ of P in Q. Consider the complex vector spaces $\mathbb{C}Q$ with basis Q and $\mathbb{C}P\backslash Q$ with basis $P\backslash Q$. Identify linear maps between these spaces (and themselves) by their matrices with respect to these bases. Let A_P be the incidence matrix of elements of Q in the L-orbits forming $P\backslash Q$.

Now the definition (4.14) of the homogeneous space action matrices yields a function ρ or

$$\rho_{P\backslash Q} : \mathrm{End}_{\mathbb{C}}\mathbb{C}Q \to \mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q; C \mapsto A_P^+ C A_P \tag{9.1}$$

from the set of endomorphisms of the vector space $\mathbb{C}Q$ to the set of endomorphisms of the vector space $\mathbb{C}P\backslash Q$. The function (9.1) is linear, but is generally not a homomorphism for the monoid structures of the two endomorphism sets under composition. Define

$$E_P = A_P A_P^+ .$$

By the property (4.2) of the pseudoinverse, E_P is an idempotent of $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ under composition. Consider

$$(C, D) \mapsto C E_P D \tag{9.2}$$

as a binary operation on $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$. It is convenient to denote this binary operation by E_P, regarding the right-hand side of (9.2) as infix notation for the binary operation. Under the original $\mathbb{C}$-space structure and the multiplication E_P, the set $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ forms a nonunital ring. (Verification of the associative and distributive laws is immediate.) Since

$$\begin{aligned} C^\rho D^\rho &= A_P^+ C A_P A_P^+ D A_P \\ &= (C E_P D)^\rho , \end{aligned}$$

the map (9.1) then becomes a ring homomorphism

$$\rho_{P\backslash Q} : (\mathrm{End}_{\mathbb{C}}\mathbb{C}Q, +, E_P) \to (\mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q, +, \cdot) \tag{9.3}$$

from the nonunital ring structure on $\mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ to the ring $\mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q$ with the original multiplication given by composition.

Let G be the combinatorial multiplication group of Q, and let

$$\lambda : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}\mathbb{C}Q \tag{9.4}$$

be the linear permutation representation of G on Q. Proposition 9.1 below implies that $(\lambda(\mathbb{C}G), +, E_P)$ is a subring of $(\mathrm{End}_{\mathbb{C}}\mathbb{C}Q, +, E_P)$, and that (9.3) restricts to a representation

$$\rho_{P\backslash Q} : (\lambda(\mathbb{C}G), +, E_P) \to \mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q \tag{9.5}$$

of the subring.

DEFINITION 9.1 *The ring* $(\lambda(\mathbb{C}G), +, E_P)$ *is defined as the* enveloping algebra *of the homogeneous space* $P\backslash Q$*, and the representation* (9.5) *is called the* canonical representation *of the enveloping algebra.*

PROPOSITION 9.1

For a subquasigroup P of Q with relative left multiplication group L in Q, one has

$$E_P = \frac{1}{|L|} \sum_{l \in L} l^\lambda \,. \tag{9.6}$$

In particular, E_P is an element of $\lambda(\mathbb{C}G)$.

PROOF To simplify notation, drop the suffix P from A_P and A_P^+. For an element x of the basis Q of $\mathbb{C}Q$, it must be shown that the endomorphisms on each side of (9.6) have the same effect on x. Now

$$\begin{aligned} xE_P &= \sum_{y \in Q} x(AA^+)_{xy} \\ &= x \sum_{X \in P\backslash Q} \sum_{y \in Q} A_{xX} A^+_{Xy} \\ &= x \sum_{y \in xL} A_{x,xL} A^+_{xL,y} \\ &= \sum_{y \in xL} (xL) A^+_{xL,y} \,. \end{aligned}$$

On the other hand,

$$\begin{aligned} \frac{1}{|L|} \sum_{l \in L} xl &= \frac{1}{|L|} \cdot \frac{|L|}{|xL|} \sum_{y \in xL} y \\ &= \frac{1}{|xL|} \sum_{y \in xL} y \\ &= \sum_{y \in xL} (xL) A^+_{xL,y} \end{aligned}$$

as well. □

9.2 Structure of enveloping algebras

Theorem 6.4(a) (p. 150) shows that the permutation representation λ of G on Q is multiplicity-free, so that the G-module $\mathbb{C}Q$ decomposes as a direct sum (6.21) of mutually inequivalent irreducible G-modules. Let the corresponding linear representations be $\lambda_i : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}} X_i$ with characters $\chi_i = \mathrm{Tr}(\lambda_i)$, so

that $\lambda = \sum_{i=1}^{s} \lambda_i$ and $\lambda_i(\mathbb{C}G) = \mathrm{End}_{\mathbb{C}} X_i$, i.e.,

$$\lambda(\mathbb{C}G) = \bigoplus_{i=1}^{s} \mathrm{End}_{\mathbb{C}} X_i \ . \tag{9.7}$$

For $1 \le i \le s$, define idempotents $E_i = E_P^{\lambda_i}$ and subspaces $Y_i = X_i E_i$, $Z_i = X_i(1 - E_i)$, yielding an orthogonal decomposition

$$X_i = Y_i \oplus Z_i \tag{9.8}$$

of $\mathbb{C}$-spaces. By (9.6), one has

$$E_i = \frac{1}{|L|} \sum_{l \in L} l^{\lambda_i} \, ,$$

whence

$$\mathrm{Tr}\,(E_i) = \frac{1}{|L|} \sum_{l \in \mathrm{LMlt}_Q P} \chi_i(l) \ . \tag{9.9}$$

Note that $\mathrm{End}_{\mathbb{C}} X_i$ has the $\mathbb{C}$-space decomposition

$$\mathrm{End}_{\mathbb{C}} X_i = \mathrm{End}_{\mathbb{C}} Y_i \oplus \mathrm{Hom}_{\mathbb{C}}(Y_i, Z_i) \oplus \mathrm{Hom}_{\mathbb{C}}(Z_i, Y_i) \oplus \mathrm{End}_{\mathbb{C}} Z_i \ . \tag{9.10}$$

Consider $\mathrm{End}_{\mathbb{C}} X_i$ as a nonunital ring with multiplication

$$E_i : (a, b) \mapsto a E_i b \, .$$

PROPOSITION 9.2
For $1 \le i \le s$, the Jacobson radical of the ring $(\mathrm{End}_{\mathbb{C}} X_i, E_i)$ is

$$\{ a \in \mathrm{End}_{\mathbb{C}} X_i \mid E_i a E_i = 0 \} \ . \tag{9.11}$$

PROOF Denote the ring $(\mathrm{End}_{\mathbb{C}} X_i, E_i)$ by A, and its Jacobson radical by J. Now the Jacobson radical is characterized as the set of all elements a of the ring A for which ar is right quasiregular for each element r of A [43, Lemma 54]. In other words, J is the set of elements a of A satisfying

$$\forall\, r \in A \, , \, \exists\, s \in A \, . \quad ar + s + ars = 0 \ . \tag{9.12}$$

For a $\mathbb{C}$-endomorphism a of X_i, denote the respective components in the direct sum (9.11) by

$$\begin{aligned} a_{11} &= E_i a E_i \ , \\ a_{12} &= E_i a (1 - E_i) \ , \\ a_{21} &= (1 - E_i) a E_i \ , \\ a_{22} &= (1 - E_i) a (1 - E_i) \ . \end{aligned}$$

It is convenient to assemble these components into a 2×2-matrix, and to record composition in $\mathrm{End}_{\mathbb{C}}X_i$ by matrix multiplication [128, §3.4], [165, II§1.2]. A product aE_ib in A then takes the form

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} \\ a_{21}b_{11} & a_{21}b_{12} \end{bmatrix} , \tag{9.13}$$

so the equation in (9.12) becomes

$$\begin{bmatrix} a_{11}r_{11} + s_{11} + a_{11}r_{11}s_{11} & a_{11}r_{12} + s_{12} + a_{11}r_{12}s_{12} \\ a_{21}r_{11} + s_{21} + a_{21}r_{11}s_{11} & a_{21}r_{12} + s_{22} + a_{21}r_{11}s_{12} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} . \tag{9.14}$$

Note that the bottom rows of the matrices in (9.14) are made to coincide on setting

$$\begin{aligned} s_{21} &= -a_{21}r_{11} - a_{21}r_{11}s_{11} , \\ s_{22} &= -a_{21}r_{12} - a_{21}r_{11}s_{12} . \end{aligned}$$

Now if $a_{11} = 0$, setting $s_{11} = s_{12} = 0$ makes the top rows of the matrices in (9.14) coincide. Thus the set (9.11) is certainly contained in the Jacobson radical of A. Conversely, suppose a_{11} is nonzero. Let y be an element of Y_i for which ya_{11} is nonzero. Suppose $ya_{11}r_{11} = -y$. Then whatever the element s of A, one cannot satisfy

$$a_{11}r_{11} + s_{11} + a_{11}r_{11}s_{11} = 0 , \tag{9.15}$$

since applying each side of (9.15) to y would yield the contradiction

$$-y + ys_{11} - ys_{11} = 0 .$$

In other words, J coincides with (9.11). □

COROLLARY 9.1
For $1 \le i \le s$, the Jacobson radical J_i of the ring $(\mathrm{End}_{\mathbb{C}}X_i, E_i)$ satisfies $J_i^3 = 0$.

PROOF In the matrix notation of (9.13), one has

$$\begin{bmatrix} 0 & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & a_{21}b_{12} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} .$$

□

COROLLARY 9.2
For $1 \le i \le s$, the natural projection of the ring $(\mathrm{End}_{\mathbb{C}}X_i, E_i)$ onto its quotient by its Jacobson radical J_i retracts onto the subring $\mathrm{End}_{\mathbb{C}}Y_i$ under composition.

PROOF Since $(E_i)_{11}$ is the identity automorphism of the subspace Y_i of X_i, the ring $\mathrm{End}_{\mathbb{C}}Y_i$ under composition is a subring of $(\mathrm{End}_{\mathbb{C}}X_i, E_i)$. □

As final preparation for the Structure Theorem, it is helpful to characterize the dimensions (9.9) of the spaces Y_i.

LEMMA 9.1

For $1 \leq i \leq s$, the dimension (9.9) *of the space Y_i is the multiplicity m_i of the representation λ_i in the representation of G induced by the trivial representation of the relative left multiplication group L of P in Q.*

PROOF By Frobenius reciprocity (7.35), one has

$$\mathrm{Tr}(E_i) = \langle \chi_i \downarrow_L^G, 1_L \rangle_L = \langle \chi_i, 1_L \uparrow_L^G \rangle_G = m_i \tag{9.16}$$

for $1 \leq i \leq s$. □

The natural numbers (9.16) are called the *multiplicities*. They play a key role in the Structure Theorem:

THEOREM 9.1 (***Structure Theorem for Enveloping Algebras***)

Let P be a subquasigroup of a finite, nonempty quasigroup Q with multiplication group G. Suppose that the permutation representation $\lambda : G \to \mathrm{End}_{\mathbb{C}}\mathbb{C}Q$ of G on Q decomposes as a direct sum (6.21) *of irreducible G-modules with characters χ_i, for $1 \leq i \leq s$.*

(a) The Jacobson radical J of the enveloping algebra $(\lambda(\mathbb{C}G), +, E_P)$ satisfies $J^3 = 0$.

(b) The semisimple quotient $(\lambda(\mathbb{C}G), +, E_P)/J$ is the direct sum

$$\bigoplus_{i=1}^{s} \mathrm{End}_{\mathbb{C}}Y_i \tag{9.17}$$

of matrix rings whose respective sizes are given by the multiplicities (9.16).

PROOF (a) Apply Corollary 9.1 and $J = \bigoplus_{i=1}^{s} J_i$ [128, §4.3].
(b) Apply (9.7) and Corollary 9.2. □

9.3 The canonical representation

The first step in the analysis of the canonical representation (9.5) is to identify the space $\mathbb{C}P\backslash Q$ as a subspace of $\mathbb{C}Q$. The identification is achieved via the isomorphism given as follows.

PROPOSITION 9.3
There is an isomorphism of the space $\mathbb{C}P\backslash Q$ with the subspace

$$\mathbb{C}Q \cdot E_P = \bigoplus_{i=1}^{s} Y_i$$

of $\mathbb{C}Q$, under which the L-orbit qL of an element q of Q is mapped to the element qE_P of $\mathbb{C}Q \cdot E_P$.

PROOF For elements q, q' of Q, one has

$$qE_P = q'E_P \quad \text{iff} \quad \frac{1}{|L|}\sum_{l\in L} ql = \frac{1}{|L|}\sum_{l\in L} q'l$$

by (9.6). Thus a linear injection $\mathbb{C}P\backslash Q \to \mathbb{C}Q \cdot E_P$ is well-defined by setting $qL \mapsto qE_P$ for q in Q. Since Q spans $\mathbb{C}Q$, this injection surjects. □

From now on, the space $\mathbb{C}P\backslash Q$ will be identified with $\mathbb{C}Q \cdot E_P$.

PROPOSITION 9.4
The incidence matrix A_P corresponds to the linear map

$$A : \mathbb{C}Q \to \mathbb{C}P\backslash Q; q \mapsto qE_P \ , \tag{9.18}$$

while the pseudoinverse A_P^+ corresponds to

$$A^+ : \mathbb{C}P\backslash Q \to \mathbb{C}Q; qE_P \mapsto \frac{1}{|qL|}\sum_{x\in qL} x \ . \tag{9.19}$$

PROOF The matrix of (9.18) taken with respect to the bases Q of $\mathbb{C}Q$ and QE_P of $\mathbb{C}P\backslash Q$ is A_P. The matrix of (9.19) with respect to these bases is A_P^+. □

PROPOSITION 9.5
The map A of (9.18) is a retraction of $\mathbb{C}Q$ onto its subspace $\mathbb{C}P\backslash Q$. The map A^+ of (9.19) is the embedding of $\mathbb{C}P\backslash Q$ into $\mathbb{C}Q$.

PROOF By Corollary 4.1 (p. 95), $A^+A = 1_{\mathbb{C}P\backslash Q}$. On the other hand, A^+ is the embedding, since

$$\frac{1}{|qL|}\sum_{x\in qL} x = \frac{1}{|L|}\sum_{l\in L} ql$$

for q in Q. □

Using the identifications, one may analyze the canonical representation (9.5).

THEOREM 9.2

Let P be a subquasigroup of a quasigroup Q with multiplication group G. Suppose that the permutation representation

$$\lambda : G \to \mathrm{End}_{\mathbb{C}}\mathbb{C}Q$$

of G on Q decomposes as a direct sum (6.21) *of irreducible G-modules. Now consider the canonical representation*

$$\rho_{P\backslash Q} : (\lambda(\mathbb{C}G), +, E_P) \to \mathrm{End}_{\mathbb{C}}\mathbb{C}P\backslash Q; C \mapsto A^+CA \tag{9.20}$$

of the enveloping algebra.

(a) The kernel of $\rho_{P\backslash Q}$ is just the Jacobson radical $J(\lambda(\mathbb{C}G), +, E_P)$ of the enveloping algebra.

(b) The image of $\rho_{P\backslash Q}$ is the semisimple quotient (9.17).

PROOF (b) For $1 \le i \le s$ in the decomposition (6.21), let $p_i : \mathbb{C}Q \to X_i$ be the projection onto the i-th direct summand. By (9.18) and the definition (9.8) of Y_i, this projection restricts to $p_i : \mathbb{C}P\backslash Q \to Y_i$. Let $j_i : X_i \to \mathbb{C}Q$ be the insertion of the i-th summand in (6.21). For an endomorphism C of the $\mathbb{C}$-space $\mathbb{C}Q$, define $C_i = j_iCp_i$. Consider the following commutative diagram:

$$\begin{array}{ccccccc}
\mathbb{C}P\backslash Q & \xrightarrow{A^+} & \mathbb{C}Q & \xrightarrow{C} & \mathbb{C}Q & \xrightarrow{A} & \mathbb{C}P\backslash Q \\
\downarrow{\scriptstyle p_i} & & \downarrow{\scriptstyle p_i} & & \downarrow{\scriptstyle p_i} & & \downarrow{\scriptstyle p_i} \\
Y_i & \xrightarrow{j} & X_i & \xrightarrow{C_i} & X_i & \xrightarrow{E_i} & Y_i
\end{array}$$

(in which j denotes the embedding of Y_i in X_i). The composite across the top row is the image of C under $\rho_{P\backslash Q}$. Now for an element of (9.17) having c_{11} in the i-th summand and zero elsewhere, there is an endomorphism c of the $\mathbb{C}$-space X_i whose first component in the direct sum (9.10) is c_{11}. There is an element C of $\lambda(\mathbb{C}G)$ having c in the i-th summand of (9.7) and zero

elsewhere. Since $C_i = c$, the image of C under $\rho_{P\backslash Q}$ is c_{11}. It follows that the image of $\rho_{P\backslash Q}$ contains (9.16). Conversely, for C in the domain (9.7) of $\rho_{P\backslash Q}$, one has

$$Y_i A^+ C A \subseteq X_i C A \subseteq X_i A = Y_i$$

for $1 \leq i \leq s$, so the image of $\rho_{P\backslash Q}$ is contained in (9.17).
(a) Suppose C lies in the kernel of $\rho_{P\backslash Q}$, so that $A^+CA = 0$. Then

$$E_P C E_P = A A^+ C A A^+ = 0,$$

whence $E_i \pi_i(C) E_i = 0$ for $1 \leq i \leq s$. By Proposition 9.2, it follows that $\lambda_i(C) \in J_i$ for each i. Since

$$J = \bigoplus_{i=1}^{s} J_i \,,$$

one then has $C \in J$. So the kernel of $\rho_{P\backslash Q}$ is contained in the Jacobson radical J. Now (b) above, (9.7), the First Isomorphism Theorem, and Lemma 9.1 imply

$$\begin{aligned} \dim_{\mathbb{C}} \operatorname{Ker} \rho_{P\backslash Q} &= \sum_{i=1}^{s} \chi_i(1)^2 - \sum_{i=1}^{s} \operatorname{Tr}(E_i)^2 \\ &= \dim_{\mathbb{C}} J \,, \end{aligned}$$

so (a) follows. □

Theorem 9.2 may be summarized by saying that the canonical representation (9.5) corestricts to the natural projection of $(\lambda(\mathbb{C}G), +, E_P)$ onto the quotient by its Jacobson radical.

9.4 Commutative actions

This section presents one simple application of Theorems 9.1 and 9.2 — examining sufficient conditions for commutativity of the image of the canonical representation (9.5). As before, it is convenient to set $L = \mathrm{LMlt}_Q P$.

DEFINITION 9.2 *Let P be a subquasigroup of a quasigroup Q. The action of Q on the homogeneous space $P \setminus Q$ is said to be* commutative *if the image* (9.17) *of the representation* (9.20) *is a commutative algebra.*

If the action of Q on $P\backslash Q$ is commutative, then the various transition matrices (4.14) of the homogeneous space $P\backslash Q$ commute mutually.

PROPOSITION 9.6
Suppose that the permutation representation of the multiplication group G of Q on the group homogeneous space $L\backslash G$ given by the relative left multiplication group L of P in Q is multiplicity-free. Then the action of Q on the quasigroup homogeneous space $P\backslash Q$ is commutative.

PROOF The multiplicity-freeness of the action of G on $L\backslash G$ means that each irreducible linear representation of G appears at most once in the permutation representation of G on $L\backslash G$. Then by Lemma 9.1, each multiplicity m_i is 1 or 0. By Theorem 9.1(b), the semisimple quotient $(\lambda(\mathbb{C}G), +, E_P)/J$ is commutative. Theorem 9.2(b) then shows that the action of Q on $P\backslash Q$ is commutative. □

COROLLARY 9.3
Suppose that P is a singleton subquasigroup $\{e\}$ whose relative left multiplication group L in Q is the stabilizer G_e of e in G. Then the action of Q on $P\backslash Q$ is commutative.

PROOF The action of G on $G_e \setminus G$, namely the action of G on Q, is multiplicity free. □

One instance of the corollary occurs for the singleton subquasigroup $\{0\}$ of the quasigroup $(\mathbb{Z}/n\mathbb{Z}, -)$ of integers modulo n under subtraction (compare Example 2.2 on p.37). For a fairly general class of quasigroup actions to which Corollary 9.3 applies, let $(Q, +, \cdot)$ be a finite unital ring. Suppose that r is an invertible element of Q for which $1 - r$ is a power of r. Define a quasigroup multiplication on Q by

$$x * y = x(1 - r) + yr.$$

Many examples of such quasigroups Q or $(Q, *)$ are described in [28, §II.5]. They are idempotent, entropic, and thus distributive (compare Exercise 3 in Chapter 2).

PROPOSITION 9.7
The singleton $P = \{0\}$ is a subquasigroup of the quasigroup Q or $(Q, *)$. Then the action of Q on $P\backslash Q$ is commutative.

PROOF By Theorem 3.5 (p.76), the multiplication group G of Q is the split extension of the abelian translation group $(Q, +)$ by the subgroup $\langle r\rangle$ of the group of units of $(Q, +, \cdot)$ generated by r. Then the stabilizer G_0 of 0 in G is $\langle r\rangle$. However, the generating set $\{L_Q(p) \mid p \in P\}$ of the relative left multiplication group L of P in Q is just $\{r\}$. Thus L coincides with G_0, and Corollary 9.3 shows that the action of Q on $P\backslash Q$ is commutative. □

9.5 Faithful homogeneous spaces

THEOREM 9.3
Let P be a subquasigroup of a finite quasigroup Q. Then the map

$$\rho_{P\backslash Q} : \mathrm{End}_{\mathbb{C}G}\mathbb{C}Q \to \mathrm{End}\mathbb{C}P\backslash Q\,;\ B \mapsto A_P^+ B A_P \tag{9.21}$$

is a homomorphism of $\mathbb{C}$-algebras.

PROOF Consider two elements B_1, B_2 of $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q$. The definition (9.21) gives

$$\rho_{P\backslash Q}(B_1)\rho_{P\backslash Q}(B_2) = A_P^+ B_1 A_P A_P^+ B_2 A_P\ . \tag{9.22}$$

By Proposition 9.1, the central product $A_P A_P^+$ of the right-hand side of (9.22) lies in $\lambda(\mathbb{C}G)$, and so commutes with elements of $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q$ such as B_2. Moreover, one has $A_P A_P^+ A_P = A_P$ as part (4.2) of the specification of the pseudoinverse A_P^+ of A_P. The right-hand side of (9.22) thus reduces to $\rho_{P\backslash Q}(B_1 B_2)$, as required to show that (9.21) gives a monoid homomorphism. □

DEFINITION 9.3 *Let P be a subquasigroup of a finite quasigroup Q. The homogeneous space $P\backslash Q$ is said to be* faithful *if the corresponding map $\rho_{P\backslash Q}$ of* (9.21) *injects.*

PROPOSITION 9.8
Let P be a subgroup of a finite group Q. Then the homogeneous space $P\backslash Q$ yields a faithful transitive permutation representation of Q if and only if the homogeneous space is faithful in the quasigroup sense of Definition 9.3.

PROOF Suppose that $P\backslash Q$ yields a transitive permutation representation which is not faithful. Let K be a nonidentity group conjugacy class of Q contained in the kernel of the group permutation representation. Define the element

$$C = \sum_{q \in K} R_Q(q)$$

of $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q$ — compare (6.15). Then $\rho_{P\backslash Q}(C)$ is a multiple of the identity in $\mathrm{End}\mathbb{C}P\backslash Q$, so that $\rho_{P\backslash Q}$ cannot inject.

On the other hand, if $P\backslash Q$ does yield a faithful transitive permutation representation, then the permutation matrices $A_P^+ R_Q(q) A_P$ of the elements q of Q afford a faithful linear representation of the complex group algebra of

Q. In this case the map $\rho_{P\backslash Q}$, as the restriction of the linear representation to the center of the group algebra, certainly injects. □

REMARK 9.1 As noted in the proof of Proposition 9.8, a homogeneous space $P\backslash Q$ over a finite group Q is faithful (if and) only if the corresponding Markov matrices (4.14) of different group elements differ. In the nonassociative quasigroup case, a homogeneous space $P\backslash Q$ may be faithful in the sense of Definition 9.3, and yet have $R_{P\backslash Q}(q_1) = R_{P\backslash Q}(q_2)$ for distinct elements q_1, q_2 of Q. For instance, in the example Q of Section 9.8 below, the homogeneous space $0\backslash Q$ is faithful, but $R_{0\backslash Q}(1) = R_{0\backslash Q}(3)$ according to (9.25). □

9.6 Characters of homogeneous spaces

DEFINITION 9.4 *Let P be a subquasigroup of a finite quasigroup Q. Then the* permutation character *(or just* character*) of the homogeneous space $P\backslash Q$ is the class function $\pi_{P\backslash Q} : Q \times Q \to \mathbb{C}$ taking the value*

$$n_i^{-1} \operatorname{Tr}(A_P^+ A_i A_P) \tag{9.23}$$

on each member of the i-th quasigroup conjugacy class C_i (for $1 \leq i \leq s$), the matrix A_i being the incidence matrix of the subset C_i of $Q \times Q$.

Example 9.1
The permutation character of the regular space $\varnothing\backslash Q$ of a quasigroup Q is the *regular character* π_Q, taking the value $|Q|$ on the diagonal conjugacy class $C_1 = \widehat{Q}$, and zero elsewhere. □

In order to verify the consistency of Definition 9.4 with the usual definition of a permutation character in the group case, recall that each quasigroup class function $\theta : Q \times Q \to \mathbb{C}$ over a group Q determines a corresponding group class function $\theta' : Q \to \mathbb{C}; q \mapsto \theta(1, q)$.

PROPOSITION 9.9
Let P be a subgroup of a finite group Q. Then $\pi'_{P\backslash Q}$ is the permutation character of the transitive permutation representation of Q on $P\backslash Q$.

PROOF For each element q of Q, the value of the permutation character on q is the trace of the permutation matrix $A_P^+ R_Q(q) A_P$. For each of the n_i

elements of the i-th group conjugacy class of Q, these traces remain constant. Thus the value of the permutation character at an element q of the i-th group conjugacy class K_i may be written as

$$n_i^{-1} \sum_{q \in K_i} \mathrm{Tr}\big(A_P^+ R_Q(q) A_P\big) \,. \tag{9.24}$$

Since the incidence matrix of the i-th quasigroup conjugacy class C_i is just $\sum_{q \in K_i} R_Q(q)$, the quantity (9.24) agrees with (9.23). Finally, note that if q lies in the i-th group conjugacy class, then $(1, q)$ lies in the i-th quasigroup conjugacy class, as required to complete the proof of the proposition. □

REMARK 9.2 In the context of Proposition 9.9, the permutation character of $P\backslash Q$ is obtained by inducing the principal character on the subgroup P up to the full group Q. For a subquasigroup P of a nonassociative quasigroup Q, however, it need no longer be true that the permutation character of $P\backslash Q$ is obtained in this way (using the general quasigroup induction procedure discussed in Section 7.4). In the example Q of Section 9.8 below, for instance, the principal character on the subquasigroup $\{0\}$ induces up to the regular character π_4 on Q, and this of course differs from the permutation character π_3 of the homogeneous space $0\backslash Q$. On the other hand, the character π_2 of the homogeneous space $\{0, 2\}\backslash Q$ *is* obtained by inducing up the principal character on the subquasigroup $\{0, 2\}$. □

9.7 General permutation characters

For the image of a homogeneous space $P\backslash Q$ given by a surjective function with incidence matrix F, one may extend Definition 9.4 by assigning value

$$n_i^{-1} \,\mathrm{Tr}(F^+ A_P^+ A_i A_P F)$$

to each element of the i-th quasigroup conjugacy class C_i. The *permutation character* π_X of a general permutation representation X of Q is then defined to be the sum of the characters of its orbits. By Corollary 5.7 (p. 122) and Proposition 9.9, the definition is consistent with the usual definition for groups. The following results illustrate the use of these general quasigroup permutation characters.

PROPOSITION 9.10

Let X be a permutation representation of a finite quasigroup Q. Then the cardinality $|X|$ of the set X is the dimension of the permutation character π_X of X.

PROOF It suffices to assume that X is the image of a homogeneous space $P\backslash Q$ under a surjective intertwining $\varphi : P\backslash Q \to X$ with incidence matrix F. In this case, two applications of Corollary 4.1 (p. 95) give the dimension of π_X as

$$\begin{aligned}\mathrm{Tr}(F^+ A_P^+ A_P F) &= \mathrm{Tr}(F^+ I_{P\backslash Q} F)\\ &= \mathrm{Tr}(F^+ F)\\ &= \mathrm{Tr}(I_X)\\ &= |X|\,,\end{aligned}$$

proving the proposition. □

THEOREM 9.4
Let X be a permutation representation of a finite quasigroup Q. Then the number of orbits of X is given by the multiplicity of the principal character ψ_1 of Q in the permutation character π_X of X.

PROOF It suffices to show that ψ_1 occurs with multiplicity 1 in the character π of the image of a homogeneous space $P\backslash Q$ under a surjective intertwining with incidence matrix F. Indeed, one has

$$\begin{aligned}n^2\langle \pi, \psi_1\rangle &= \pi * \psi_1(\widehat{Q})\\ &= \sum_{x\in Q}\sum_{y\in Q} \pi(x,y)\psi_1(y,x)\\ &= \sum_{x\in Q}\sum_{y\in Q} \pi(x,y)\\ &= n\sum_{i=1}^{s} \mathrm{Tr}(F^+ A_P^+ A_i A_P F)\\ &= n\mathrm{Tr}(F^+ A_P^+ J A_P F)\\ &= n^2\,,\end{aligned}$$

the last equation following by the quasigroup version of Burnside's Lemma (Theorem 5.9, p. 134). Thus $\langle \pi, \phi_1\rangle = 1$, as required. □

9.8 The Ising model

Consider the quasigroup $Q = (\mathbb{Z}/4\mathbb{Z}, -)$ of integers modulo 4 under subtraction. Its subquasigroups Q, $\{0,2\}$, $\{0\}$, and $\varnothing$ yield homogeneous spaces

with $1, 2, 3$, and 4 elements, respectively. The 1-, 2-, and 4-element spaces are quite analogous to the homogeneous spaces of the group $\mathbb{Z}/4\mathbb{Z}$: in particular, the corresponding action matrices (4.14) are all permutation matrices. On the other hand, the 3-element homogeneous space $0\backslash Q$ exhibits stochasticity. The orbits of the relative left multiplication group of $\{0\}$ in Q are $\{0\}$, $\{1, 3\}$ and $\{2\}$, yielding

$$A_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

as the corresponding incidence matrix. The pseudoinverse of A_0 is the matrix

$$A_0^+ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 1 & 0 \end{bmatrix} \ .$$

From (4.14), one then obtains

$$R_{0\backslash Q}(1) = R_{0\backslash Q}(3) = \begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \end{bmatrix} \tag{9.25}$$

and

$$R_{0\backslash Q}(2) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \ ,$$

while $R_{0\backslash Q}(0)$ is the 3×3 identity matrix.

$(\mathbb{Z}/4\mathbb{Z}, -)$	C_1	C_2	C_3
ψ_1	1	1	1
ψ_2	1	1	-1
ψ_3	$\sqrt{2}$	$-\sqrt{2}$	0
$\psi_1 = \pi_1$	1	1	1
$\psi_1 + \psi_2 = \pi_2$	2	2	0
$\psi_1 + \psi_2 + \psi_3/\sqrt{2} = \pi_3$	3	1	0
$\psi_1 + \psi_2 + \psi_3 \cdot \sqrt{2} = \pi_4$	4	0	0

FIGURE 9.1: Basic and permutation characters of $(\mathbb{Z}/4\mathbb{Z}, -)$.

Figure 9.1 shows the character table of $(\mathbb{Z}/4\mathbb{Z}, -)$ and the permutation characters of its homogeneous spaces. The character table is determined by Theorem 7.10 (p. 191). The respective permutation characters are indexed by the cardinalities of the corresponding spaces. They are exhibited as linear combinations of the basic characters ψ_1, ψ_2, ψ_3. Note that for $1 \leq r \leq 4$, the dimension of the permutation character π_r is the cardinality r of the corresponding homogeneous space, in accordance with Proposition 9.10. Also, the principal character ψ_1 occurs exactly once in each permutation character, as described by Theorem 9.4. For the decomposition of the regular character π_4, compare Exercise 4. From Figure 9.1, it may be seen that the inequivalent permutation representations

$$\{0, 2\}\backslash Q + \varnothing\backslash Q$$

and

$$0\backslash Q + 0\backslash Q$$

have the same permutation character $\pi_2 + \pi_4 = 2\pi_3$.

REMARK 9.3 Consider the conformal field theory describing the scaling limit of the Ising model at the critical point (compare Ex. 5.2.12 of [26] or [109]). This theory has three physical representations

$$\rho_0, \rho_1, \rho_{1/2}$$

with respective statistical dimensions

$$1, 1, \sqrt{2}$$

(Ex. 11.3.22 of [26] or (1.57) of [109]). These statistical dimensions are the dimensions of the basic characters ψ_1, ψ_2, and ψ_3 of $(\mathbb{Z}/4\mathbb{Z}, -)$. Now the centralizer ring of $(\mathbb{Z}/4\mathbb{Z}, -)$ yields the fusion rules of the conformal field theory under the assignments

$$\rho_0 \mapsto A_1,\ \rho_1 \mapsto A_2,\ \rho_{1/2} \mapsto A_3/\sqrt{2}$$

of physical representations to incidence matrices of quasigroup conjugacy classes. It is then of interest to note that the Markov matrices $R_{0\backslash Q}(1)$ and $R_{0\backslash Q}(3)$ in the faithful permutation representation $0\backslash Q$ of $Q = (\mathbb{Z}/4\mathbb{Z}, -)$ have exactly the stochasticity of the sites of the Ising model: a uniform two-way split between "spin up" and "spin down." □

9.9 Exercises

1. Show that a quasigroup is abelian if and only if its actions are all commutative.

2. (a) Show that each 2-element homogeneous space affords a commutative action.

   (b) Give an example of a 3-element homogeneous space which does not afford a commutative action.

3. Verify the claim of Example 9.1.

4. For a finite, nonempty quasigroup Q, show that the regular character decomposes as the sum

$$\pi_Q = \sum_{i=1}^{s} \psi_{i1}\psi_i$$

   of multiples of basic characters.

5. For a finite quasigroup Q, consider finite Q-sets X and Y.

   (a) If Q is a group, show that $\pi_{X\times Y} = \pi_X\pi_Y$.

   (b) Give an example of Q, X, Y for which $\pi_{X\times Y} \neq \pi_X\pi_Y$.

6. Let Q be a finite group.

   (a) For finite Q-sets X and Y, show that $\langle \pi_X, \pi_Y\rangle$ is the number of orbits of Q on $X \times Y$.

   (b) For a transitive Q-set X, show that $\langle \pi_X, \pi_X\rangle$ is the number of orbitals of Q on X.

7. Let Q be a finite quasigroup. Show that if two finite Q-sets X and Y are isomorphic, then $\pi_X = \pi_Y$. Conclude that the map

$$A^+(Q) \to \mathbb{C}\mathrm{Cl}(Q); [X] \mapsto \pi_X\,, \tag{9.26}$$

   taking an isomorphism class of permutation representations to the permutation character of a representative, is well defined.

8. Let Q be a finite group, with Burnside algebra $A(Q)$ and algebra $\mathbb{C}\mathrm{Cl}(Q)$ of class functions. Consider the rational linear extension

$$p : A(Q) \to \mathbb{C}\mathrm{Cl}(Q)$$

   of the map (9.26). Show that p is an algebra homomorphism.

9. Consider the Burnside algebra $A(\mathbb{Z}/4\mathbb{Z}, -)$ and the class function algebra $\mathbb{C}\mathrm{Cl}(\mathbb{Z}/4\mathbb{Z}, -)$ for the quasigroup of integers modulo 4 under subtraction. Let

$$p : A(\mathbb{Z}/4\mathbb{Z}, -) \to \mathbb{C}\mathrm{Cl}(\mathbb{Z}/4\mathbb{Z}, -)$$

   be the rational linear extension of the map (9.26).

(a) Determine the kernel of the rational linear map p.

(b) For what algebra structures on $A(\mathbb{Z}/4\mathbb{Z}, -)$ and $\mathbb{C}\mathrm{Cl}(\mathbb{Z}/4\mathbb{Z}, -)$ does p provide a homomorphism?

10. Show that each class function on $(\mathbb{Z}/4\mathbb{Z}, -)$ may be expressed as a complex linear combination of permutation characters.

11. Let Q be a 3-element quasigroup without idempotent elements.

(a) Show that the only homogeneous spaces are trivial or regular.

(b) Show that the nontrivial basic characters cannot be expressed as a complex linear combination of permutation characters.

12. Let Q be a finite rank 2 quasigroup. Show that each class function on Q can be expressed as a complex linear combination of permutation characters.

13. Let X be a permutation representation of a finite quasigroup Q. The action is said to be 2-*transitive* if

$$\pi_X = \psi_1 + \psi_i$$

for a nonprincipal basic character ψ_i of Q.

(a) Show that a 2-transitive action is transitive.

(b) If Q is a group, show that a permutation representation X of Q is 2-transitive if and only if Q acts transitively on the diversity relation $X^2 \setminus \widehat{X}$ of X. (Thus the quasigroup-theoretic definition of 2-transitivity generalizes the standard group-theoretic definition.)

14. Let Q be a finite quasigroup. Show that a transitive permutation representation X is 2-transitive if and only if $\langle \pi_X, \pi_X \rangle_Q = 2$.

15. Let Q be a rank 2 quasigroup of finite order n. Let X be a transitive permutation representation of Q, with $|X| = r$.

(a) Show that the permutation character of X is

$$\pi_X = \psi_1 + \frac{r-1}{\sqrt{n-1}} \cdot \psi_2 \,.$$

(b) Conclude that X is 2-transitive if and only if

$$n = 1 + (r-1)^2 \,.$$

16. Let P be a right Lagrangean subquasigroup of a rank 2 quasigroup Q. If the homogeneous space $P\backslash Q$ is 2-transitive, show that Q is a cyclic group of order 2.

17. [121] Let Q be a group of permutations on a homogeneous space $P\backslash Q$ of finite order n. Let S be a subset of Q of order n.

    (a) Show that S is sharply transitive if and only if

    $$\sum_{q\in S} R_{P\backslash Q}(q) = J_n\,.$$

    (b) Show that S is sharply transitive if and only if

    $$\psi'\Big(\sum_{q\in S} q\Big) = 0$$

    for each nonprincipal basic summand ψ of the permutation character $\pi_{P\backslash Q}$.

    (c) Let N be a subgroup of Q such that

    $$\pi_{P\backslash Q} = \pi_{N\backslash Q} + \theta$$

    for a sum θ of nonnegative integer multiples of basic characters of Q. If S is sharply transitive, consider the equation

    $$\sum_{q\in S} R_{N\backslash Q}(q) = \frac{nJ}{|N\backslash Q|}$$

    to show that $|N\backslash Q|$ divides n.

18. Let $Q = S_r$ for an even integer $r > 4$. In the natural representation of S_r, let N be the stabilizer of a point, and let P be the stabilizer of a 2-element set of points. Note that $|N\backslash Q|$ does not divide

    $$n = \frac{r(r-1)}{2}\,.$$

    Show that there are basic characters ψ_2, ψ_3 of Q such that

    $$\pi_{N\backslash Q} = \psi_1 + \psi_2$$

    and

    $$\pi_{P\backslash Q} = \psi_1 + \psi_2 + \psi_3\,.$$

    Conclude that there are no sharply transitive subsets in the permutation group $S_r^{[2]}$ of Proposition 8.3 (p. 202).

9.10 Problems

1. For which finite quasigroups Q can each class function be expressed as a complex linear combination of permutation characters?

2. For a finite quasigroup Q, consider the rational linear extension

$$p : A(Q) \to \mathbb{C}\mathrm{Cl}(Q)$$

of the map $[X] \mapsto \pi_X$, taking an isomorphism class of permutation representations to the permutation character of a representative (compare Exercises 7 through 9). Characterize those finite quasigroups Q for which p is an algebra homomorphism.

3. Consider a subquasigroup P of a finite quasigroup Q. Under what conditions is the permutation character $\pi_{P\backslash Q}$ of the quasigroup homogeneous space $P\backslash Q$ obtained by induction from the principal character on the subquasigroup P? (Compare Remark 9.2.)

9.11 Notes

Section 9.1

The results of the first four sections appeared originally in [160].

Section 9.5

Most of the results in this and the subsequent sections are taken from [96], with the exception of Example 9.1 and Proposition 9.10.

Chapter 10

MODULES

This chapter provides an introduction to quasigroup module theory. Since matrix multiplication is associative, naive attempts to extend group module theory are doomed to failure. However, as described in Section 10.1, a module over a group Q yields a split extension, which may be characterized as an abelian group in the slice category of groups over Q. The most general definition of a module over a quasigroup Q is thus given in Section 10.2 as an abelian group in the slice category $\mathbf{Q}/Q$ of quasigroups over Q. An alternative characterization in terms of self-centralizing congruences is also presented. In particular, the central piques of Chapter 3 emerge as modules over the singleton quasigroup (Exercise 8). In Section 10.3, the Fundamental Theorem 10.1 of Quasigroup Representations identifies quasigroup modules as being equivalent to modules over stabilizers in the universal multiplication group. While these modules are too general to yield specific information about a quasigroup Q, they do provide a framework for the representations in varieties that are the topic of Section 10.5. For a unital commutative ring S, and for a quasigroup Q in a variety $\mathbf{V}$, these representations are defined as S-modules in the slice category $\mathbf{V}/Q$ of $\mathbf{V}$-quasigroups over Q. They are equivalent to modules over a certain quotient of the group S-algebra of stabilizers in the universal multiplication group of Q in $\mathbf{V}$. The quotient is determined by a process of combinatorial partial differentiation of the quasigroup words appearing in the identities defining the variety $\mathbf{V}$. This process is described in Section 10.4. Section 10.6 shows that modules over groups may be recovered as quasigroup modules in the variety of associative quasigroups.

10.1 Abelian groups and slice categories

An abelian group may be described as an object A in the category **Set** of sets and functions, equipped with a zero function

$$0 : A^0 \to A; * \mapsto 0\,,$$

negation function

$$- : A \to A; a \mapsto -a\,,$$

and addition function

$$+ : A^2 \to A; (a, b) \mapsto a + b\,,$$

satisfying the usual identities that may be expressed by commutative diagrams. For example, the identity $-a + a = 0$ corresponds to the commuting of the diagram

$$\begin{array}{ccc} A & \xrightarrow{(-,1)} & A^2 \\ \downarrow & & \downarrow{\scriptstyle +} \\ A^0 & \xrightarrow[0]{} & A \end{array} \tag{10.1}$$

in the category of sets. More generally, let $\mathcal{C}$ be a category with finite products. Then an *abelian group in the category* $\mathcal{C}$ is an object A of $\mathcal{C}$, equipped with $\mathcal{C}$-morphisms

$$\begin{aligned} &0 : A^0 \to A \ \ (\textit{zero}), \\ &- : A \to A \ \ (\textit{negation}), \text{ and} \\ &+ : A^2 \to A \ \ (\textit{addition}), \end{aligned}$$

such that all the diagrams representing abelian group identities, like (10.1), commute when interpreted in $\mathcal{C}$.

Now let Q be an object of a category $\mathcal{C}$. The *slice category* "$\mathcal{C}$ over Q" or $\mathcal{C}/Q$ has the $\mathcal{C}$-morphisms $p : E \to Q$ with codomain Q as its objects. There is a $\mathcal{C}/Q$-morphism

$$f : (p_1 : E_1 \to Q) \longrightarrow (p_2 : E_2 \to Q) \tag{10.2}$$

precisely when there is a $\mathcal{C}$-morphism

$$f : E_1 \to E_2 \tag{10.3}$$

such that the diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{f} & E_2 \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle p_2} \\ Q & \xrightarrow[1_Q]{} & Q \end{array}$$

commutes in $\mathcal{C}$. It is often convenient to describe a slice morphism (10.2) simply by the corresponding morphism (10.3) in the base category. If the original category $\mathcal{C}$ has pullbacks, then the slice category $\mathcal{C}/Q$ has finite products. The empty product or terminal object is the identity $1_Q : Q \to Q$ on Q in $\mathcal{C}$, while the product of two objects $p_i : E_i \to Q$ is the pullback object $E_1 \times_Q E_2$ in $\mathcal{C}$,

equipped with the $\mathcal{C}$-morphism to Q given by either path through the pullback diagram

$$\begin{array}{ccc} E_1 \times_Q E_2 & \xrightarrow{\pi_2} & E_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle p_2} \\ E_1 & \xrightarrow[p_1]{} & Q \end{array} \tag{10.4}$$

in $\mathcal{C}$. The projections of the product are given by the π_i from (10.4).

Now let Q be a group, and let M be a right Q-module. Recall that the split extension $E = Q \ltimes M$ is the set $Q \times M$ equipped with the product

$$(q_1, m_1)(q_2, m_2) = (q_1 q_2, m_1 q_2 + m_2)\,. \tag{10.5}$$

The split extension comes equipped with the projection

$$p : E \to Q; (q, m) \mapsto q \tag{10.6}$$

and the insertion η_Q or

$$\eta : Q \to E; q \mapsto (q, 0), \tag{10.7}$$

both of which are group homomorphisms. For a fixed element q of Q, it is convenient to think of the preimage

$$p^{-1}\{q\} = \{(q, m) \mid m \in M\}$$

as a neighborhood of q^η in E, consisting of a local copy M_q of the set M. The conjugation action of an element q^η on the normal subgroup M_1 of E is given by

$$(q, 0)\backslash(1, m)(q, 0) = (mq, 0), \tag{10.8}$$

thereby reflecting the action of Q on the module M.

Let **Gp** be the category of group homomorphisms. Then the projection (10.6) becomes an object of the slice category $\mathbf{Gp}/Q$. The pullback

$$E \times_Q E = \left\{ \big((q, m_1), (q, m_2)\big) \;\middle|\; q \in Q, m_1, m_2 \in M \right\} \tag{10.9}$$

in **Gp** is the domain of a local addition

$$+_Q : E \times_Q E \to E; \big((q, m_1), (q, m_2)\big) \mapsto (q, m_1 + m_2)$$

that makes (10.6) an abelian group in the category $\mathbf{Gp}/Q$, with (10.7) as zero morphism. Conversely, let $p : E \to Q$ be an abelian group in the slice category $\mathbf{Gp}/Q$. Let M be the group kernel $p^{-1}\{1_Q\}$ of p. Then in analogy with (10.8), each element q of Q acts on M by

$$q : m \mapsto q^\eta \backslash m q^\eta,$$

making M a right Q-module. This construction, along with the split extension, shows that Q-modules are equivalent to abelian groups in the slice category $\mathbf{Gp}/Q$ of groups over Q.

10.2 Quasigroup modules

Section 10.1 related modules over a group Q to abelian groups in the category of groups over Q. For a general quasigroup Q, one thus defines a Q-*module* or *module* over Q to be an abelian group object in the category $\mathbf{Q}/Q$ of quasigroups over Q. Since the category $\mathbf{Q}$ has pullbacks, products in the slice category are given by (10.4). Then a Q-*morphism* or Q-*module homomorphism* $f : E_1 \to E_2$ between Q-modules is a $\mathbf{Q}/Q$-morphism such that $0f = 0$, $-f = f-$, and $+f = (f \times_Q f)+$. The category $\mathbb{Z} \otimes \mathbf{Q}/Q$ has Q-modules as its objects and Q-morphisms between them as its morphisms.

In this section, Q-modules will be identified with self-centralizing quasigroup congruences V whose quotient is Q. First, let $p : E \to Q$ be an abelian group in the slice category $\mathbf{Q}/Q$. Note that for each object $D \to Q$ of the slice category, the set $\mathbf{Q}/Q(D, E)$ of slice category morphisms to E inherits an abelian group structure from $E \to Q$. The zero element is the composite

$$D \to Q \xrightarrow{0} E\,.$$

Negation of $f : D \to E$ is the composite

$$-f : D \xrightarrow{f} E \xrightarrow{-} E\,.$$

The sum of two morphisms $f : D \to E$ and $f' : D \to E$ is the composite

$$f + f' : D \xrightarrow{(f,f')} E \times_Q E \xrightarrow{+} E\,.$$

Verification of the various identities is straightforward (Exercise 4). In particular, $\mathbf{Q}/Q(1_Q : Q \to Q, p : E \to Q)$ is an abelian group. Since the zero element $0_Q : Q \to E$ of this abelian group gives a commuting diagram

$$\begin{array}{ccc} Q & \xrightarrow{0_Q} & E \\ {\scriptstyle 1_Q}\downarrow & & \downarrow{\scriptstyle p} \\ Q & \xrightarrow[1_Q]{} & Q \end{array} \tag{10.10}$$

it follows that $p : E \to Q$ is an epimorphism in $\mathbf{Q}$ (Exercise 3). Its kernel is the congruence $V = E \times_Q E$ on E, and the quotient E^V, being naturally isomorphic to the quasigroup Q, may be identified with it. Now there is a $\mathbf{Q}/Q$-morphism $- : V \to E$ called *subtraction* defined, as usual for abelian groups, by the composite

$$E \times_Q E \xrightarrow{(1,-)} E \times_Q E \xrightarrow{+} E\,.$$

The kernel of $- : V \to E$ is a congruence W on V.

PROPOSITION 10.1
The congruence W on V is the centering congruence $(V|V)$ by which V centralizes itself.

PROOF The conditions of Definition 3.1 must be checked.
(C0):

$$\begin{aligned}&(x,y)W(x',y')\\&\quad\Rightarrow x-y=x'-y'\\&\quad\Rightarrow x^V=(x-y)^V=(x'-y')^V=x'^V\\&\quad\Rightarrow (x,x')\in V\,.\end{aligned}$$

(C1): For (x,y) in V, the map

$$\pi:(x,y)^W\to x^V;(x',y')\mapsto x'$$

has the two-sided inverse

$$x'\mapsto \big(x',x'-(x-y)\big)\,.$$

(RR):

$$\begin{aligned}&(x,y)\in V\\&\quad\Rightarrow x-x=x^V0_Q=y^V0_Q=y-y\\&\quad\Rightarrow (x,x)W(y,y)\,.\end{aligned}$$

(RS):

$$\begin{aligned}&(x_1,x_2)W(y_1,y_2)\\&\quad\Rightarrow x_1-x_2=y_1-y_2\\&\quad\Rightarrow x_2-x_1=y_2-y_1\\&\quad\Rightarrow (x_2,x_1)W(y_2,y_1)\,.\end{aligned}$$

(RT):

$$\begin{aligned}&(x_1,x_2)W(y_1,y_2)\text{ and}\\&\qquad(x_2,x_3)W(y_2,y_3)\\&\Rightarrow x_1-x_2=y_1-y_2\text{ and}\\&\qquad x_2-x_3=y_2-y_3\\&\Rightarrow x_1-x_3=y_1-y_3\\&\Rightarrow (x_1,x_3)W(y_1,y_3)\,.\end{aligned}$$

□

Proposition 10.1 has a number of immediate comsequences.

COROLLARY 10.1

(a) *For (x, y) in V, one has $(x^V 0_Q, x)W(y, x+y)$.*

(b) *The category of Q-modules is a full subcategory of the slice category $\mathbf{Q}/Q$. In other words, every slice category morphism between Q-modules is a Q-morphism.*

PROOF (a): By reflexivity,

$$(x^V 0_Q, x)W(x^V 0_Q, x)\,.$$

By (RR),

$$(x^V 0_Q, x^V 0_Q)W(y, y)\,.$$

Adding,

$$(x^V 0_Q, x)W(y, x+y)\,.$$

(b): Suppose $f : E \to E'$ is a $\mathbf{Q}/Q$-morphism between abelian groups in $\mathbf{Q}/Q$. Using the operation P of (2.27), (a) and Proposition 3.4 imply

$$x + y = (x, x^V 0_Q, y)P\,. \tag{10.11}$$

Then since f is a quasigroup homomorphism,

$$\begin{aligned}(x+y)f &= (x, x^V 0_Q, y)Pf\\ &= (xf, x^V 0_Q f, yf)P\\ &= xf + yf\,,\end{aligned}$$

the latter equation holding by (10.11) in E'. □

One may now show the equivalence of Q-modules with self-centralizing quasigroup congruences whose quotient is Q. The first result summarizes the foregoing, and serves to recover a Q-module from the self-centralizing congruence it contains.

PROPOSITION 10.2

Let $p : E \to Q$ be an abelian group in the slice category $\mathbf{Q}/Q$. Then $p : E \to Q$ is an epimorphism in $\mathbf{Q}$ whose kernel congruence V is self-centralizing with centering congruence $(V|V)$. Identifying E^V with Q via the natural isomorphism, the object

$$V^{(V|V)} \to E^V; (x, y)^{(V|V)} \mapsto x^V$$

of $\mathbf{Q}/Q$ is isomorphic in $\mathbf{Q}/Q$ to $p : E \to Q$.

PROOF There are mutually inverse $\mathbf{Q}/Q$-morphisms

$$E \to V^{(V|V)}; x \mapsto (x, x^V 0_Q)^{(V|V)}$$

and

$$V^{(V|V)} \to E; (x, y)^{(V|V)} \mapsto x - y.$$

□

The converse of Proposition 10.2 constructs Q-modules from self-centralizing congruences whose quotient is (isomorphic to) Q.

PROPOSITION 10.3
Suppose that a quasigroup E has a self-centralizing congruence V with centering congruence $(V|V)$. Suppose that the quotient E^V is identified with a quasigroup Q. Then

$$V^{(V|V)} \to E^V; (x, y)^{(V|V)} \mapsto x^V$$

is an abelian group in $\mathbf{Q}/Q$.

PROOF There are well-defined $\mathbf{Q}/Q$-morphisms

$$0 : E^V \to V^{(V|V)}; x^V \mapsto (x, x)^{(V|V)}, \tag{10.12}$$

$$- : V^{(V|V)} \to V^{(V|V)}; (x, y)^{(V|V)} \mapsto (y, x)^{(V|V)} \tag{10.13}$$

and

$$+ : V^{(V|V)} \times_{E^V} V^{(V|V)} \to V^{(V|V)} \tag{10.14}$$

making $V^{(V|V)} \to E^V$ an abelian group in $\mathbf{Q}/Q$. The morphism $+$ is defined by

$$(x, y)^{(V|V)} + (x', y')^{(V|V)} = (x, z)^{(V|V)}$$

for elements x, y, x', y' of E in a single congruence class of E, the element z being defined uniquely by the bijection

$$(x', y')^{(V|V)} \to x'^V; (y, z) \mapsto y$$

in the centrality condition (C1) for $(V|V)$ on V. The morphism $+$ is well-defined by (RT). It is straightforward to verify that the morphisms (10.12) through (10.14) furnish an abelian group in the slice category $\mathbf{Q}/Q$ (compare Exercise 5). □

10.3 The Fundamental Theorem

For a quasigroup Q, the previous section identified Q-modules with self-centralizing congruences having Q as quotient. For an element e of Q, the main theorem of this section identifies Q-modules with modules for the universal stabilizer of e in $\mathbf{Q}$.

THEOREM 10.1
(***Fundamental Theorem of Quasigroup Representations***)
Let Q be a quasigroup with an element e. Let $\widetilde{G}$ be the universal multiplication group $\mathrm{U}(Q;\mathbf{Q})$ of Q in the variety $\mathbf{Q}$ of all quasigroups. Then Q-modules, as abelian groups in the slice category $\mathbf{Q}/Q$, are equivalent to modules over the universal stabilizer $\widetilde{G}_e$.

Suppose that $p : E \to Q$ is an abelian group in $\mathbf{Q}/Q$. The inverse image $M = p^{-1}\{e\}$ forms an abelian group under the restriction of the addition morphism

$$+ : E \times_Q E \to E\,.$$

The zero morphism $0 : Q \to E$ embeds Q in E. By Corollary 2.5 (p. 52), the relative multiplication group $\mathrm{Mlt}_E(Q)$ is a quotient of $\widetilde{G}$. Then $\widetilde{G}$ acts on E via this quotient. The action restricts to an action of the universal stabilizer $\widetilde{G}_e$ on M. As the following lemma shows, the action consists of automorphisms of the abelian group M. Thus the Q-module $p : E \to Q$ yields a $\widetilde{G}_e$-module $M = p^{-1}\{e\}$.

LEMMA 10.1
The universal stabilizer $\widetilde{G}_e$ acts on $M = p^{-1}\{e\}$ as a group of automorphisms.

PROOF Use the notation of Section 2.2 for elements of the universal stabilizer. Let $E(q_1, \ldots, q_n)$ be such an element, with corresponding quasigroup word

$$qE(q_1, \ldots, q_n) = qq_1 \ldots q_n w_E\,.$$

Let m and m' be elements of the abelian group M. Let V be the kernel of p, centered by W as in Proposition 10.2. Now

$$(e, m)\, W\, (m', m + m')$$

by Corollary 10.1(a), while

$$(q_i, q_i)\, W\, (q_i, q_i)$$

for $1 \le i \le n$. Applying the quasigroup word w_E to these relations, and recalling that W is a congruence on V, gives

$$\big(e, mE(q_1, \ldots, q_n)\big)\, W\, \big(m'E(q_1, \ldots, q_n), (m+m')E(q_1, \ldots, q_n)\big)\,.$$

But again by Corollary 10.1(a),

$$\big(e, mE(q_1, \ldots, q_n)\big)\, W\, \big(m'E(q_1, \ldots, q_n), mE(q_1, \ldots, q_n) + m'E(q_1, \ldots, q_n)\big)\,.$$

Property (C1) of W (see Proposition 10.1) yields

$$(m+m')E(q_1, \ldots, q_n) = mE(q_1, \ldots, q_n) + m'E(q_1, \ldots, q_n)\,,$$

so the universal stabilizer element acts as an abelian group automorphism. □

Conversely, for a $\widetilde{G}_e$-module M, a corresponding abelian group $\pi : E \to Q$ in $\mathbf{Q}/Q$ has to be constructed. For each element q of Q, consider the element

$$\rho(e, q) = R(e\backslash e)^{-1} R(e\backslash q)$$

of a transversal to the subgroup $\widetilde{G}_e$ of $\widetilde{G}$. For each element g of $\widetilde{G}$ and q of Q, there is a unique element $s(q, g)$ of $\widetilde{G}_e$ such that

$$s(q, g)\rho(e, qg) = \rho(e, q)g\,. \tag{10.15}$$

In the Cayley diagram, $s(q, g)$ may be represented by the composite path

$$e \xleftarrow{R} e \xrightarrow{R} q \xrightarrow{g} qg \xleftarrow{R} e \xrightarrow{R} e\,. \tag{10.16}$$

Note that

$$s(e, g_e) = g_e \tag{10.17}$$

for g_e in $\widetilde{G}_e$ and

$$s(q, g)s(qg, h) = s(q, gh) \tag{10.18}$$

for $q \in Q$ and $g, h \in G$. Now consider the $\widetilde{G}$-set $E = M \times Q$ with action

$$(m, q)g = \big(ms(q, g), qg\big)\,. \tag{10.19}$$

(The crossed product condition (10.18) guarantees that (10.19) does give a group action — Exercise 6.) Define local abelian group structures on E by

$$(m_1, q) - (m_2, q) = (m_1 - m_2, q) \tag{10.20}$$

for $m_i \in M$ and $q \in Q$. Let $\pi : E \to Q$ be projection onto the second factor. Then a quasigroup structure is defined on E by

$$\begin{cases} a \cdot b = aR(b\pi) + bL(a\pi)\,; \\ a/b = (a - bL(a\pi/b\pi))R(b\pi)^{-1}\,; \\ a\backslash b = (b - aR(a\pi\backslash b\pi))L(a\pi)^{-1}\,. \end{cases} \tag{10.21}$$

With this structure, $\pi : E \to Q$ becomes an abelian group object in the category $\mathbf{Q}/Q$. Note that by (10.17), the $\widetilde{G}_e$-modules M and $\pi^{-1}\{e\}$ are isomorphic.

The proof of the Fundamental Theorem is completed by the following observation.

LEMMA 10.2
A Q-module

$$p : E \to Q$$

is isomorphic to the corresponding

$$\pi : p^{-1}\{e\} \times Q \to Q$$

constructed according to (10.19) *through* (10.21).

PROOF Let V be the kernel congruence of $p : E \to Q$, centered by W. For elements a, b of E, the relations $(ap, a)\, W\, (ap, a)$ and $(bp, bp)\, W\, (b, b)$ yield

$$(ap \cdot bp, a \cdot bp)\, W\, (ap \cdot b, a \cdot b)\,.$$

But by Corollary 10.1(a),

$$(ap \cdot bp, a \cdot bp)\, W\, (ap \cdot b, a \cdot bp + ap \cdot b)\,.$$

Thus

$$a \cdot b = a \cdot bp + ap \cdot b\,,$$

so that

$$p^{-1}\{e\} \times Q \to E; (m, q) \mapsto m\rho(e, q)$$

and

$$E \to p^{-1}\{e\} \times Q; a \mapsto (a\rho(e, ap)^{-1}, ap)$$

are mutually inverse isomorphisms. □

10.4 Differential calculus

The Fundamental Theorem provides a *differentiation* process that may be applied to quasigroup words and identities. Fix a quasigroup Q with element e and universal multiplication group $\widetilde{G} = U(Q; \mathbf{Q})$ in the variety of all quasigroups. The category of $\widetilde{G}_e$-modules is generated by the integral group algebra $\mathbb{Z}\widetilde{G}_e$, considered as a $\widetilde{G}_e$-module. Under the equivalence given by the Fundamental Theorem, the corresponding object is the Q-module $\pi : \mathbb{Z}\widetilde{G}_e \times Q \to Q$.

Using (10.21), the action of a quasigroup word $x_1 \dots x_n w$ on this object is given by

$$(m_1, q_1) \dots (m_n, q_n) w = \Big(\sum_{h=1}^{n} m_h \rho(e, q_h) \frac{\partial w}{\partial x_h} \rho(e, w)^{-1}, q_1 \dots q_n w \Big) \quad (10.22)$$

for certain elements

$$\frac{\partial w}{\partial x_h} = \frac{\partial w}{\partial x_h}(q_1, \dots, q_n) \quad (10.23)$$

of $\mathbb{Z}\widetilde{G}$. Notational conventions similar to those of calculus are employed. The functions

$$\frac{\partial w}{\partial x_h} : Q^n \to \mathbb{Z}\widetilde{G}; (q_1, \dots, q_n) \mapsto \frac{\partial w}{\partial x_h}(q_1, \dots, q_n) \quad (10.24)$$

for $1 \leq h \leq n$ are known as the *partial derivatives* of the quasigroup word $x_1 \dots x_n w$. They are computed inductively using the parsing of the word $x_1 \dots x_n w$. For $xw = x$, (10.22) simply gives

$$\frac{\partial x}{\partial x} = 1 \,. \quad (10.25)$$

More generally, the derivatives of the projection

$$x_1 \dots x_i \dots x_n \pi_i = x_i$$

are given by

$$\frac{\partial \pi_i}{\partial x_j} = \delta_{ij} \,.$$

For $x_1 \dots x_k x_{k+1} \dots x_{k+l} w = x_1 \dots x_k u \cdot x_{k+1} \dots x_{k+l} v$, (10.21) and (10.22) give

$$\begin{aligned}
(m_1,q_1) \dots (m_{k+l}, q_{k+l}) w &= \Big(\sum_{h=1}^{k+l} m_h \rho(e, q_h) \frac{\partial w}{\partial x_h} \rho(q_h, w)^{-1}, w \Big) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1}, u \Big) \cdot \Big(\sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1}, v \Big) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1}, u \Big) R(q_{k+1} \dots q_{k+l} v) \\
&\quad + \Big(\sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1}, q_{k+1} \dots q_{k+l} v \Big) L(q_1 \dots q_k u) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1} s\big(u, R(v)\big) + \\
&\qquad \sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1} s\big(v, L(u)\big), w \Big) \,,
\end{aligned}$$

leading to the *Product Rules*

$$\frac{\partial w}{\partial x_i} = \frac{\partial u}{\partial x_i} R(x_{k+1} \dots x_{k+l} v)$$

for $1 \leq i \leq k$ and

$$\frac{\partial w}{\partial x_j} = \frac{\partial v}{\partial x_j} L(x_1 \dots x_k u)$$

for $k < j \leq k + l$. These may be summarized as

$$\frac{\partial (u \cdot v)}{\partial x_i} = \frac{\partial u}{\partial x_i} R(v)\,; \tag{10.26}$$

$$\frac{\partial (u \cdot v)}{\partial x_j} = \frac{\partial v}{\partial x_j} L(u)\,. \tag{10.27}$$

Note that if there are repeated arguments in the word w, say $q_i = q_j$ with $i \leq k < j$, then $\partial w / \partial x_i$ will include the sum of $\partial (u \cdot v)/\partial x_i$ as given by (10.26) and $\partial (u \cdot v)/\partial x_j$ as given by (10.27).

Example 10.1

The Product Rules give

$$\frac{\partial xy}{\partial x} = R(y)$$

and

$$\frac{\partial xy}{\partial y} = L(x)\,.$$

Thus

$$\frac{\partial x^2}{\partial x} = R(x) + L(x)\,.$$

□

Arguments similar to those used for the Product Rules also yield the *Right Quotient Rules*

$$\frac{\partial (u/v)}{\partial x_i} = \frac{\partial u}{\partial x_i} R(v)^{-1}\,; \tag{10.28}$$

$$\frac{\partial (u/v)}{\partial x_j} = -\frac{\partial v}{\partial x_j} L(u/v) R(v)^{-1}\,; \tag{10.29}$$

and the *Left Quotient Rules*

$$\frac{\partial (u\backslash v)}{\partial x_i} = -\frac{\partial u}{\partial x_i} R(u\backslash v) L(u)^{-1}\,; \tag{10.30}$$

$$\frac{\partial (u\backslash v)}{\partial x_j} = \frac{\partial v}{\partial x_j} L(u)^{-1}\,. \tag{10.31}$$

10.5 Representations in varieties

The Fundamental Theorem 10.1 of Quasigroup Representations shows that general Q-modules are equivalent to $\widetilde{G}_e$-modules. The only influence that Q itself has on these modules is through its cardinality, which determines the ranks of the free groups $\widetilde{G}$ and $\widetilde{G}_e$.

For representations that involve more of the structure of Q, one has to restrict the possibilities. There are two methods for doing this. The first method is to take a subvariety $\mathbf{V}$ of $\mathbf{Q}$ that still contains Q. The smaller the variety $\mathbf{V}$, the more it will reflect Q. By Birkhoff's Theorem B.1, the minimal such variety is the variety $\mathsf{HSP}\{Q\}$ generated by Q. For some quasigroups Q, the universal multiplication group $U(Q;\mathsf{HSP}\{\mathrm{Q}\})$ actually collapses to the combinatorial multiplication group, although for other quasigroups this does not happen [126].

The second method for refining the representation theory is to take a unital commutative ring S other than the ring $\mathbb{Z}$ that gives abelian groups in $\mathbf{V}/Q$, and then consider unital S-modules in $\mathbf{V}/Q$. (Unital S-modules in a category with finite products are abelian groups in the category, equipped with additional morphisms corresponding to scalar multiplications by elements of S. Diagrams corresponding to distributive laws are required to commute, and scalar multiplication by the identity element 1_S is required to act as the identity morphism.) The category of S-modules in $\mathbf{V}/Q$ is written as $S \otimes \mathbf{V}/Q$. This section shows how to describe S-modules in $\mathbf{V}/Q$ as modules over quotients of the group algebra $S\widetilde{G}_e$ of an element stabilizer in the universal multiplication group $\widetilde{G} = U(Q;\mathbf{V})$ of Q in $\mathbf{V}$. The real value of the unrestricted representation theory is then seen to lie in the way it provides a uniform framework within which to study all the various special theories.

Varieties $\mathbf{V}$ of quasigroups are axiomatized, within the variety $\mathbf{Q}$ of all quasigroups, by additional identities $u = v$ between quasigroup words. For example, Steiner triple systems are given by (1.15) and (1.20). Suppose that e is an element of a quasigroup Q lying in the variety $\mathbf{V}$, and that $\widetilde{G} = U(Q;\mathbf{V})$ is the universal multiplication group of Q in $\mathbf{V}$. The partial derivatives (10.24) of a quasigroup word w may then be construed as mapping into the integral group algebra of $U(Q;\mathbf{V})$, rather than $U(Q;\mathbf{Q})$. Suppose that B is a *relative equational basis* for $\mathbf{V}$ in $\mathbf{Q}$, a set of quasigroup identities specifying $\mathbf{V}$ within the variety of all quasigroups. For a general commutative ring S with identity 1_S, let $JS\widetilde{G}_e$ be the two-sided ideal of $S\widetilde{G}_e$ generated by the set of all elements

$$1_S \otimes \rho(e,q_h)\Big(\frac{\partial u}{\partial x_h}(q_1,\ldots,q_n) - \frac{\partial v}{\partial x_h}(q_1,\ldots,q_n)\Big)\rho(e,q_1\ldots q_n u)^{-1} \quad (10.32)$$

for all $q_h \in Q$ and $(u,v) \in B$. Note that since Q lies in $\mathbf{V}$, its elements $q_1\ldots q_n u$ and $q_1\ldots q_n v$ coincide. Let $S\mathbf{V}Q$ be the quotient ring $S\widetilde{G}_e/JS\widetilde{G}_e$. There is then a relativized version of the Fundamental Theorem 10.1.

THEOREM 10.2
(***Fundamental Theorem of Representations in Varieties***)
Let Q be a nonempty quasigroup in a variety $\mathbf{V}$. Then the category $S \otimes \mathbf{V}/Q$ of S-modules in $\mathbf{V}/Q$ is equivalent to the category of modules over the ring $S\mathbf{V}Q$.

PROOF Let M be a unital right $S\mathbf{V}Q$-module. Then M is a right $U(Q;\mathbf{Q})_e$-module via the monoid morphism

$$U(Q;\mathbf{Q})_e \to \widetilde{G}_e \to \mathbb{Z}\widetilde{G}_e \xrightarrow{1_S \otimes} S\widetilde{G}_e \to S\mathbf{V}Q\,. \tag{10.33}$$

Since M is a right $U(Q;\mathbf{Q})_e$-module, the Fundamental Theorem 10.1 furnishes a corresponding Q-module $\pi : M \times Q \to Q$. For each element s of the ring S, define

$$s : M \times Q \to M \times Q; (m,q) \mapsto (ms,q)\,. \tag{10.34}$$

Since the S-action on M commutes with the $\widetilde{Q}_e$-action, the maps (10.34) are $\mathbf{Q}/Q$-morphisms. Furthermore, $\pi : M \times Q \to Q$ becomes an S-module in $\mathbf{Q}/Q$. For each element $u = v$ of the relative equational basis B,

$$\begin{aligned}
&(m_1,q_1)\dots(m_n,q_n)u \\
&\quad = \Big(\sum_{i=1}^{n} m_i \rho(e,q_i)\frac{\partial u}{\partial x_i}\rho(e,q_1\dots q_n u)^{-1}, q_1\dots q_n u\Big) \\
&\quad = \Big(\sum_{i=1}^{n} m_i \rho(e,q_i)\frac{\partial v}{\partial x_i}\rho(e,q_1\dots q_n v)^{-1}, q_1\dots q_n v\Big) \\
&\quad = (m_1,q_1)\dots(m_n,q_n)v\,,
\end{aligned}$$

the central equality holding since M is an $S\mathbf{V}Q$-module, annihilated by the elements (10.32) of $JS\widetilde{G}_e$. Thus $\pi : M \times Q \to Q$ is an S-module in $\mathbf{V}/Q$.

If $E(q_1,\dots,q_n)$ is a generic element of the domain of (10.33), use the same notation for its image in the codomain. Let $qq_1\dots q_n w_E = qE(q_1\dots,q_n)$ be the corresponding quasigroup word. Now suppose that $p : A \to Q$ is an S-module in $\mathbf{V}/Q$. In particular, it is an abelian group in $\mathbf{Q}/Q$. The Fundamental Theorem 10.1 furnishes a corresponding $U(Q;\mathbf{Q})_e$-module $M = p^{-1}\{e\}$. For each element s of S, there is a $\mathbf{Q}/Q$-morphism $s : A \to A$. Then for m in M and $E(q_1,\dots q_n)$ in $U(Q;\mathbf{Q})_e$,

$$\begin{aligned}
&mE(q_1,\dots,q_n)s \\
&\quad = mq_1\dots q_n w_E s \\
&\quad = msq_1 s\dots q_n s w_E \\
&\quad = msq_1\dots q_n w_E \\
&\quad = msE(q_1,\dots,q_n)\,.
\end{aligned}$$

Thus the S-action on M commutes with the $U(Q;\mathbf{Q})_e$-action, whence M is a right $S \otimes \mathbb{Z}U(Q;\mathbf{Q})_e$-module or $SU(Q;\mathbf{Q})_e$-module. Suppose $E(q_1,\ldots,q_n)$ and $F(q_1,\ldots,q_n)$ are elements of $U(Q;\mathbf{Q})_e$ lying in the kernel congruence of the canonical map $r_c : U(Q;\mathbf{Q})_e \to U(Q;\mathbf{V})_e$. Since A is a $\mathbf{V}$-quasigroup containing Q (embedded via 0_Q as always), Corollary 2.5 (p. 52) supplies a group homomorphism $r_A : U(Q;\mathbf{V}) \to \mathrm{Mlt}_A Q$. Then

$$\begin{aligned} mE(q_1,\ldots,q_n) &= mE(q_1,\ldots,q_n)^{r_c r_A} \\ &= mF(q_1,\ldots,q_n)^{r_c r_A} \\ &= mF(q_1,\ldots,q_n) \end{aligned}$$

for each m in M. The $SU(Q;\mathbf{Q})_e$-module M becomes an $S\widetilde{G}_e$-module or $SU(Q;\mathbf{V})_e$-module. Using the categorical equivalence given by the Fundamental Theorem 10.1, the construction of $M \times Q$ recovers the quasigroup A from M up to natural isomorphism. Since A is a $\mathbf{V}$-quasigroup, the elements (10.32) annihilate M, so M is an $S\widetilde{G}_e/JS\widetilde{G}_e$-module or $S\mathbf{V}Q$-module. □

DEFINITION 10.1 *In the context of Theorem 10.2, the* principal bundle *over Q in $\mathbf{V}$ is defined to be the S-module in $\mathbf{V}/Q$ corresponding to the generating $S\mathbf{V}Q$-module $S\mathbf{V}Q$.*

Given a relative equational basis B for a variety $\mathbf{V}$ of quasigroups, and an element e of a quasigroup Q in $\mathbf{V}$, the computation of the ring $S\mathbf{V}Q$ involves determination of the generators (10.32) of the ideal $JS\widetilde{G}_e$. The process is simplified by the observation that in certain cases, these generators will vanish. Consider a quasigroup word $x_1 \ldots x_n w$ written out using infix notation as a well-formed string of symbols

$$(\ ,\ )\ ,x_1\ ,\ldots,\ x_n\ ,\cdot\ ,/\ ,\backslash\ .$$

The argument x_h (for $1 \le h \le n$) is said to *occur uniquely* in w if the symbol x_h appears only once in the string. The following result is readily proved by induction using the Product and Quotient Rules.

LEMMA 10.3
Suppose that an argument x_h of a quasigroup word w occurs uniquely. Then the elemnt $\partial w/\partial x_h$ of $\mathbb{Z}\widetilde{G}$ actually lies in $\widetilde{G}$.

If the argument x_h of w occurs uniquely, then it is further said to *occur above the line* in w if it appears to the left of all the symbols / and to the right of all the symbols \ in the string. For example, x occurs above the line in $(x/y)\cdot z$, in $z\backslash(x/y)$, and in $(t\cdot x)\cdot(y\cdot z)$. The following result is again proved by induction using the Product Rules (10.26), (10.27) and Quotient Rules (10.28), (10.31).

LEMMA 10.4
Suppose that an argument x_h of a quasigroup word w occurs uniquely above the line. Then the function (10.24) *does not depend on q_h.*

PROPOSITION 10.4
Let $u = v$ be an element of a relative equational basis B for a variety $\mathbf{V}$ of quasigroups. Let e be an element of a quasigroup Q in $\mathbf{V}$. If the argument x_h occurs uniquely above the line in both u and v, then the generator (10.32) *of the ideal $JS\widetilde{G}_e$ vanishes.*

PROOF By Lemmas 10.3 and 10.4, the derivatives $\partial u/\partial x_h(q_1, \ldots, q_n)$ and $\partial v/\partial x_h(q_1, \ldots, q_n)$ are elements of $\widetilde{G}$ that do not involve q_h. Further, the equations

$$q_1 \ldots X \ldots q_n u = X\rho(e, q_h)\frac{\partial u}{\partial x_h}(q_1, \ldots, q_n)\rho(e, q_1, \ldots, q_n u)^{-1} \qquad (10.35)$$

and

$$q_1 \ldots X \ldots q_n v = X\rho(e, q_h)\frac{\partial v}{\partial x_h}(q_1, \ldots, q_n)\rho(e, q_1, \ldots, q_n v)^{-1} \qquad (10.36)$$

hold in the coproduct $Q[X]$ of Q in $\mathbf{V}$ with the free $\mathbf{V}$-quasigroup on the singleton $\{X\}$. Since the coproduct $Q[X]$ lies in $\mathbf{V}$, the elements (10.35) and (10.36) coincide. Thus

$$\frac{\partial u}{\partial x_h}(q_1, \ldots, q_n) = \frac{\partial v}{\partial x_h}(q_1, \ldots, q_n)\,,$$

whence the corresponding generator (10.32) vanishes. □

10.6 Group representations

As a first application of the ideas of the preceding section, group representations are recovered within the present scheme. Consider the variety $\mathbf{G}$ of associative quasigroups. A nonempty member Q of $\mathbf{G}$ is just a group. For such a quasigroup Q, take e to be the identity element, selected as $e = x/x$ for any element x of Q. By (2.40), the universal multiplication group $\widetilde{G} = U(Q; \mathbf{G})$ of Q in $\mathbf{G}$ is

$$\{T(x, y) = L(x)^{-1}R(y) \mid x, y \in Q\}$$

(omitting the tildes from the universal right and left multiplications). The stabilizer of the identity element e is generated by (2.45). However, since the

coproduct $Q[X]$ in $\mathbf{G}$ is associative, $R(x,y) = L(x,y) = 1$ for all x, y in Q. Thus there is an isomorphism

$$T_e : Q \to \widetilde{G}_e; x \mapsto T_e(x) = T(x,x) \tag{10.37}$$

from the group Q to the universal stabilizer $\widetilde{G}_e$. Define quasigroup words

$$x_1x_2x_3u = x_1x_2 \cdot x_3$$

and

$$x_1x_2x_3v = x_1 \cdot x_2x_3\,.$$

Then $B = \{(u,v)\}$ forms a relative equational basis for $\mathbf{G}$ in $\mathbf{Q}$. Since each argument x_h occurs uniquely above the line in both u and v, Proposition 10.4 shows that $J\mathbb{Z}\widetilde{G}_e = 0$. The Fundamental Theorem 10.2 of Representations in Varieties then states that a Q-module in $\mathbf{G}$ is equivalent to a unital right $\mathbb{Z}\widetilde{G}_e$-module. By the isomorphism (10.37), such an object in turn is the same as a unital right $\mathbb{Z}Q$-module. Thus for a group Q, a Q-module in the variety $\mathbf{G}$ is equivalent to a right Q-module in the traditional sense.

10.7 Exercises

1. Express the associative law for an abelian group as a commuting diagram in the category of sets.

2. Verify the associativity of the multiplication (10.5), and the subsequent assertions of Section 10.1. In particular, show that a general abelian group $p : E \to Q$ in $\mathbf{Gp}/Q$ is isomorphic to the corresponding split extension $Q \ltimes p^{-1}\{1_Q\} \to Q$.

3. Show that the commuting of (10.10) implies that the projection morphism $p : E \to Q$ is an epimorphism in $\mathbf{Q}$.

4. Let $E \to Q$ be an abelian group in the slice category $\mathbf{Q}/Q$. For an object $D \to Q$ of $\mathbf{Q}/Q$, complete the verification that $\mathbf{Q}/Q(D,E)$ is an abelian group.

5. Verify that the morphisms (10.12) through (10.14) furnish an abelian group in the slice category $\mathbf{Q}/Q$.

6. Use the crossed product condition (10.18) to verify that (10.19) does give a group action of $\widetilde{G}$ on $M \times Q$.

7. Let e be an element of a quasigroup Q with universal stabilizer $\widetilde{G}_e$. Let M be a trivial $\widetilde{G}_e$-module. Show that the corresponding Q-module constructed by the Fundamental Theorem 10.1 is just the direct product $M \times Q$ of the abelian group M with the quasigroup Q.

8. Use the results of Section 10.2 to identify central piques with modules over the singleton quasigroup.

9. Use the results of Section 10.5 to identify abelian groups with modules over the singleton group in the variety of associative quasigroups.

10. Use the results of Section 10.5 to identify entropic piques with modules over the singleton quasigroup in the variety of entropic quasigroups.

11. Let $f : P \to Q$ be a quasigroup homomorphism, and let $q : E \to Q$ be a Q-module. If

$$\begin{array}{ccc} F & \longrightarrow & E \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ P & \xrightarrow[f]{} & Q \end{array}$$

is a pullback, show that $p : F \to P$ is a P-module. (This P-module is known as the *pullback* of the Q-module E to P along f).

12. Let $f : P \to Q$ be a group homomorphism, and let M be a Q-module determined by a group homomorphism $a : Q \to \operatorname{Aut} M$ from Q to the group of automorphisms of the abelian group reduct of M. Show that the pullback of M to P is determined by the composite homomorphism

$$P \xrightarrow{f} Q \xrightarrow{a} \operatorname{Aut} M\,.$$

13. Derive the Right and Left Quotient Rules.

14. How does Section 10.6 account for left modules over a group Q?

15. Let $\mathbf{L}$ be the variety of quasigroups satisfying the identity (1.13). Let Q be a loop, and let Q^* denote the set of elements of Q that are distinct from its identity element e. Finally, set $\widetilde{G} = U(Q; \mathbf{L})$.

    (a) By arguments similar to those used in the proof of Theorem 2.2 (p. 53), show that $\widetilde{G}$ is free on $\widetilde{L}(Q^*) + \widetilde{R}(Q^*)$.

    (b) Show that the universal stabilizer $\widetilde{G}_e$ is free on

$$\widetilde{L}_e(Q^* \times Q^*) + \widetilde{R}_e(Q^* \times Q^*) + \widetilde{T}_e(Q^*)\,.$$

    (c) Show that the rank of the free group $\widetilde{G}_e$ is $2|Q|^2 - 3|Q| + 1$.

    (d) Show that for a unital commutative ring S, the category of unital right $S\widetilde{G}_e$-modules is equivalent to the category of Q-modules in $\mathbf{L}$ over S.

(In [90], K.W. Johnson and C.R. Leedham-Green showed that the category of Q-modules in $\mathbf{L}$ is equivalent to the category of modules for a free group on $2|Q|^2 - 3|Q| + 1$ generators.)

16. Let $\mathbf{C}$ be the variety of commutative quasigroups. For an element e of Q in $\mathbf{C}$, show that $\widetilde{G} = U(Q; \mathbf{C})$ is free on $\widetilde{R}(Q)$. Determine $\widetilde{G}_e$.

17. Let $\mathbf{K}$ be the variety of commutative $\mathbf{L}$-quasigroups (compare Exercise 15), the variety of commutative loops and the empty set. For a commutative loop Q with identity element e, let $\widetilde{G} = U(Q; \mathbf{K})$. Let $Q^* = Q \setminus \{e\}$.

    (a) Show that $\widetilde{G}$ is free on $\widetilde{R}(Q^*)$.

    (b) Show that $\widetilde{G}_e$ is free on $\widetilde{R}_e(Q^* \times Q^*)$.

10.8 Problems

1. A variety $\mathbf{V}$ of quasigroups is said to be *universally free* if the universal multiplication group $U(Q; \mathbf{V})$ is free for each Q in $\mathbf{V}$. In particular, the varieties $\mathbf{Q}$, $\mathbf{L}$, $\mathbf{C}$ and $\mathbf{K}$ are universally free — compare Theorem 2.2 (p. 53) and Exercises 15 through 17.

    (a) Classify the universally free varieties.

    (b) In particular, are $\mathbf{Q}$, $\mathbf{L}$, $\mathbf{C}$ and $\mathbf{K}$ the only nontrivial universally free varieties of quasigroups?

2. For a commutative, unital ring S and a quasigroup Q in a variety $\mathbf{V}$, determine:

    (a) The universal multiplication group $U(Q; \mathbf{V})$; and

    (b) The ring $S\mathbf{V}Q$.

10.9 Notes

Section 10.1

The idea of treating modules as abelian groups in a slice category goes back to Beck [9, p. 33].

Section 10.3

The two versions of the Fundamental Theorem were initially proved in [148]. The main idea of Theorem 10.1 is reminiscent of the equivalence between equivariant bundles and modules [176], although a bundle structure on an induced module as discussed there does not include a copy of the base set, in the way that a Q-module includes a copy of Q as the image of the zero map.

Section 10.4

For combinatorial differentiation in groups, see [61].

Chapter 11

APPLICATIONS OF MODULE THEORY

This chapter applies the module theory introduced in Chapter 10 to address various issues in quasigroup theory. Section 11.1 interprets central piques as modules over a singleton quasigroup, and shows how the free central pique on one generator is the nonassociative analogue of the group of integers, providing indices for nonassociative powers. Section 11.2 uses the concepts of Section 10.5 to define the exponent of a quasigroup. Based on this definition, Section 11.4 formulates Burnside's problem for quasigroups. As discussed in Section 11.3, Steiner triple systems play a critical role here: although they have exponent 3, they have infinite universal multiplication groups in the variety of all Steiner triple systems. Section 11.5 applies module theory to explain the apparently *ad hoc* details of the Zassenhaus-Bruck construction of the free commutative Moufang loop on three generators. It also transpires that the module concept due to Eilenberg [51], as interpreted by Loginov for Moufang loops [105], is not strong enough to implement the Zassenhaus-Bruck construction. The final section, Section 11.6, gives a brief survey of extension and cohomology theory for each variety of quasigroups, using the equivalence between modules and self-centralizing congruences described in Section 10.2.

11.1 Nonassociative powers

In group theory, it is often convenient to interpret abelian groups as group modules over the trivial group. What are the corresponding analogues in quasigroup theory? In Chapter 3, the normality of the diagonal in the direct square was taken as the characteristic property of abelian groups. Arbitrary central quasigroups then emerged as the analogues in quasigroup theory. Now, regarding abelian groups as trivial modules leads to a more restricted quasigroup analogue, namely central piques.

DEFINITION 11.1 *A* banal module *E is a quasigroup module over the trivial quasigroup $\{e\}$.*

Following the convention introduced in Section 2.4, the right and left multiplications $R(e)$ and $L(e)$ in the universal multiplication group $U(\mathbf{Q};\{e\})$ and its quotients will be abbreviated as R and L respectively. The free group on the 2-element set $\{R, L\}$ is denoted by $\langle R, L\rangle$. Its integral group algebra is $\mathbb{Z}\langle R, L\rangle$.

PROPOSITION 11.1
The following structures are equivalent:

(a) *A $\mathbb{Z}\langle R, L\rangle$-module E;*

(b) *A banal module $p : E \to \{e\}$;*

(c) *A central pique E.*

PROOF By Theorem 2.2 (p. 53), both the universal multiplication group $U(\mathbf{Q};\{e\})$ and the universal stabilizer $U(\mathbf{Q};\{e\})_e$ are the free group $\langle R, L\rangle$. The equivalence between (a) and (b) thus becomes a direct consequence of the Fundamental Theorem 10.1 (p. 252). For the equivalence between (b) and (c), compare (10.21) with (2.17). Note that the pointed idempotent of a banal module $E \to \{e\}$ is given by the zero homomorphism $0 : \{e\} \to E$. □

The group $\mathbb{Z}$ of integers is the free abelian group on one generator 1. Inside the group of integers, the semigroup generated by 1 under addition is the semigroup $\mathbb{Z}^+$ of positive integers. This semigroup is the free semigroup on the single generator 1. As such, it indexes the powers $x^1, x^2, x^3, \ldots$ of an element x of an arbitrary semigroup.

By Proposition 11.1, the free central pique on one generator 1 is the quasigroup $\mathbb{Z}\langle R, L\rangle$ under the multiplication

$$x \cdot y = xR + yL\,, \tag{11.1}$$

the principal bundle in the sense of Definition 10.1 (p. 259). The nonassociative analogue of a semigroup is a *magma*, a set with a single binary operation (usually described as "multiplication"). It will now be shown that the magma $\mathbb{Z}\langle R, L\rangle^+$ generated by 1 in the principal bundle $\mathbb{Z}\langle R, L\rangle$ under the multiplication (11.1) is the free magma on a single generator x, indexing all the possible nonassociative powers x, x^2, $x \cdot x^2$, $x^2 \cdot x$, x^2x^2, $x^2x \cdot x$, $x \cdot xx^2$, $x \cdot x^2x$, $\cdots$. Such a power is said to be an *n-th power* if it is a product of n copies of x. For each positive integer n, each n-th power is a quasigroup word $x \ldots xw$ that only involves the multiplication. With Q as the singleton quasigroup $\{e\}$, the partial derivative (10.24) reduces to a function

$$\frac{\partial w}{\partial x} : \{e\} \to \mathbb{Z}\langle R, L\rangle; e \mapsto w' \tag{11.2}$$

selecting an element w' of $\mathbb{Z}\langle R, L\rangle^+$. This element is known as the *derivative* of the nonassociative power $x \dots xw$. The inductive definitions of Section 10.4 give $x' = 1$ and

$$(u \cdot v)' = u'R + v'L \tag{11.3}$$

for powers u and v of x.

THEOREM 11.1

Derivation gives an isomorphism from the free magma on a singleton $\{x\}$ *to the submagma* $\mathbb{Z}\langle R, L\rangle^+$ *generated by* 1 *in the multiplicative reduct of the free central pique* $\mathbb{Z}\langle R, L\rangle$ *generated by* 1.

PROOF Since $x' = 1$, comparison of (11.1) and (11.3) shows that derivation gives a surjective magma homomorphism to $\mathbb{Z}\langle R, L\rangle^+$ from the free magma on x. In other words, for each element $p(R, L)$ of $\mathbb{Z}\langle R, L\rangle^+$ (a polynomial in the noncommuting variables R and L), the *linear differential equation*

$$w' = p(R, L) \tag{11.4}$$

with forcing term $p(R, L)$ has a solution w.

It remains to show that derivation injects, i.e., to prove the uniqueness of the solution to each linear differential equation (11.4) with forcing term $p(R, L)$ in $\mathbb{Z}\langle R, L\rangle^+$. The proof is by induction on the degree of the polynomial $p(R, L)$. As an induction basis, note that x is the unique solution of the unique instance $w' = 1$ of (11.4) for which $p(R, L)$ has degree zero (is constant). Now if $p(R, L)$ has positive degree, it decomposes uniquely as a sum

$$p(R, L) = p_1(R, L)R + p_2(R, L)L \tag{11.5}$$

with $p_i(R, L)$ in $\mathbb{Z}\langle R, L\rangle^+$ for $i = 1, 2$. Since the degrees of the polynomials $p_i(R, L)$ are less than the degree of $p(R, L)$, there are unique solutions u and v to $u' = p_1(R, L)$ and $v' = p_2(R, L)$. A solution w to (11.4) with $p(R, L)$ of positive degree cannot be x, so it must be of the form $w = u_1 \cdot v_1$ with $u_1' = p_i(R, L)$ and $v_1' = p_2(R, L)$. Thus $u_1 = u$ and $v_1 = v$, proving that the solution $w = u \cdot v$ to (11.4) is unique. □

REMARK 11.1 The group of integers is the free group on one generator. As such, it might well be expected to furnish indices for arbitrary associative powers. On the other hand, the free quasigroup on one generator is not central (Exercises 2, 3). Thus it is rather surprising that the free *central* pique on one generator provides adequate indexing for arbitrary nonassociative powers. □

11.2 Exponents

The *exponent* of a group Q is defined as 0 if Q has an element x of infinite order. Otherwise, the exponent is the smallest positive integer n for which Q satisfies the equivalent identities $x^n = 1$ or $x^{1+n} = x$. Only the trivial group has exponent 1.

A naive attempt at defining the exponent of a quasigroup Q might seek a minimal nonassociative power $x \dots xw$ such that Q satisfies the identity $x \dots xw = x$, or ask for the maximal size of a singly generated subquasigroup of Q. Unfortunately, these attempts would assign exponent 1 to any idempotent quasigroup, trivial or not. Module theory suggests a more informative definition of the exponent. Recall that by Birkhoff's Theorem B.1, the variety $\mathsf{HSP}\{Q\}$ generated by a quasigroup Q is the class of quasigroups satisfying all the identities satisfied by Q.

DEFINITION 11.2

(*a*) *The* exponent *of a quasigroup Q in a variety $\mathbf{V}$ of quasigroups is the characteristic of the ring $\mathbb{Z}\mathbf{V}Q$.*

(*b*) *The* exponent *of a quasigroup Q is the exponent of Q in the variety $\mathsf{HSP}\{Q\}$ generated by Q.*

(*c*) *The* exponent *of a variety $\mathbf{V}$ is the exponent of the countably generated free quasigroup in the variety.*

The following proposition presents one connection between Definition 11.2 and the more naive concepts of exponent.

PROPOSITION 11.2

Let A be a singly generated abelian subquasigroup of a quasigroup Q.

(a) *If A is infinite, then the exponent of Q is* 0.

(b) *If A has finite order n, then the exponent of Q is a multiple of n.*

PROOF The projection $A \times Q \to Q$ forms a trivial Q-module in $\mathsf{HSP}\{Q\}$ (compare Exercise 7 in Chapter 10). By the relative Fundamental Theorem 10.2 (p. 258), there is an equivalent $\mathbb{Z}(\mathsf{HSP}\{Q\})Q$-module structure on the abelian group A. Thus the characteristic of $\mathbb{Z}(\mathsf{HSP}\{Q\})Q$, the quasigroup exponent of Q, is a multiple of n if $|A| = n$, and is 0 if A is infinite. □

It will now be shown that for a group Q, the quasigroup exponent specified in Definition 11.2 agrees with the group-theoretical exponent. A preparatory lemma about nonassociative powers is needed.

LEMMA 11.1

Suppose that a quasigroup word $x \dots xw$ is an n-th nonassociative power for some positive integer n. If the derivative w' of w in the free magma $\mathbb{Z}\langle R, L\rangle^+$ is the polynomial $p(R, L)$, then $p(1, 1) = n$.

PROOF Use induction on n. If $n = 1$, then $x \dots xw = x$, so the derivative x' is the constant 1. For $n > 1$, the word w decomposes as a product $w = u \cdot v$ of an r-th power u and an s-th power v, with $r+s = n$. Suppose $u' = p_1(R, L)$ and $v' = p_2(R, L)$. As in (11.5), $p(R, L) = p_1(R, L)R + p_2(R, L)L$. By the induction hypothesis, $p_1(1, 1) = r$ and $p_2(1, 1) = s$. Then

$$p(1, 1) = p_1(1, 1) + p_2(1, 1) = r + s = n\,,$$

as required. □

THEOREM 11.2

Suppose that a group Q has group-theoretical exponent n, for some natural number n. Then the exponent of Q according to Definition 11.2 is n.

PROOF If Q has group-theoretical exponent 0, it contains an infinite cyclic subgroup A. Proposition 11.2(a) then shows that the quasigroup exponent of Q is 0.

If Q has a positive group-theoretical exponent n, it satisfies the identity

$$x \dots xw = x \tag{11.6}$$

for some $(1 + n)$-th nonassociative power w. Corresponding to the identity (11.6) and the identity element e of Q, (10.32) gives a generator

$$\rho(e, e)\Big(\frac{\partial w}{\partial x}(e, \dots, e) - \frac{\partial x}{\partial x}(e, \dots, e)\Big)\rho(e, e \dots ew)^{-1} \tag{11.7}$$

of the ideal $J\mathbb{Z}\widetilde{G}_e$. Since $\widetilde{R}(e) = \widetilde{L}(e) = 1$ in the associative quasigroup variety $\mathsf{HSP}\{Q\}$, Lemma 11.1 shows that the generator (11.7) of $J\mathbb{Z}\widetilde{G}_e$ reduces to $(1 + n) - 1 = n$. Thus the quasigroup exponent of Q is a divisor of n. Conversely, a cyclic subgroup A of Q with $|A| = n$ exists by the definition of the group-theoretic exponent. Proposition 11.2(b) then shows that the quasigroup exponent of Q is a multiple of n. □

11.3 Steiner triple systems II

This section studies modules and exponents in the variety **STS** of Steiner triple systems introduced in Section 1.6, quasigroups satisfying the identities (1.15) of idempotence and (1.20) of total symmetry. Since Steiner triple systems are idempotent, each singly-generated subquasigroup is a singleton. It will transpire that the exponent of a nontrivial Steiner triple system is 3.

The first task is the determination of the universal multiplication groups in the variety of Steiner triple systems. Given a set Q, let $Q^\times$ be the set of all words in the alphabet Q in which all adjacent letters are distinct. Define a multiplication on $Q^\times$ using juxtaposition followed by cancellation of any resulting pairs of equal adjacent letters. Then $Q^\times$ becomes a monoid with the empty word as identity element. Defining an inversion by reversal of words, i.e., $(q_1 q_2 \dots q_n)^{-1} = q_n \dots q_2 q_1$, the monoid $Q^\times$ becomes a group. It is presented as the group generated by Q, subject only to relations specifying that the elements of Q are involutions. It may also be described as the free product (coproduct in **Gp**) of $|Q|$ copies of the cyclic group of order 2.

THEOREM 11.3

Let Q be a Steiner triple system. Then the universal multiplication group $\widetilde{G} = \mathrm{U}(Q; \mathbf{STS})$ of Q in the variety of Steiner triple systems is the group $Q^\times$.

PROOF For q in Q, the equalities $R(q)^{-1} = R(q) = L(q)$ hold in $\widetilde{G}$ by the identities (1.20). Each element of $\widetilde{G}$ may thus be written as a product $R(q_1)R(q_2)\dots R(q_r)$ with $q_1 q_2 \dots q_r$ in $Q^\times$, so that

$$R : Q^\times \to \widetilde{G}; q_1 \dots q_r \mapsto R(q_1)\dots R(q_r) \tag{11.8}$$

gives an epimorphism of groups. Let $q_1 q_2 \dots q_r$ be an element of the group kernel of R. If $q_1 q_2 \dots q_r \neq 1$, so that $r > 0$, then

$$X = XR(q_1)R(q_2)\dots R(q_r) \tag{11.9}$$

in the Steiner triple system $Q[X]$. But in this system, the free extension of the idempotent, S_3-symmetric partial Latin square $\big(Q + \{X\}, T(Q)\big)$ in the variety of Steiner triple systems, the elements on each side of (11.9) are distinct, representing distinct normal forms in the Normal Form Theorem for idempotent, S_3-symmetric quasigroups (compare Exercise 33 in Chapter 1). Thus $r = 0$, and R is the required isomorphism. □

In a nonempty Steiner triple system Q, fix an element e. Set $\overline{e} = e$. If q is an element of Q distinct from e, define $\overline{q} = qe$ in Q. Under the isomorphism (11.8), $R_e(a, e)$ is the image of $\overline{a}ea$ and $R_e(a, b)$ is the image of $\overline{a}b\overline{c}$ for a block

$\{a, b, c\}$ not containing e. Let each block $\{a, b, c\}$ not containing e be ordered $a < b < c$, and let each block $\{e, a, \overline{a}\}$ containing e be ordered $e < a < \overline{a}$.

THEOREM 11.4

The stabilizer $\widetilde{G}_e$ of e in $\widetilde{G}$ is the free product of the 2-element groups $\langle R_e(q,q)\rangle$ for q in Q with the free group on the union of the sets

$$\{R_e(a,b), R_e(b,c,), R_e(c,a)\}$$

for each block $a < b < c$ not containing e and the sets $\{R_e(a,e)\}$ for each block $e < a < \overline{a}$ containing e. In particular, if Q has n elements, then $\widetilde{G}_e$ is the free product of n copies of $\mathbb{Z}/2\mathbb{Z}$ with a free group of rank $\binom{n-1}{2}$.

PROOF This follows by an application of the Reidemeister-Schreier Theorem to the action of $\widetilde{G}$ on Q. The version [34, Th. 6.2] lends itself particularly well to this application, $\widetilde{G}$ having the presentation of $Q^{\times}$. Take the set T of [34, §6(9)] to be $\{e \wedge \overline{q} \mid e \neq q \in Q\}$. Then $\widetilde{G}_e$ is presented as generated by $\{q \wedge r \mid q, r \in Q\}$ subject to the relations

$$\begin{cases} e \wedge r = 1 \text{ for } r \neq e\,; \\ q \wedge r = q \wedge r^{-1} = (qr \wedge r)^{-1}\,. \end{cases}$$

The generators $q \wedge r$ correspond to $R_e(q,r) = R_e(qr,r)^{-1}$ for $r \neq \overline{q}$ and $R_e(q,q)R(e)$ for $r = \overline{q}$. If Q has a finite number n of elements, then there are $(n-1)/2$ blocks containing e and $n(n-1)/6$ blocks altogether, so that the free part of $\widetilde{G}_e$ is free on

$$\frac{1}{2}\big((n-3)(n-1) + (n-1)\big) = \binom{n-1}{2}$$

generators. □

Modules in the variety **STS** are described by the following theorem.

THEOREM 11.5

Let Q be a Steiner triple system with element e. Let F be the field of order 3. Let J be the ideal in the group algebra $\mathsf{F}\widetilde{G}_e$ generated by the elements

$$\begin{cases} 1 + R_e(x,y) \\ \quad \textit{if } \{x,y\} \textit{ is a subset of a block containing } e\,; \\ R_e(a,b) + R_e(a,c)R_e(b,a) \\ \quad \textit{if } \{a,b,c\} \textit{ is a block not containing } e\,. \end{cases} \tag{11.10}$$

Then the category of Q-modules in **STS** *is equivalent to the category of unital right $(\mathsf{F}\widetilde{G}_e)/J$-modules.*

PROOF As an equational basis for the variety **STS** of Steiner triple systems relative to the variety **Q** of all quasigroups, it is most convenient to take idempotence (1.15), commutativity, and right symmetry (1.39) (compare Exercise 10 in Chapter 1). Commutativity gives $R(x) = L(x)$ in $\widetilde{G}$ for x in Q, while right symmetry gives $R(x) = R(x)^{-1}$. Also,

$$\rho(e, x) = R(e\backslash e)^{-1} R(e\backslash x) = R(e)^{-1} R(e\backslash x) = R(e) R(\overline{x})$$

using the notation introduced before Theorem 11.4.

Each argument in the commutative law occurs uniquely above the line. By Proposition 10.4 (p. 260), commutativity then makes no contribution to the generation of $J\mathbf{STS}Q$. Next, consider right symmetry as the identity $x_1 x_2 u = x_1 x_2 v$ equating the words $x_1 x_2 u = x_1 x_2 \cdot x_2$ and $x_1 x_2 v = x_1$. Here x_1 occurs uniquely above the line on each side, and so makes no contribution to $J\mathbf{STS}Q$. Now

$$\begin{aligned} \frac{\partial u}{\partial x_2} &= \frac{\partial x_1 x_2}{\partial x_2} R(x_2) + L(x_1 x_2) \\ &= L(x_1) R(x_2) + L(x_1 x_2) \\ &= R(x_1) R(x_2) + R(x_1 x_2) \end{aligned}$$

by the Product Rule, while

$$\frac{\partial v}{\partial x_2} = 0\,.$$

Thus the generators (10.32) of $J\mathbf{STS}Q$ obtained from the right symmetry take the form

$$\begin{aligned} &\rho(e, x_2)\Big(R(x_1)R(x_2) + R(x_1 x_2)\Big)\rho(e, x_1)^{-1} \\ &\qquad = R(e)R(\overline{x}_2)\Big(R(x_1)R(x_2) + R(x_1 x_2)\Big)R(\overline{x}_1)R(e)\,, \end{aligned}$$

equivalent as ideal generators in $\mathbb{Z}\widetilde{G}_e$ to

$$\begin{aligned} &R(\overline{x}_2)\Big(R(x_1)R(x_2) + R(x_1 x_2)\Big)R(\overline{x}_1) \\ &\qquad = R_e(x_2, x_1) R_e(x_1 x_2, x_2) + R_e(x_2, x_1 x_2)\,. \end{aligned}$$

If $\{a, b, c\}$ is a block, setting $x_2 = a$ and $x_1 = c$ gives the second line of (11.10). Setting $x_1 = x_2 = a$ gives $\Big(R_e(a, a) + 1\Big)R_e(a, a)$. Now

$$R(e) = R_e(e, e) = R_e(e, a) = R_e(a, \overline{a}) \tag{11.11}$$

for any a in Q (Exercise 14). Setting $x_2 = a$ and $x_1 = \overline{a}$ then gives $1 + R_e(a, e)$. Thus the ideal of $\mathbb{Z}\widetilde{G}_e$ generated by (11.10) is the ideal generated by all the contributions from the right symmetry.

Now consider the idempotent law as $x^2 = x$. Since

$$\frac{\partial x^2}{\partial x} = R(x) + L(x) = 2R(x)\,,$$

(10.32) for idempotence becomes

$$\rho(e,x)\big(2R(x) - 1\big)\rho(e,x)^{-1} = 2R_e(x,x) - 1\,. \tag{11.12}$$

Setting $x = e$ and recalling (11.11), one then has the following congruences modulo the ideal $J\mathbf{STS}Q$:

$$1 \equiv 2R(e) \equiv -2\,,$$

the second coming from the first line of (11.10). Now modulo 3, (11.12) reduces to $-\big(R_e(x,x)+1\big)$, which lies in the ideal of $\mathsf{F}\widetilde{G}_e$ generated by (11.10). This completes the proof of the theorem. □

COROLLARY 11.1
The exponent of a nontrivial Steiner triple system is 3.

11.4 The Burnside Problem

One of the most fascinating problems of the theory of groups is the Burnside Problem [22] asking whether a given variety of groups of finite (nonzero) exponent is necessarily locally finite. Recall that a variety is *locally finite* if its finitely generated free algebras are finite. S.I. Adyan and P.S. Novikov showed that for odd exponents larger than 664, the Burnside Problem may have a negative answer [1]. The proofs are long and extremely delicate.

For a variety $\mathbf{V}$ of quasigroups, there are several concepts of finiteness: local finiteness, finite (nonzero) exponent, and universal finiteness. The variety $\mathbf{V}$ is said to be *universally finite* if, for a finite quasigroup Q in $\mathbf{V}$, the universal multiplication group $U(Q;\mathbf{V})$ is finite. For example, any variety of groups is universally finite, while the variety of all quasigroups is not. The relationship between local finiteness and universal finiteness is given as follows.

PROPOSITION 11.3
Let $\mathbf{V}$ *be a variety of quasigroups.*

(a) *If* $\mathbf{V}$ *is locally finite, then it is universally finite.*

(b) *If* $\mathbf{V}$ *is universally finite, then so is each variety* $\mathbf{W}$ *contained in* $\mathbf{V}$.

PROOF **(a)**: Suppose that Q is a finite quasigroup in $\mathbf{V}$. Then the coproduct $Q[X]$, being a quotient of the finite free quasigroup in $\mathbf{V}$ on the finite set $Q+\{X\}$, is finite. It follows that the subgroup $U(Q;\mathbf{V}) = \mathrm{Mlt}_{Q[X]}Q$ of the finite group $\mathrm{Mlt}\, Q[X]$ is finite.

(b): Let Q be a member of $\mathbf{W}$, and let Q' be the coproduct $Q[X]$ in $\mathbf{W}$. Since $\mathbf{W}$ is contained in $\mathbf{V}$, the quasigroup Q lies in $\mathbf{V}$. By Corollary 2.5 (p. 52), $U(Q;\mathbf{W}) = \mathrm{Mlt}_{Q'}Q$ is a quotient of the finite group $U(Q;\mathbf{V})$, and so is itself finite. □

REMARK 11.2 The converse to Proposition 11.3(a) is false. By Proposition 2.9 (p. 52), the variety of associative quasigroups is universally finite. However, it is not locally finite. □

The problem of determining the universally finite varieties of quasigroups that are not locally finite appears interesting. Such varieties are likely to have a strong structure.

The Burnside Problem for quasigroups might initially be posed as asking whether a given variety of quasigroups of finite (nonzero) exponent is locally finite, the Adyan-Novikov result saying that the variety of groups of odd exponent e is not locally finite for $e > 664$. It is then important to note that, while the variety of Steiner triple systems has exponent 3 (Corollary 11.1), it is not locally finite. Indeed it is not universally finite, since the group $Q^{\times}$ of Theorem 11.3 is infinite for all nontrivial Steiner triple systems Q. By contrast, the variety of groups of exponent 3 is locally finite, with its finitely generated free groups being the universal multiplication groups of finitely generated free loops in the locally finite variety of nilpotent commutative Moufang loops of exponent 3 and class at most 2 (see Section 11.5 below).

The extra significance of the Adyan-Novikov examples is that they are universally finite varieties of finite (nonzero) exponent which are not locally finite. Are there any varieties of nonassociative quasigroups with these properties that are genuinely different (e.g., not obtained from the Adyan-Novikov groups by isotopy)? At any rate, the sharpness of the Burnside Problem for groups appears to be best preserved on extension to quasigroups by the formulation of Problem 1 below: Determine conditions under which universally finite quasigroup varieties of finite (nonzero) exponent are locally finite.

11.5 A free commutative Moufang loop

This section shows how quasigroup module theory may be used to give a complete account of the otherwise apparently *ad hoc* details of the Zassenhaus-Bruck construction [20, Th. II.9A] of the free commutative Moufang loop on

three generators. Commutative Moufang loops may be described as nonempty quasigroups that are commutative ($xy = yx$) loops ($x/x = y\backslash y$) satisfying the identity

$$x_1x_1 \cdot x_2x_3 = x_1x_2 \cdot x_1x_3 \tag{11.13}$$

(Exercise 15). Abelian groups are commutative Moufang loops, and indeed any commutative Moufang loop generated by two elements is an abelian group, according to Moufang's Theorem. Thus the free commutative loop on two generators is $\mathbb{Z}^2$. Following Zassenhaus, Bruck constructed the free commutative Moufang loop on three generators by equipping the abelian group $\mathbb{Z}^3 \oplus (\mathbb{Z}/3\mathbb{Z}) =$

$$\{\mathbf{x} = (x_1, x_2, x_3, x_4) \mid x_1, x_2, x_3 \in \mathbb{Z},\ x_4 \in \mathbb{Z}/3\mathbb{Z}\}$$

with a product $\mathbf{x} \cdot \mathbf{y}$ defined as

$$\mathbf{x} + \mathbf{y} + \big(0, 0, 0, (x_3 - y_3)(x_1y_2 - x_2y_1) + 3\mathbb{Z}\big). \tag{11.14}$$

Module theory describes this construction as follows.

THEOREM 11.6

The free commutative Moufang loop on three generators is the domain of the principal bundle

$$\pi : \mathbb{Z}^3 \oplus (\mathbb{Z}/3\mathbb{Z}) \to \mathbb{Z}^2; \mathbf{x} \mapsto (x_1, x_2) \tag{11.15}$$

over the free algebra $\mathbb{Z}^2$ on two generators in the variety **CML** *of commutative Moufang loops.*

Proving Theorem 11.6 amounts to answering Problem 2 of Chapter 10 for $\mathbb{Z}^2$ in the variety **CML**. The universal multiplication group $\widetilde{G} = U(\mathbb{Z}^2; \mathbf{CML})$ is the relative multiplication group of the free commutative Moufang loop $\mathbb{Z}^2 = \langle b \rangle \oplus \langle c \rangle$ on the 2-element set $\{b, c\}$ in the free commutative Moufang loop on the 3-element set $\{a, b, c\}$. The group $\widetilde{G}$ is nilpotent of class 2, with center of order 3 generated by $[R(c), R(b)] = R(b, c)$ [21, VIII.2]. The latter term in the equation is the element (2.43) for e the identity element $(0, 0)$ of the loop $\mathbb{Z}^2$. Then $\widetilde{G}_e$ is the center $\langle R(b, c) \rangle$ of $\widetilde{G}$. The solution of the problem is completed by determining the two-sided ideal $J\mathbb{Z}\widetilde{G}_e$ of the integral group algebra $\mathbb{Z}\widetilde{G}_e$ generated by (10.32).

The commutative and loop identities make no contribution to (10.32). Consider the quasigroup words $x_1x_2x_3u = x_1x_1 \cdot x_2x_3$ and $x_1x_2x_3v = x_1x_2 \cdot x_1x_3$ appearing in (11.13). Now x_2 and x_3 appear uniquely above the line, so the only contributions to (10.32) come from

$$\frac{\partial v}{\partial x_1} - \frac{\partial u}{\partial x_1} = R(x_2)R(x_3x_1) + R(x_3)R(x_1x_2) - 2R(x_1)R(x_2x_3)\,.$$

After some calculation (Exercise 16) it turns out that the ideal $J\mathbb{Z}\widetilde{G}_e$ is determined by the requirement that, modulo $J\mathbb{Z}\widetilde{G}_e$, the following congruences hold:

$$3 \equiv 3R(b,c) \equiv 3R(c,b) \equiv 1 + R(b,c) + R(c,b). \tag{11.16}$$

Thus the typical element

$$x + yR(b,c) + zR(c,b)$$

of $\mathbb{Z}\widetilde{G}_e$ (with integers x, y, z) is congruent to

$$(x+y+z) + (y-z)\big[R(c,b) - R(b,c)\big]$$

modulo $J\mathbb{Z}\widetilde{G}_e$. Each element of the fiber $\pi^{-1}\{e\}$ of (11.15) may be written uniquely as

$$x_3 + x_4\big[R(c,b) - R(b,c)\big] \tag{11.17}$$

with $x_3 \in \mathbb{Z}$ and $x_4 \in \mathbb{Z}/3\mathbb{Z}$. The action of an element $R(b,c)^x$ on (11.17) sends it to

$$x_3 + (x_4 + x_3 x + 3\mathbb{Z})\big[R(c,b) - R(b,c)\big].$$

This is the point at which the multiplicative structure of the ring $\mathbb{Z}/3\mathbb{Z}$ enters. The equation (10.21) may then be used to show that there is an isomorphism θ from $\mathbb{Z}^3 \oplus (\mathbb{Z}/3\mathbb{Z})$ to the domain of the principal bundle. Under this isomorphism, a vector $\mathbf{x} = (x_1, x_2, x_3, x_4)$ is sent to

$$\mathbf{x}^\theta = \Big(x_3 + x_4\big[R(c,b) - R(b,c)\big], R(b^{x_1}c^{x_2})\Big) \tag{11.18}$$

(Exercise 17).

Following Eilenberg [51], Loginov [105] introduced a concept of linear representation for Moufang loops. Given two maps σ, τ from a Moufang loop Q with identity e to the automorphism group of an abelian group M, the group M is said to be an *Eilenberg-Loginov module* [39] for Q if the set $M \times Q$ equipped with the multiplication

$$(m_1, q_1)(m_2, q_2) = \big(m_1\sigma(q_2) + m_2\tau(q_1), q_1q_2\big) \tag{11.19}$$

is a Moufang loop $M \rtimes Q$ with identity $(0, e)$ (compare [105, §2]). Despite the superficial similarities between (10.21) and (11.19), the Zassenhaus-Bruck construction cannot be realized as an Eilenberg-Loginov module.

PROPOSITION 11.4

There are no maps $\sigma, \tau : \mathbb{Z}^2 \to \mathrm{Aut}\,(\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z}))$ such that $\mathbb{Z}^3 \oplus (\mathbb{Z}/3\mathbb{Z})$ with the product (11.14) *can be written in the form* (11.19).

PROOF Assume the existence of suitable maps σ, τ so that

$$(m_1 + m_2, m_1' + m_2' + (m_1 - m_2)(q_1q_2' - q_1'q_2) + 3\mathbb{Z}) = \\ (m_1, m_1' + 3\mathbb{Z})\sigma(q_2, q_2') + (m_2, m_2' + 3\mathbb{Z})\tau(q_1, q_1').$$

Set $q_1 = q_1' = m_2 = 1$, $m_1 = m_1' = m_2' = 0$. Then for all q, q' in $\mathbb{Z}$, one obtains

$$(1, q - q' + 3\mathbb{Z}) = (1, 3\mathbb{Z})\tau(1, 1).$$

Thus $\tau(1, 1)$ cannot be well defined. □

11.6 Extensions and cohomology

The final application of quasigroup modules is to the theory of extensions and cohomology for quasigroups in a given variety $\mathbf{V}$ of quasigroups. Here, heavy use is made of the equivalence between modules and self-centralizing congruences described in Section 10.2. Now a quasigroup T is said to be an *extension* of a quasigroup R if there is a surjective quasigroup homomorphism $T \to R$, i.e., if T has R as a quotient. Extension theory aims to reconstruct an extension T from its quotient R and additional data. The reconstruction, as ultimately presented in the "only if" part of the proof of Theorem 11.7 below, requires cohomological machinery.

The data used for specifying extensions are most succinctly expressed in terms of simplicial maps. These are defined with the direct algebraic approach of [147], to which the reader is referred for fuller detail. Let ε_n^i be the operation which deletes the $(i+1)$-th letter from a nonempty word of length n. Let δ_n^i be the operation which repeats the $(i+1)$-th letter in a nonempty word of length n. These operations, for all positive integers n and natural numbers $i < n$, generate (the morphisms of) a category Δ called the *simplicial category*.

A *simplicial object* B^* in $\mathbf{V}$ is (the image of) a functor from Δ to $\mathbf{V}$. A *simplicial map* is (the set of components of) a natural transformation between such functors. Generically, the morphisms of a simplicial object B^* are denoted by their preimages in Δ, namely as $\varepsilon_n^i : B^n \to B^{n-1}$ and $\delta_n^i : B^n \to B^{n+1}$. Note the use of the convention denoting the domain of the morphisms ε_n^i and δ_n^i as B^n. This does not mean that the domain is an n-th power in the category $\mathbf{V}$. The notation is a relic of the subject's topological origins, labeling homological objects with suffices (e.g., B_n) and cohomological objects with superscripts (such as B^n). The index n on B^n is called its *dimension*.

Given $(\theta^0, \ldots, \theta^{n-1}) \in \mathbf{V}(X, Y)^n$, the *simplicial kernel* $\ker(\theta^0, \ldots, \theta^{n-1})$ is the largest subquasigroup K of the power X^{n+1} for which the θ^i and the restrictions of the projections from the power model the identities satisfied by the simplicial ε_n^i and ε_{n+1}^i. For example, the simplicial kernel of a single $\mathbf{V}$-morphism $\theta^0 : X \to Y$ is $K = \{(x_0, x_1) \in X^2 \mid x_0\theta^0 = x_1\theta^0\}$, the usual kernel of θ^0, modeling the single simplicial identity $\varepsilon_2^0\varepsilon_1^0 = \varepsilon_2^1\varepsilon_1^0$ by $\pi^0\theta^0 = \pi^1\theta^0$ for $\pi^i : K \to X; (x_0, x_1) \mapsto x_i$.

For each positive integer n, removing all operations from Δ that involve words of length greater than n leaves the *simplicial category* Δ_n *truncated*

at n. Functors from Δ_n are called *simplicial objects truncated at dimension n.* Truncated simplicial objects may be extended to full simplicial objects by successively tacking on simplicial kernels. In such cases one may omit the epithet "truncated," speaking merely of simplicial objects, even when one has only specified the lower-dimensional part.

DEFINITION 11.3 *A simplicial object B^* is said to be* seeded *if:*

(a) *It is truncated at dimension* 2*;*

(b) $(\varepsilon_2^0, \varepsilon_2^1) : B^2 \to \ker(\varepsilon_1^0)$ *surjects;*

(c) $\varepsilon_1^0 : B^1 \to B^0$ *surjects;*

(d) $\ker(\varepsilon_2^0 : B^2 \to B^1) = \eta\big(\ker(\varepsilon_2^1 : B^2 \to B^1)\big)$.

LEMMA 11.2
In a seeded simplicial object B, define

$$C = \{c \in B^2 \mid c\varepsilon_2^0 = c\varepsilon_2^1\}.$$

Define a congruence D on C by

$$c\ D\ c' \Leftrightarrow \big((c\varepsilon_2^0\delta_1^0, c), (c'\varepsilon_2^0\delta_1^0, c')\big) \in \big(\ker\varepsilon_2^0 \circ \ker\varepsilon_2^1 \,\big|\, \ker\varepsilon_2^0 \cap \ker\varepsilon_2^1\big).$$

Then

$$C^D \to B^0; c^D \mapsto c\varepsilon_2^0\varepsilon_1^0 \tag{11.20}$$

is a module over B^0, isomorphic to $(\ker\varepsilon_2^0 \cap \ker\varepsilon_2^1)^{(\ker\varepsilon_2^0 \circ \ker\varepsilon_2^1 \,|\, \ker\varepsilon_2^0 \cap \ker\varepsilon_2^1)}$.

The module (11.20) of Lemma 11.2 is called the module *grown* by the seeded simplicial object B^*. If V is a congruence on a $\mathbf{V}$-quasigroup T, then

$$V^{(\eta(V)|V)} \rightrightarrows T^{\eta(V)} \to T^{V\circ\eta(V)} \tag{11.21}$$

is a seeded simplicial object with $\varepsilon_2^i : (t_0, t_1)^{(\eta(V)|V)} \mapsto t_i^{\eta(V)}$, growing the module

$$(V \cap \eta(V))^{(V\circ\eta(V)|V\cap\eta(V))} \to T^{V\circ\eta(V)}; (t_0, t_1)^{(V\circ\eta(V)|V\cap\eta(V))} \mapsto t_0^{V\circ\eta(V)}.$$

The seeded simplicial object (11.21) is said to be *planted* by the congruence V on the algebra T.

DEFINITION 11.4 *A simplicial map $p^* : A^* \to B^*$ is said to be* seeded *if the codomain object B^* is seeded in the sense of Definition 11.3, and if $p^0 : A^0 \to B^0$ surjects.*

The second tool used for studying extensions in quasigroup varieties is monadic cohomology. Once again, full details may be found in [147].

For each $\mathbf{V}$-quasigroup A, let AG denote the free $\mathbf{V}$-quasigroup over the generating set $\{\{a\} \mid a \in A\}$. Given a $\mathbf{V}$-quasigroup R, consider the uniquely defined $\mathbf{V}$-morphism $\varepsilon_n^j : RG^n \to RG^{n-1}$ deleting the j-th layer of braces, where $j = 0$ corresponds to the inside layer and $j = n-1$ to the outside. Let $\delta_n^j : RG^n \to RG^{n+1}$ insert the j-th layer of braces. One obtains a simplicial object RG^*, known as the *free resolution* of A. Each RG^n projects to R by a composition

$$\varepsilon_n^0 \dots \varepsilon_1^0 : RG^n \to R. \tag{11.22}$$

An R-module $E \to R$ becomes an RG^n-module by pullback along (11.22). Write $\mathrm{Der}(RG^n, E)$ for the abelian group $\mathbf{V}/R(RG^n \to R, E \to R)$ of *derivations*. Define *coboundary homomorphisms*

$$d_n : \mathrm{Der}(RG^n, E) \to \mathrm{Der}(RG^{n+1}, E); f \mapsto \sum_{i=0}^{n} (-)^i \varepsilon_{n+1}^i f$$

for each natural number n. For each positive integer n, define

$$\mathrm{H}^n(R, E) = \mathrm{Ker}(d_n)/\mathrm{Im}(d_{n-1}), \tag{11.23}$$

the so-called n-th *monadic cohomology group of R with coefficients in E*. [Note that [147] uses $\mathrm{H}^{n-1}(R, E)$ for (11.23).] The cosets forming (11.23) are known as *cohomology classes*. Elements of $\mathrm{Ker}(d_n)$ are known as *cocycles*, and elements of $\mathrm{Im}(d_{n-1})$ are *coboundaries*.

LEMMA 11.3
Let $p^* : RG^* \to B^*$ be a seeded simplicial map whose codomain grows module M. Pull M from B^0 back to R along p^0. Then

$$p^3(\varepsilon_3^0, \varepsilon_3^1, \varepsilon_3^2)P^D : RG^3 \to M \tag{11.24}$$

is a cocycle in $\mathrm{Der}(B^3, M)$.

DEFINITION 11.5 *The cohomology class of* (11.24) *is called the* obstruction *of the seeded simplicial map p^*. The simplicial map is said to be* unobstructed *if this class is zero.*

LEMMA 11.4
The obstruction of a seeded simplicial map $p^* : RG^* \to B^*$ is uniquely determined by its bottom component $p^0 : R \to B^0$.

The diagram-chasing proofs of Lemmas 11.3 and 11.4 are given in [147, pp. 124–127].

DEFINITION 11.6 *A seeded simplicial map $p^* : RG^* \to B^*$ is said to be* realized *by a* $\mathbf{V}$*-quasigroup T if there is a congruence V on T planting B^* such that p^0 is the natural projection $T^V \to T^{V\circ\eta(V)}$.*

THEOREM 11.7
A seeded simplicial map $p^* : RG^* \to B^*$ is unobstructed if and only if it is realized by a quasigroup T.

PROOF (Sketch.) "**If:**" Consider the diagram

$$\begin{array}{ccccccc}
\Rrightarrow & RG^2 & \Rightarrow & RG & \to & R & \\
 & \downarrow \sigma^2 & & \downarrow \sigma^1 & & \downarrow \sigma^0 & \\
\Rrightarrow & V & \Rightarrow & T & \to & R & \\
 & \downarrow & & \downarrow & & \downarrow p^0 & \\
\Rrightarrow & V^{(\eta(V)|V)} & \Rightarrow & T^{\eta(V)} & \to & T^{V\circ\eta(V)} &
\end{array} \tag{11.25}$$

in which σ^0 is the identity on $R = T^V$, σ^1 is given by the freeness of RG, and σ^2 exists since $V = \ker(T \to R)$. Take p^2, p^1, p^0 to be the composites down the respective columns of (11.25), the second factors of these composites all being natural projections. Writing $\pi^i : V \to T; (t_0, t_1) \mapsto t_i$, one has

$$\begin{aligned}(\varepsilon_3^0\sigma^2, \varepsilon_3^1\sigma^2, \varepsilon_3^2\sigma^2)P\pi^0 &= (\varepsilon_3^0\varepsilon_2^0, \varepsilon_3^1\varepsilon_2^0, \varepsilon_3^2\varepsilon_2^0)P\sigma^1 = \varepsilon_3^2\varepsilon_2^0\sigma^1 \\ &= \varepsilon_3^0\varepsilon_2^1\sigma^1 = (\varepsilon_3^0\varepsilon_2^1, \varepsilon_3^1\varepsilon_2^1, \varepsilon_3^2\varepsilon_2^1)P\sigma^1 = (\varepsilon_2^0\sigma^2, \varepsilon_2^1\sigma^2, \varepsilon_2^2\sigma^2)P\pi^1,\end{aligned}$$

so the obstruction of p^* is the zero element $(\varepsilon_3^0p^2, \varepsilon_3^1p^2, \varepsilon_3^2p^2)P^D$ of the group $\mathrm{Der}\Big(RG^3, \big(V \cap \eta(V)\big)^{(V\circ\eta(V)|V\cap\eta(V))}\Big)$, as required.

"**Only if:**" If p^* is unobstructed, then as shown in [147, p.129], one may assume without loss of generality that (11.24) itself is zero, and not just in the zero cohomology class. Let Q be a pullback in

$$\begin{array}{ccc}
Q & \longrightarrow & RG \\
\big\downarrow & & \big\downarrow p_1 \\
B^2 & \xrightarrow[\varepsilon_2^1]{} & B^1
\end{array}$$

realized, say, by $Q = \{(b, w) \in B^2 \times RG \mid wp^1 = b\varepsilon_2^1\}$. Define a congruence W on Q by $(b, w)\ W\ (b', w')$ iff $w\varepsilon_1^0 = w'\varepsilon_1^0$ and

$$(b, b')\ (\ker\varepsilon_2^1 \mid \ker\varepsilon_2^0)\ (\{w\}p^2, \{w'\}p^2).$$

Set $T = Q^W$, and take V on T to be the kernel of

$$T \to R; (b, w)^W \mapsto w\varepsilon_1^0 .$$

For the details of the verification that T realises p^*, with V planting B^*, see [147, pp. 129–132]. In particular, note that the kernel of

$$T \to B^1; (b, w)^W \mapsto b\varepsilon_2^0$$

is $\eta(V)$. □

Let $p^* : RG^* \to B^*$ be a seeded simplicial map whose codomain grows a module $M \to B^0$. Pull M back along $p^0 : R \to B^0$ to an R-module. An extension $V \rightrightarrows T \to R$ is said to be *singular for* p^* if its kernel V is self-centralizing, with an R-module isomorphism $V^{(V|V)} \to M$. Let p^*S be the set of $\mathbf{V}/R$-isomorphism classes of extensions that are singular for p^*. This set becomes an abelian group, with the class of the split extension $M \to R$ as zero. The addition operation on p^*S is known as the *Baer sum*. To obtain a representative of the Baer sum of the isomorphism classes of two extensions $V_i \rightrightarrows T_i \to R$, with module isomorphism $\theta : V_1^{(V_1|V_1)} \to V_2^{(V_2|V_2)}$, take the quotient of the pullback $T_1 \times_R T_2$ by the congruence

$$\left\{ \big((t_1, t_2), (t_1', t_2')\big) \;\middle|\; (t_i, t_i') \in V_i,\ (t_1, t_1')^{(V_1|V_1)}\theta = (t_2, t_2')^{(V_2|V_2)} \right\}.$$

Singular extensions are then classified as follows [147, Th. 632].

THEOREM 11.8
The groups p^*S and $\mathrm{H}^2(R, M)$ are isomorphic.

Now assume additionally that the seeded simplicial map $p^* : RG^* \to B^*$ is unobstructed. An extension $V \rightrightarrows T \to R$ is said to be *nonsingular for* p^* if T realizes p^*. Let p^*N denote the set of $\mathbf{V}/R$-isomorphism classes of extensions that are nonsingular for p^*. By Theorem 11.7, p^*N is nonempty. Nonsingular extensions are then classified as follows [147, Th. 634].

THEOREM 11.9
The abelian group p^*S acts regularly on p^*N, so the sets p^*N and $\mathrm{H}^2(R, M)$ are isomorphic.

Let $U \rightrightarrows S \to R$ be singular for p^*, and let $V \rightrightarrows T \to R$ be nonsingular for p^*. To obtain a representative for the image of the class of V under the action of the class of U, assuming an R-module isomorphism

$$\theta : (V \cap \eta(V))^{(V \circ \eta(V)|V \cap \eta(V))} \to U^{(U|U)} ,$$

take the quotient of the pullback $T \times_R S$ by the congruence

$$\{((t, s), (t', s')) \mid (t, t') \in V \cap \eta(V),\ (s', s) \in U,\ (t, t')^{(V|V \cap \eta(V))}\theta = (s', s)^{(U|U)}\}.$$

11.7 Exercises

1. Basing on the proof of Theorem 11.1, solve the differential equations $w' = R^2 + LR + L$ and $w' = (R + L)^3$.

2. (a) Show that the quasigroup Q with the multiplication table given in Figure 1.2 is generated by the single element 4.
   (b) Show that Q is not central. (Compare Remark 3.1.)
   (c) Conclude that the free quasigroup on one generator is not central.

3. Use Section 1.9 and Exercises 14(b), (c), or 16 in Chapter 3 to show that the free quasigroup on one generator is not central.

4. For each positive integer n, show that the number of n-th nonassociative powers is the n-th *Catalan number*

$$c_n = \frac{1}{n}\binom{2n-2}{n-1}.$$

5. Define a multiplication on the free group algebra $\mathbb{Z}\langle R, L\rangle$ by

$$x \circ y = xR + yL + 1\,.$$

   (a) Show that $(\mathbb{Z}\langle R, L\rangle, \circ)$ is a quasigroup.
   (b) Show that $(\mathbb{Z}\langle R, L\rangle, \circ)$ is centrally isotopic to $(\mathbb{Z}\langle R, L\rangle, \cdot)$.
   (c) Show that the submagma of $(\mathbb{Z}\langle R, L\rangle, \circ)$ generated by 0 is free.
   (d) Show that the submagma of $(\mathbb{Z}\langle R, L\rangle, \circ)$ generated by 1 is free.

6. Let $\mathbb{Z}[R, R^{-1}, L, L^{-1}]$ be the ring of integral Laurent polynomials over two (commuting) variables R and L. Show that the following structures are equivalent:

   (a) A $\mathbb{Z}[R, R^{-1}, L, L^{-1}]$-module E;
   (b) An entropic banal module $p : E \to \{e\}$;
   (c) An entropic pique E.

7. [153] In the notation of the previous exercise, consider the element 1 of the principal bundle $\mathbb{Z}[R, R^{-1}, L, L^{-1}]$ for entropic banal modules.

   (a) Show that the corresponding Conway algebra given by Exercise 22 in Chapter 3 yields skein polynomials of links.
   (b) In particular, show that for a positive integer c, the element u_c corresponding to an unlink with c components is given by $u_c = (R + L)^{c-1}$.

8. If there is a containment relation $\mathbf{V} \subseteq \mathbf{W}$ between quasigroup varieties $\mathbf{V}$ and $\mathbf{W}$, show that the exponent of $\mathbf{W}$ is a multiple of the exponent of $\mathbf{V}$.

9. If Q' is a subquasigroup of a quasigroup Q, show that the exponent of Q is a multiple of the exponent of Q'.

10. If Q' is a quotient of a quasigroup Q, show that the exponent of Q is a multiple of the exponent of Q'.

11. Let Q be a Moufang loop with identity element e. Show that the exponent of Q is 0 if Q contains a subloop isomorphic to $(\mathbb{Z}, +, 0)$. Otherwise, show that the exponent of Q is the least positive integer n such that Q satisfies the identity $x^n = e$.

12. A variety $\mathbf{V}$ of quasigroups is said to be *anti-associative* if it contains no non-trivial groups (compare [57] for the loop case). Show that a quasigroup variety of exponent 1 is anti-associative.

13. Give an example of an anti-associative quasigroup variety of exponent larger than 1.

14. Verify the equations (11.11).

15. Show that a commutative loop is a Moufang loop if and only if it satisfies the identity (11.13).

16. Verify that the congruences (11.16) specify $J\mathbb{Z}\widetilde{G}_e$ for $\mathbb{Z}^2$ in the variety **CML** of commutative Moufang loops.

17. Show that (11.18) gives an isomorphism from $\mathbb{Z}^3 \oplus (\mathbb{Z}/3\mathbb{Z})$ to the domain of the principal bundle.

18. Let n be an integer greater than 2. Show that the free group of exponent 3 on n generators is the multiplication group of the free commutative Moufang loop of exponent 3 and nilpotence class 2 on n generators.

19. Write out the identities connecting the first few morphisms ε_n^i and δ_n^i in the simplicial category Δ.

20. Verify that the free resolution is a simplicial object.

11.8 Problems

1. Which universally finite quasigroup varieties of positive exponent are locally finite?

2. Does the set of universally finite varieties have maximal elements? Does its complement have minimal elements?

3. Can methods similar to those of Section 11.5 be used to construct free commutative Moufang loops of higher rank?

4. For which varieties $\mathbf{V}$ does the Eilenberg-Loginov construction (11.19) suffice for the construction of modules?

5. In general, the free resolution used in Section 11.6 is very large. For which quasigroup varieties $\mathbf{V}$ is a smaller free resolution available?

11.9 Notes

Section 11.1

The term "groupoid" is occasionally used as a synonym for "magma." However, a *groupoid* is generally defined as a category in which each arrow is invertible.

The description of the free magma on one generator is originally due to Minc [116]. Minc' "bifurcating root-trees" are finite (rooted) binary trees in modern jargon. His abstractly defined "index ψ-polynomials" become the derivatives (11.2) within the context of banal modules. The elements of the free magma in Exercise 5(c) are Minc' "index θ-polynomials." The elements of the free magma in Exercise 5(d) are his "index χ-polynomials."

Section 11.3

As an alternative to the use of Exercise 33 from Chapter 1 for the proof of Theorem 11.3, one may note that in the construction of [129], X has rank 0, while $XR(q_1)R(q_2)\dots R(q_r)$ has rank r. In the language of that paper, $Q[X]$ is the free extension of the partial system $Q \cdot \{X\}$.

Section 11.6

Full details of the results summarized in this section may be found in [147, Ch. 6]. A more general and abstract description of monadic cohomology was given by Duskin [49]. Note that the term *monadic cohomology* has replaced the older "triple cohomology." A cohomology theory for varieties of loops was given in [90]. The loop case is more straightforward, because of the pointing by identity elements.

Chapter 12

ANALYTICAL CHARACTER THEORY

This chapter introduces the analytical characters of a finite quasigroup Q with element e, as almost-periodic functions on the stabilizer of e in the universal multiplication group $U(Q;\mathbf{Q})$ of Q. Although the finite-dimensional complex representations of a finite group are determined up to equivalence by its ordinary characters, the corresponding combinatorial characters of Q, as treated in Chapters 6 and 7, are inadequate for the task of classifying all the so-called *ordinary* Q-modules, the finite-dimensional complex vector spaces in the slice category $\mathbf{Q}/Q$. As shown by Theorem 12.4, this classification is achieved by the analytical characters.

The chapter is organized around various spaces of complex-valued functions. Section 12.1 looks at the space $L^!(Q)$ of functions $f : Q \to \mathbb{C}$. The combinatorial character theory of Q defines so-called "generalized Laplace operators" on this space. If Q has s conjugacy classes and basic characters, then it has s generalized Laplace operators $\Delta_1, \ldots, \Delta_s$. The ordinary representation theory of Q furnishes coefficient functions f_m in $L^1(Q)$ for each element m of $M = p^{-1}\{e\}$ in a Q-module $p : E \to Q$. One thus studies the behavior of the coefficient functions under the generalized Laplace operators. The intimate connection between modules and characters in the group case is interpreted in this theory as Theorem 12.1. The limitations of the approach are readily seen in the ordinary representation theory of the singleton quasigroup. There the unique generalized Laplace operator Δ_1 on the 1-dimensional space $L^1(\{e\})$ cannot hope to classify the rich supply of modules.

As an intermediate step towards the analytical character theory which does classify modules, Section 12.2 looks at periodic functions on groups. These are complex-valued functions that remain invariant under translation by a subgroup of finite index. The space $L^1(Q)$ is embedded into the space $P(\widetilde{G})$ of periodic functions on the universal multiplication group $\widetilde{G} = U(Q;\mathbf{Q})$ of Q, and the generalized Laplace operators are extended from $L^1(Q)$ to $P(\widetilde{G})$. The Laplace operator Δ_1 is related to the Laplace operator used in harmonic analysis on free groups (Theorem 12.2).

The actual analytical character theory for classifying modules is given in Section 12.3, in terms of almost-periodic functions on the stabilizer $\widetilde{G}_e$ of e in the universal multiplication group $\widetilde{G}$. Almost-periodic functions on the universal stabilizer $\widetilde{G}_e$ correspond to continuous complex-valued functions on a

compact topological group constructed from $\widetilde{G}_e$, its "Bohr compactification." In essence the ordinary representation theory of Q reduces to the ordinary representation theory of this compact group. Working with compact groups in the category of topological spaces is just like working with finite groups in the category of sets. One can thus classify Q-modules by their corresponding characters, which are almost-periodic functions on the universal stabilizer $\widetilde{G}_e$.

Section 12.4 broadens consideration to the space $AP(\widetilde{G})$ of almost-periodic functions on the full universal multiplication group $\widetilde{G}$. The spaces $L^1(Q)$ and $P(\widetilde{G})$ embed into $AP(\widetilde{G})$, and the generalized Laplace operators extend to $AP(\widetilde{G})$. The space $AP(\widetilde{G})$ is thus viewed as the location in which to study the relationships between the combinatorial and analytical character theories, together with the ordinary representation theory of the quasigroup Q. A typical task for such a study is the investigation in the final sections of solutions of the Laplace equations $\Delta_i u = 0$ in $AP(\widetilde{G})$, as a generalization of the observation (Theorem 12.7) that the unique solution of Laplace's equation $\Delta_1 u = 0$ on the closed convex hull of the set of left translates of an almost-periodic function f on $\widetilde{G}$ is the Neumann mean of f,

12.1 Functions on finite quasigroups

Given a finite, nonempty quasigroup Q, let $L^1(Q)$ denote the set of all functions $f : Q \to \mathbb{C}$, with algebra structure induced pointwise from $\mathbb{C}$. The quasigroup structure on Q furnishes certain operators on $L^1(Q)$, defined from the combinatorial character theory. For $1 \leq i \leq s$, define $H_i(x, y) = \eta_{ij}$ for (x, y) in the quasigroup conjugacy class C_i. Then for f in $L^1(Q)$, define $\Delta_i f$ in $L^1(Q)$ by

$$\Delta_i f(q) = f_i(q) - \sum_{r \in Q} H_i(q, r) f(r)\,. \tag{12.1}$$

In particular,

$$\Delta_1 f(q) = f(q) - \frac{1}{|Q|} \sum_{r \in Q} f(r)\,.$$

In view of Theorem 12.2 below, Δ_1 is called the *Laplace operator* on $L^1(Q)$, while the Δ_i are called *generalized Laplace operators* on $L^1(Q)$.

Certain Q-modules give rise to complex-valued finctions on Q. Suppose that $p : E \to Q$ is a Q-module over $\mathbb{C}$. For a fixed element e of Q, the $\widetilde{G}_e$-module $M = p^{-1}\{e\}$ induces a $\widetilde{G}$-module $M^{\widetilde{G}}$. As in Section 10.3, identify Q with its isomorphic image in E under 0_Q. Then $E \setminus Q$ is a subset of $M^{\widetilde{G}}$. If $M^{\widetilde{G}}$ has a $\widetilde{G}$-invariant inner product $\langle\ ,\ \rangle$, then E is said to be a *unitary Q-module*. For such a module E, and for q in Q, let $\langle\ ,\ \rangle_q$ denote the restriction of the

invariant inner product on $M^{\widetilde{G}}$ to $p^{-1}\{q\}$. By analogy with the definition (10.21) of the quasigroup product on E as $a \cdot b = aR(bp) + bL(ap)$, define a form $\{\ ,\ \}$ on E by

$$\{a, b\} = \langle aR(bp), bL(ap)\rangle_{ap\cdot bp}\,. \tag{12.2}$$

This form may be calculated from knowledge of the $\widetilde{G}_e$-module M with its $\widetilde{G}_e$-invariant inner product $\langle\ ,\ \rangle_e$ as follows.

LEMMA 12.1
For m, n in M and x, y in Q,

$$\{(m, x), (n, y)\} = \Big\langle ms\big(x, R(y)\big), ns\big(y, L(x)\big)\Big\rangle_e\,.$$

PROOF By (12.2),

$$\begin{aligned}\{(m, x), (n, y)\} &= \langle (m, x)R(y), (n, y)L(x)\rangle_{xy}\\ &= \Big\langle \Big(ms\big(x, R(y)\big), xy\Big), \Big(ns\big(y, L(x)\big), xy\Big)\Big\rangle_{xy}\\ &= \Big\langle \Big(ms\big(x, R(y)\big), e\Big), \Big(ns\big(y, L(x)\big), e\Big)\Big\rangle_{e}\\ &= \Big\langle ms\big(x, R(y)\big), ns\big(y, L(x)\big)\Big\rangle_e\,.\end{aligned}$$

□

For an element m of M, a so-called *coefficient function* f_m in $L^1(Q)$ is defined by

$$f_m(q) = \{(m, q), (m, e)\}\,. \tag{12.3}$$

If Q is a group, the traditional link between the ordinary representation theory of Q and the combinatorial character theory of Q is that the group class functions ψ_i' determined by the basic combinatorial characters ψ_i are the traces of the matrices of the irreducible representations. This link is interpreted in the current theory as follows.

THEOREM 12.1
Let Q be a finite group with identity element e, and M an ordinary irreducible Q-module with character ψ_i'. Take M as a $\widetilde{G}_e$-module via (10.37)*. Let m be an element of M that has unit length $\langle m, m\rangle_e$ under the $\widetilde{G}_e$-invariant inner product $\langle\ ,\ \rangle$ on M. Then the coefficient function f_m is an eigenfunction for all the generalized Laplace operators. It lies in the kernel of Δ_i, and is fixed by each Δ_j for $j \neq i$.*

PROOF Extend $\{m\}$ to an orthonormal basis of M, and take matrices of the automorphisms of M representing Q with respect to this basis. Let q in Q be represented by the matrix $[a_{kl}^{(i)}(q) \mid 1 \leq k, l \leq \dim M = \psi_i'(e)]$. Then by Lemma 12.1,

$$\begin{aligned} f_m(q) &= \{(m,q),(m,e)\} \\ &= \langle ms(q,R(e)), ms(e,L(q))\rangle_e \\ &= \langle mR(q)R(q)^{-1}, mL(q)R(q)^{-1}\rangle_e \\ &= \langle m, mT_e(q)^{-1}\rangle_e = \langle mT_e(q), m\rangle_e = a_{11}^{(i)}(q)\,. \end{aligned}$$

For each positive integer $j \leq s$ distinct from i, let $[a_{ln}^{(j)}(q)]$ be the matrix of q in an irreducible representation with character ψ_j'. For q, r in Q, one has

$$H_j(q,r) = |Q|^{-1}\psi_j'(e)\psi_j(r,q) = |Q|^{-1}\psi_j'(e)\psi_j'(qr^{-1})\,.$$

Then

$$\begin{aligned} \sum_{r\in Q} H_j(q,r)f_m(r) &= \sum_{r\in Q} |Q|^{-1}\psi_j'(e)\psi_j'(qr^{-1})f_m(r \\ &= |Q|^{-1}\psi_j'(e)\sum_{r\in Q}\sum_{k=1}^{\psi_j'(e)} a_{kk}^{(j)}(qr^{-1})a_{11}^{(i)}(r) \\ &= |Q|^{-1}\psi_j'(e)\sum_{k=1}^{\psi_j'(e)}\sum_{r\in Q} a_{kk}^{(j)}(qr^{-1})a_{11}^{(i)}(r) \\ &= |Q|^{-1}\psi_j'(e)\sum_{k=1}^{\psi_j'(e)} a_{k1}^{j}(q)\delta_{1k}\delta_{ji}|Q|\psi_j'(e)^{-1} \\ &= a_{11}^{j}(q)\delta_{ji} = \delta_{ij}f_m(q)\,, \end{aligned}$$

the fourth equality using the general orthogonality condition [35, p. 219] for matrix coefficients of irreducible representations. Thus

$$\Delta_j f_m(q) = f_m(q) - \sum_{r\in Q} H_j(q,r)f_m(r) = f_m(q)(1-\delta_{ij})\,,$$

as required. □

For general quasigroups Q in a variety $\mathbf{V}$, the generalized Laplace operators do not possess sufficient resolving power to distinguish the coefficient functions of the various inequivalent irreducible unitary Q-modules in $\mathbf{V}$, to the extent demonstrated by Theorem 12.1 for the case $Q \in \mathbf{G} = \mathbf{V}$. The extreme example of this is where $Q = \{e\}$ and $\mathbf{V} = \mathbf{Q}$. There are many irreducible ordinary representations of the singleton quasigroup, but the kernel of the unique (generalized) Laplace operator of Q is still all of $L^1(Q)$.

12.2 Periodic functions on groups

As the preceding section showed, the combinatorial character theory of a finite nonempty quasigroup Q is generally inadequate for classifying the unitary representations of Q. A substitute must be found. That substitute is the analytical character theory developed in the next section. The theory uses almost-periodic functions on the universal stabilizer $\widetilde{G}_e$ of an element e of Q in the universal multiplication group $\widetilde{G}$. As an intermediate step, the present section examines periodic functions on groups. Functions on a finite quasigroup Q will be interpreted as periodic functions on the full group $\widetilde{G}$, and a connection will be made between the Laplace operators on $L^1(Q)$ and on $\widetilde{G}$.

A complex-valued function f on a group G is said to be *left invariant* under a subgroup H, or *left H-invariant*, if

$$\forall\, h \in H\,, \forall\, x \in G\,, f(hx) = f(x)\,.$$

In other words, f is constant on each $\mathrm{LMlt}_G H$-orbit in G. Right invariance is defined similarly. Finally, a function f is said to be *bi-invariant* under H or *H-bi-invariant* if it is both left and right invariant, or constant on each $\mathrm{Mlt}_G H$-orbit in G.

LEMMA 12.2
For $f : G \to \mathbb{C}$, the following conditions are equivalent:

(a) *There is a subgroup H of finite index in G under which f is left invariant;*

(b) *There is a subgroup H' of finite index in G under which f is right invariant;*

(c) *There is a subgroup H'' of finite index in G under which f is bi-invariant;*

(d) *There is a normal subgroup K of finite index in G under which f is bi-invariant.*

PROOF Clearly (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d). It will be shown that (a) $\Rightarrow$ (d); the proof of (b) $\Rightarrow$ (d) is similar. Suppose that f is left H-invariant, so that f is constant on each coset Hx. Let K be the kernel of the permutation representation $g \mapsto (Hx \mapsto Hxg)$ of G on the homogeneous space $H\backslash G$. Then K is a normal subgroup of G, and $|K\backslash G| \leq |H\backslash G|!$, so that K has finite index in G. Since K fixes H, it is a subgroup of H, making f left K-invariant. Then for x in G and k in K, one has $f(xk) = f(xkx^{-1} \cdot x) = f(x)$ since $xkx^{-1} \in K$, so that f is also right K-invariant. ∎

DEFINITION 12.1 *On a group G, a complex-valued function f satisfying the equivalent conditions of Lemma 12.2 is called a* periodic function *on G. The subgroups H, H' and H'' are called* periods *of f. More specifically, H is a* left period*, H' is a* right period*, H'' is a* bilateral period*, and K is a* normal period*,*

Let $P(G)$ denote the set of all periodic functions on G. If f and g are in $P(G)$, with respective left periods H and K, then $f - g$ and fg are in $P(G)$, each with left period $H \cap K$. Note that

$$\begin{aligned} |(H \cap K)\backslash G| &= |(H \cap K)\backslash H| \cdot |H\backslash G| \\ &= |K\backslash HK| \cdot |H\backslash G| \leq |K\backslash G| \cdot |H\backslash G| < \infty\,. \end{aligned}$$

Thus $P(G)$ becomes a $\mathbb{C}$-algebra. If T is a right transversal to $H \cap K$ in G, define

$$\langle f, g\rangle = \frac{1}{|T|}\sum_{t\in T} f(t)\overline{g(t)}\,. \tag{12.4}$$

To see that this is well-defined, let U be a right transversal to a subgroup L of finite index m in $H \cap K$, with

$$U \cap (H \cap K)t = \{k_{1t}t, \ldots, k_{mt}t\} \tag{12.5}$$

for each t in T. Then

$$\frac{1}{|U|}\sum_{u\in U} f(u)\overline{g(u)} = \frac{1}{|U|}\sum_{t\in T}\sum_{i=1}^{m} f(k_{it})\overline{g(k_{it}t)} = \frac{1}{|T|}\sum_{t\in T} f(t)\overline{g(t)}\,,$$

since each k_{it} lies in $H \cap K$. Thus $P(G)$ becomes an inner product space. A convolution is defined as follows.

PROPOSITION 12.1
If f has bilateral period H, and g has left period K, then

$$f * g(x) = \frac{1}{|T|}\sum_{t\in T} f(x/t)g(t) \tag{12.6}$$

(for a right transversal T to $H \cap K$ in G) defines a convolution $f * g$ in $P(G)$ with left period H.

PROOF To see that $f * g$ is well-defined, let U be a right transversal to a subgroup L of finite index m in $H \cap K$, Take notation as in (12.5). Then

$$\frac{1}{|U|}\sum_{u\in U} f(x/u)g(u) = \frac{1}{|U|}\sum_{t\in T}\sum_{i=1}^{m} f(xt^{-1}k_{it}^{-1})g(k_{it}t) = \frac{1}{|T|}\sum_{t\in T} f(x/t)g(t)\,,$$

as required. For h in H, one has

$$f * g(hx) = \frac{1}{|T|}\sum_{t\in T} f(hxt^{-1})g(t) = \frac{1}{|T|}\sum_{t\in T} f(xt^{-1})g(t) = f * g(x)\,,$$

so that $f * g$ has left period H. □

If G is finite, then $P(G)$ under convolution becomes the usual complex group algebra (Exercise 1). If G is infinite, however, the formal convolution unit δ (with $\delta(1) = 1$ and $\delta(x) = 0$ for $x \neq 1$) is not periodic (Exercise 2).

A complex-valued function f on a finite quasigroup Q with element e corresponds to a left $\widetilde{G}_e$-invariant function

$$f^\sharp : \widetilde{G} \to \mathbb{C}; x \mapsto f(ex) \tag{12.7}$$

on the universal multiplication group $\widetilde{G} = U(Q; \mathbf{Q})$ of Q. This correspondence $\sharp : L^1(Q) \to P(\widetilde{G})$ is a $\mathbb{C}$-algebra monomorphism of $L^1(Q)$ into the algebra $P(\widetilde{G})$ of periodic functions on $\widetilde{G}$. Conversely, a left $\widetilde{G}_e$-invariant function f on $\widetilde{G}$ determines a function

$$f^\flat : Q \to \mathbb{C}; q \mapsto f(\rho(e, q))$$

in $L^1(Q)$. Note that functions $f : \mathrm{Mlt}\, Q \to \mathbb{C}$ correspond naturally to periodic functions $\widetilde{f} : \widetilde{G} \to \mathbb{C}$ having the kernel of the epimorphism $\widetilde{G} \to \mathrm{Mlt}\, Q$ as their normal period. According to [6, II(11.16)], an unnormalized convolution

$$(f \times g)(x) = \sum_{y\in \mathrm{Mlt}\, Q} f(x/y)g(y) \tag{12.8}$$

is defined on the space of all functions $f : \mathrm{Mlt}\, Q \to \mathbb{C}$. Under the correspondence with periodic functions on $\widetilde{G}$, one then has $\widetilde{f \times g} = |\mathrm{Mlt}\, Q|\widetilde{f} * \widetilde{g}$.

The generalized Laplace operators on $L^1(Q)$ extend to corresponding operators on $P(\widetilde{G})$. For $1 \leq i \leq s$, define the *signed measure*

$$\mu_i : \widetilde{G} \to \mathbb{C}; x \mapsto |Q| \cdot \overline{H_i(e, ex)}\,.$$

In terms of basic combinatorial characters, $\mu_i(x) = \psi_{i1}\psi_i(e, ex)$. Clearly μ_i is left $\widetilde{G}_e$-invariant. It is also right $\widetilde{G}_e$-invariant, since for h in $\widetilde{G}_e$ one has

$$|Q|^{-1}\mu_i(xh) = \overline{H_i(e, exh)} = \overline{H_i(eh^{-1}, ex)} = \overline{H_i(e, ex)} = |Q|^{-1}\mu_i(x)\,,$$

the second equality holding since H_i is a quasigroup class function.

PROPOSITION 12.2

For $1 \leq i \leq s$, the signed measure μ_i is an idempotent element of the algebra $P(\widetilde{G})$ under the convolution (12.6).

PROOF Define a function $\omega_i : \mathrm{Mlt}\, Q \to \mathbb{C}$ by setting $\omega_i(x) = \xi_{ji}/n_j$ when the pair (e, ex) lies in the quasigroup conjugacy class C_j. By [6, II, Cor. 11.7(i)], the function $f_i\omega_i/|\mathrm{Mlt}\, Q|$ is idempotent under the convolution (12.8). Thus $f_i\widetilde{\omega}_i$ is idempotent under the convolution (12.6). But for x in $\widetilde{G}$ with (e, ex) in C_j, one has

$$f_i\widetilde{\omega}_i(x) = f_i\xi_{ji}/n_j = |Q|\overline{\eta}_{ij} = \mu_i(x)\,,$$

the middle equality just being $\sqrt{f_i}$ times (6.30). □

PROPOSITION 12.3
For f in $L^1(Q)$, the equation

$$(\Delta_i f)^\sharp = f^\sharp - \mu_i * f^\sharp \tag{12.9}$$

holds in $P(\widetilde{G})$.

PROOF Since μ_i has bilateral period $\widetilde{G}_e$, and $f^\sharp$ has left period $\widetilde{G}_e$, the right hand side of (12.9) is a well-defined function on $\widetilde{G}$ with left period $\widetilde{G}_e$, according to Proposition 12.1. Then for x in $\widetilde{G}$, one has

$$\begin{aligned}
(\Delta_i f)^\sharp(x) &= \Delta_i f(ex) \\
&= f(ex) - \sum_{r\in Q} H_i(ex, r) f(r) \\
&= f(ex) - \sum_{r\in Q} \overline{H_i(r, ex)} f(r) \\
&= f^\sharp(x) - \sum_{r\in Q} \overline{H_i(e\rho(e,r), ex)} f^\sharp(\rho(e,r)) \\
&= f^\sharp(x) - \frac{1}{|Q|} \sum_{r\in Q} |Q| \cdot \overline{H_i(e, ex\rho(e,r)^{-1})} f^\sharp(\rho(e,r)) \\
&= f^\sharp(x) - \frac{1}{|T|} \sum_{t\in T} \mu_i(x/t) f^\sharp(t) \\
&= f^\sharp(x) - \mu_i(x) * f^\sharp(t)\,,
\end{aligned}$$

where T is the right transversal $\{\rho(e,r) \mid r \in Q\}$ to $\widetilde{G}_e$ in $\widetilde{G}$. □

DEFINITION 12.2 *Let $\widetilde{G} = U(Q, \mathbf{Q})$ be the universal multiplication group on the finite nonempty quasigroup Q. Then for $1 \le i \le s$, the* generalized Laplace operator *Δ_i on the space $P(\widetilde{G})$ of periodic functions on $\widetilde{G}$ is defined by*

$$\Delta_i f = f - \mu_i * f\,,$$

where $\mu_i(x) = \psi_i(e,e)\psi_i(e,x)$ *with* ψ_i *the i-th basic combinatorial character of* Q. *The operator* Δ_1 *is just called the* Laplace operator *on* $P(\widetilde{G})$.

Given Definition 12.2, Proposition 12.3 may be reformulated as

$$(\Delta_i f)^\sharp = \Delta_i f^\sharp$$

for f in $L^1(Q)$.

The reason for the terminology in (12.1) and Definition 12.2 will now be explained, and a connection made with some harmonic analysis on free groups [60]. Let F be the free group on a set A. For $g : F \to \mathbb{C}$, define $g^* : F \to \mathbb{C}$ by $g^*(x) = \overline{g(x^{-1})}$ [60, p. 3]. For each element a of A, difference operators D_a and D_a^* are defined by:

$$\begin{cases} D_a g(x) = g(xa) - g(x)\,; \\ D_a^* g(x) = g(xa^{-1}) - g(x)\,. \end{cases}$$

Then the operator

$$\Delta = \frac{1}{2|A|} \sum_{a \in A} D_a^* D_a$$

is called the *Laplace operator* [60, p. 51], by analogy with the classical Laplace operator

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$$

in Euclidean space $\mathbb{R}^3$, or with the operator Δ of Exercise 22 in Chapter 1.

THEOREM 12.2

Let Q *be a finite quasigroup with element* e. *Consider the universal multiplication group* $\widetilde{G}$ *of* Q *with the set* (2.49) *of free generators. Then for a function* f *in* $L^1(Q)$, *one has* $2\Delta f^{\sharp *} = (\Delta_1 f)^{\sharp *}$.

PROOF Denote the set

$$\big\{\rho(e,q), R(e\backslash e), T_e(e), T_e(q) \,\big|\, q \in Q \smallsetminus \{e\}\big\}$$

of (2.49) by A, and write B for the subset

$$\big\{\rho(e,q), R(e\backslash e) \,\big|\, q \in Q \smallsetminus \{e\}\big\}\,.$$

Then for x in $\widetilde{G}$,

$$\begin{aligned} 2\Delta f^{\sharp *}(x) &= \frac{1}{2|Q|}\sum_{a\in A}\Big(2f^{\sharp *}(x) - f^{\sharp *}(xa) - f^{\sharp *}(xa^{-1})\Big) \\ &= \frac{1}{2|Q|}\sum_{a\in A}\Big(2\overline{f^{\sharp}(x^{-1})} - \overline{f^{\sharp}(a^{-1}x^{-1})} - \overline{f^{\sharp}(ax^{-1})}\Big) \\ &= \frac{1}{2|Q|}\sum_{a\in A}\Big(2\overline{f(ex^{-1})} - \overline{f(ea^{-1}x^{-1})} - \overline{f(eax^{-1})}\Big)\,. \end{aligned}$$

For $q \in Q$ and $a = T_e(q)$, the summand $2\overline{f(ex^{-1})} - \overline{f(ea^{-1}x^{-1})} - \overline{f(eax^{-1})}$ vanishes, since $ea = e = ea^{-1}$. Thus

$$2\Delta f^{\sharp *}(x) = \frac{1}{2|Q|}\sum_{a\in B}\Big(2\overline{f^{\sharp}(x^{-1})} - \overline{f^{\sharp}(a^{-1}x^{-1})} - \overline{f^{\sharp}(ax^{-1})}\Big)\,.$$

Now $eB = Q = Qx^{-1} = eBx^{-1}$, so Bx^{-1} is a right transversal to $\widetilde{G}_e$ in $\widetilde{G}$. Further $Q = e/Q = e\backslash Q = e/(e\backslash Q) = eR(e\backslash Q)^{-1}$. Since $eR(e\backslash e)^{-1} = e$, it follows that

$$eR\Big(e\backslash\big(Q \smallsetminus \{e\}\big)\Big)^{-1} = Q \smallsetminus \{e\}\,,$$

and again

$$e\rho\big(e, Q \smallsetminus \{e\}\big)^{-1} = \big(Q \smallsetminus \{e\}\big)R(e\backslash e) = Q \smallsetminus \{e\}\,.$$

Thus

$$eB^{-1} = Q = Qx^{-1} = eB^{-1}x^{-1}\,,$$

so $B^{-1}x^{-1}$ is also a right transversal to $\widetilde{G}_e$ in $\widetilde{G}$. Let $T = Bx^{-1}$ and $U = B^{-1}x^{-1}$. Then $2\Delta f^{\sharp *}(x)$

$$\begin{aligned} &= \frac{1}{2}\Big(\overline{f^{\sharp}(x^{-1})} - \frac{1}{|T|}\sum_{t\in T}\overline{f^{\sharp}(t)}\Big) + \frac{1}{2}\Big(\overline{f^{\sharp}(x^{-1})} - \frac{1}{|U|}\sum_{u\in U}\overline{f^{\sharp}(u)}\Big) \\ &= \frac{1}{2}\Big(\overline{f^{\sharp}(x^{-1})} - \frac{1}{|T|}\sum_{t\in T}\overline{\mu_1(x^{-1}t^{-1})f^{\sharp}(t)}\Big) \\ &\quad + \frac{1}{2}\Big(\overline{f^{\sharp}(x^{-1})} - \frac{1}{|U|}\sum_{u\in U}\overline{\mu_1(x^{-1}t^{-1})f^{\sharp}(u)}\Big) \end{aligned}$$

$= \overline{\Delta_1 f^{\sharp}(x^{-1})} = (\Delta_1 f^{\sharp})^*(x)$, as required. □

12.3 Analytical character theory

This section sketches the outlines of an analytical character theory that serves to classify the finite-dimensional unitary representations of the finite

nonempty quasigroup Q, a task to which the combinatorial character theory proved unequal.

Let $\widetilde{G}$ be the universal multiplication group $U(Q;\mathbf{Q})$ of Q, and let e be a fixed element of Q. The universal stabilizer $\widetilde{G}_e$ may be regarded as a discrete topological group. As such, it is locally compact ([106, p. 7]: each element x of $\widetilde{G}_e$ has the closed compact neighborhood $\{x\}$). Since it is discrete but infinite, it is not compact. However, the forgetful functor from the category **CTG** of compact topological groups to the category **TG** of all topological groups has a left adjoint, called *Bohr compactification* [48, p. 37]. Thus there is a compact topological group $K = K(Q)$ and a continuous group homomorphism $\alpha : \widetilde{G}_e \to K$, the component at $\widetilde{G}_e$ of the unit of the adjunction, that is universal over all continuous group homomorphisms from $\widetilde{G}_e$ to a compact group [44, 16.1.1]. The Bohr compactification K is constructed by taking a set $\{\alpha_i : \widetilde{G}_e \to U(V_i) \mid i \in I\}$ of representatives for the equivalence classes of continuous representations $\alpha_i : \widetilde{G}_e :\to U(V_i)$ of $\widetilde{G}_e$ in the unitary groups $U(V_i)$ of finite-dimensional complex inner product spaces V_i. The group K is the closure of the image of $\widetilde{G}_e$ under $\prod_{i\in I}\alpha_i : \widetilde{G}_e \to \prod_{i\in I} U(V_i)$. Since the matrices $[a_{jk}]$ representing elements of $U(V_i)$ with respect to an orthonormal basis of V_i are those satisfying $\sum_j a_{jk}\overline{a}_{jl} = \delta_{kl}$, the groups $U(V_i)$ are compact. By the Tychonov Theorem [106, 5D], $\prod_{i\in I} U(V_i)$ is compact. Then K, as a closed subset of a compact space, is compact.

By the adjointness

$$\mathbf{TG}(\widetilde{G}_e, U(V_i)) \cong \mathbf{CTG}(K, U(V_i)), \tag{12.10}$$

there is a bijection between finite-dimensional continuous unitary representations of the Bohr compactification K and finite-dimensional unitary representations of $\widetilde{G}_e$ [44, 16.1.3]. An ordinary Q-module E or $p : E \to Q$ furnishes a finite-dimensional unitary $\widetilde{G}_e$-module $V = p^{-1}\{e\}$, which corresponds under (12.10) to a finite-dimensional continuous unitary representation $\sigma_E : K \to U(V)$ of K.

THEOREM 12.3

Each ordinary Q-module $p : E \to Q$ with $V = p^{-1}\{e\}$ is determined (up to equivalence) by the corresponding finite-dimensional continuous unitary representation $\sigma_E : K \to U(V)$ of the Bohr compactification $K = K(Q)$ of $\widetilde{G}_e$.

For a finite-dimensional continuous unitary representation $\sigma : K \to U(V)$ of the compact group K, a *character* χ_σ is defined by

$$\chi_\sigma : K \to \mathbb{C}; x \mapsto \operatorname{Tr}\sigma(x). \tag{12.11}$$

As for the case of ordinary representations of finite groups, the representation σ is determined up to equivalence by its character χ_σ [44, 15.3.6] [48, Ch. 7]. Thus:

PROPOSITION 12.4

Each ordinary Q-module E is determined up to equivalence by the continuous function $\chi_{\sigma_E} : K(Q) \to \mathbb{C}$.

As a free group, $\widetilde{G}_e$ is *residually finite* — the intersection of its subgroups of finite index is trivial. ([98, p. 414]: The free group on 2 generators embeds into $\mathrm{GL}_2(\mathbb{Z})$ as the free group on

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

Each nontrivial element of the image remains nontrivial on passage to some finite quotient $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.) It follows that the unit morphism $\alpha : \widetilde{G}_e \to K$ embeds $\widetilde{G}_e$ into K [44, 16.4.1]. An interesting corollary of this is the following [44, 16.4.4].

PROPOSITION 12.5

The universal stabilizer $\widetilde{G}_e$ of e in $\widetilde{G}$ is a limit of Lie groups.

By construction, K contains $\widetilde{G}_e$ as a dense subgroup. The continuous character χ_σ of a given finite-dimensional continuous unitary representation $\sigma : K \to U(V)$ of K is thus determined by its restriction to $\widetilde{G}_e$.

DEFINITION 12.3 *Let $p : E \to Q$ be an ordinary Q-module, and $\sigma_E : K \to U(p^{-1}\{e\})$ the corresponding finite-dimensional unitary continuous representation of the Bohr compactification $K = K(Q)$ of $\widetilde{G}_e$, as in Theorem 12.3. Then the* analytical character *χ_E of E is the restriction to $\widetilde{G}_e$ of the character $\chi_{\sigma_E} : K \to \mathbb{C}; x \mapsto \mathrm{Tr}\, \sigma_E(x)$ of σ_E.*

Restrictions to $\widetilde{G}_e$ of continuous complex-valued functions on its Bohr compactification K are known as *almost-periodic functions* on $\widetilde{G}_e$. Proposition 12.4 then leads to the following result showing how almost-periodic functions on $\widetilde{G}_e$ classify Q-modules.

THEOREM 12.4

Let E be an ordinary Q-module. Then E is classified up to equivalence by its analytical character χ_E, which is an almost-periodic function on the universal stabilizer $\widetilde{G}_e$ of e in Q.

12.4 Almost periodic functions

The final sections lay some foundations for a future study of the connections between the combinatorial and analytical character theories of a finite nonempty quasigroup Q in terms of almost-periodic functions on $\widetilde{G}$, the full universal multiplication group of Q. Since $\widetilde{G}$ is a free group, it embeds as a dense subgroup of its Bohr compactification $\widetilde{G}^b$ in the same way that $\widetilde{G}_e$ does. Almost-periodic functions on $\widetilde{G}$ are thus defined as the restrictions to $\widetilde{G}$ of continuous complex-valued functions on $\widetilde{G}^b$. However, they do admit an equivalent intrinsic description [44, 16.2.1] [106, §41].

Consider the (infinite-dimensional) complex vector space $\mathbb{C}^{\widetilde{G}}$ of all functions $f : \widetilde{G} \to \mathbb{C}$. For an element t of $\widetilde{G}$, the *right translate* of an element f of $\mathbb{C}^{\widetilde{G}}$ by t is

$$f^t : \widetilde{G} \to \mathbb{C}; x \mapsto f(x/t)$$

and the *left translate* is

$$^tf : \widetilde{G} \to \mathbb{C}; x \mapsto f(t\backslash x)\,.$$

If f is a periodic function on $\widetilde{G}$ with normal period K, then f^t and ^tf are also periodic with normal period K. Since $f(\widetilde{G}) = f^t(\widetilde{G}) = {}^tf(\widetilde{G})$, such f has at most $|K\backslash\widetilde{G}|!$ translates.

The complex vector space $B(\widetilde{G})$ of bounded functions $f : \widetilde{G} \to \mathbb{C}$ has a norm called the *uniform norm*, with $\|f\| = \sup\{|f(x)| \mid x \in \widetilde{G}\}$ [106, p. 14]. For the following result, see [44, 16.2.1].

THEOREM 12.5
The following conditions on a function f in $B(\widetilde{G})$ are equivalent:

(a) *The set of right translates of f has a compact closure in the uniform norm on $B(\widetilde{G})$;*

(b) *The set of left translates of f has a compact closure in the uniform norm on $B(\widetilde{G})$;*

(c) *The set of all translates of f has a compact closure in the uniform norm on $B(\widetilde{G})$;*

(d) *The function f is almost-periodic.*

A periodic function f on $\widetilde{G}$ is certainly bounded. Its set of left translates is finite, and so compact in the uniform norm on $B(\widetilde{G})$. Thus periodic functions on $\widetilde{G}$ are almost-periodic functions on $\widetilde{G}$. In particular, each periodic function

f on $\widetilde{G}$ is the restriction (to the dense subgroup $\widetilde{G}$) of a unique continuous function $f^b : \widetilde{G}^b \to \mathbb{C}$. The mapping

$$P(\widetilde{G}) \to \mathbb{C}\widetilde{G}^b; f \mapsto f^b$$

into the space $\mathbb{C}\widetilde{G}^b$ of continuous complex-valued functions on $\widetilde{G}^b$ is linear. The group $\widetilde{G}^b$, being compact, is unimodular [106, 30A], and so has a left, right, and inverse invariant measure called the *Haar integral* $\int g(x)dx$, In other words,

$$\int g(x)dx = \int g(tx)dx = \int g(xt)dx = \int g(x^{-1})dx$$

for all t in $\widetilde{G}^b$, while $\int 1dx = 1$ [106, §§29–30].

THEOREM 12.6

Let f be a periodic function on $\widetilde{G}$ with left period H, and let T be a right transversal to H in $\widetilde{G}$. Then

$$\int f^b(x)dx = \frac{1}{|T|}\sum_{t\in T} f(t)\,.$$

PROOF For a subset X of $\widetilde{G}$, let $\chi_X : \widetilde{G} \to \mathbb{C}$ denote the characteristic function with $\chi_X(x) = 1$ for x in X, and $\chi_X(x) = 0$ otherwise. Then

$$1 = \sum_{t\in T} \chi_{Ht}(x)$$

on $\widetilde{G}$, so

$$1 = \sum_{t\in T} \chi^b_{Ht}(x)$$

on $\widetilde{G}^b$. Now

$$\begin{aligned} 1 = \int 1dx &= \int \sum_{t\in T} \chi^b_{Ht}(x)dx = \sum_{t\in T}\int \chi^b_{Ht}(x)dx \\ &= \sum_{t\in T}\int \chi^b_{Ht}(xt^{-1})dx = \sum_{t\in T}\int \chi^b_H(x)dx\,, \end{aligned}$$

whence

$$\int \chi^b_H(x)dx = \int \chi^b_H(xt^{-1})dx = \int \chi^b_{Ht}(x)dx = \frac{1}{|T|}$$

for each t in T. Then

$$f(x) = \sum_{t\in T} f(t)\chi_{Ht}(x)\,,$$

so that

$$\int f^b(x)dx = \int \sum_{t\in T} f(t)\chi^b_{Ht}(x)dx = \sum_{t\in T} f(t)\int \chi^b_{Ht}(x)dx = \frac{1}{|T|}\sum_{t\in T} f(t)$$

as required. □

Let $L^1(\widetilde{G}^b)$ denote the space of functions $g : \widetilde{G}^b \to \mathbb{C}$ with $\int |g(x)|dx$ defined [106, §17]. The space $L^1(\widetilde{G}^b)$ carries a convolution given by

$$f * g(x) = \int f(xt)g(t^{-1})dt = \int f(x/t)g(t)dt$$

[106, 31A].

COROLLARY 12.1
For periodic functions f, g on $\widetilde{G}$, one has $(f * g)^b = f^b * g^b$.

The generalized Laplace operators Δ_i of Definition 12.2 on $P(\widetilde{G})$ may thus be extended to $L^1(\widetilde{G}^b)$, and hence to the space $AP(\widetilde{G})$ of almost-periodic functions on $\widetilde{G}$.

DEFINITION 12.4 *For $1 \le i \le s$, the* generalized Laplace operator Δ_i *on $L^1(\widetilde{G}^b)$ is defined by*

$$\Delta_i f = f - \mu^b_i * f\,.$$

The generalized Laplace operator Δ_i *on $AP(\widetilde{G})$ is defined by the restriction*

$$\Delta_i f = (\Delta_i f^b)\big|_{\widetilde{G}}\,.$$

As before, the Δ_1 are just called Laplace operators.

In terms of the Laplace operator on $AP(\widetilde{G})$, the theorem of J. Neumann on the existence of mean values of almost-periodic functions [44, 16.3.1], [106, 41D] may be reformulated as follows.

THEOREM 12.7
The uniformly closed convex hull of the set of left translates of an almost-periodic function f on $\widetilde{G}$ contains a unique solution u of Laplace's equation $\Delta_1 u = 0$, namely the constant function u that is the Neumann mean of f.

PROOF Laplace's equation

$$\Delta_1 u^b = u^b - \mu^b_1 * u^b = u^b - \int u^b dx = 0$$

is satisfied if and only u^b, and hence u, is constant. □

12.5 Twisted translation operators

For $1 \leq i \leq s$, and for an element t of $\widetilde{G}$, define the i-th *twisted translation operator* T_i^t on $B(\widetilde{G})$ by

$$T_i^t f(x) = \frac{\mu_i(t)}{\mu_i(1)} f(t\backslash x)\,. \tag{12.12}$$

Taking the trace of (6.29) gives $0 \neq \operatorname{Tr} E_i = \eta_{i1}|Q| = \overline{\mu_i(1)}$, so that (12.12) is always defined. Note that $T_1^t f$ is the left translate ${}^t f$. The subset $Z_i = \{\mu_i(t)/\mu_i(1) \mid t \in \widetilde{G}\}$ of $\mathbb{C}$ is finite, and contains $1 = \mu_i(1)/\mu_i(1)$. Set $M_i = \max\{|z| \mid z \in Z_i\}$. The number M_i is known as the i-th *modulus*. As a partial extension of Theorem 12.5, one has the following.

PROPOSITION 12.6
For each $1 \leq i \leq s$, the set

$$T_i f = \{T_i^t f \mid t \in \widetilde{G}\} \tag{12.13}$$

of i-th twisted translates of an almost-periodic function f on $\widetilde{G}$ has a compact closure in the uniform norm on $B(\widetilde{G})$.

PROOF Since f is almost periodic, Theorem 12.5 shows that for given $\varepsilon > 0$, there is a finite subset $\{f_1, \ldots, f_r\}$ of $B(\widetilde{G})$ such that $T_1 f$ is contained in the union $B_{\varepsilon/M_i(f_1)} \cup \cdots \cup B_{\varepsilon/M_i(f_r)}$ of balls of radius ε/M_i centered on the f_j. Consider a given i-th twisted translate $T_i^t f$ of f. Suppose $\|T_i^t f - f_j\| < \varepsilon/M_i$. Then $\|T_i^t f - \frac{\mu_i(t) f_j}{\mu_i(1)}\| = |\frac{\mu_i(t)}{\mu_i(1)}| \cdot \|T_i^t f - f_j\| < \varepsilon$. Thus $T_i f$ is contained in the union of the finite set $\{B_\varepsilon(z f_j) \mid z \in Z_i, 1 \leq j \leq r\}$ of balls of radius ε. In other words, the set $T_i f$ is totally bounded, and hence has a compact closure (compare [106, 41A]). □

The generalization of the existence statement of Theorem 12.7 may now be stated.

THEOREM 12.8 (***Existence Theorem***)
For $1 \leq i \leq s$, the equation $\Delta_i u = 0$ has a solution on the closed convex hull of the set $T_i f$ of twisted translates of any given almost periodic function f on $\widetilde{G}$.

Theorem 12.8 will be proved in the following section. The current section concludes with an example showing that a solution u of $\Delta_i u = 0$ on the closed convex hull of $T_i f$ need not be unique if $i > 1$.

Example 12.1
Let Q be the quasigroup $(\mathbb{Z}/4\mathbb{Z}, -)$ of integers modulo 4 under subtraction (compare Section 9.8). Taking the fixed element e of Q to be 0, note that $L^1(Q)$ embeds into $AP(\widetilde{G})$ via $f \mapsto f^\sharp$ with $f^\sharp$ as in (12.7). For this example, it is sufficient to work in $L^1(Q)$. Given q in Q, define $\delta_q : Q \to \mathbb{C}$ by $\delta_q(q) = 1$ and $\delta_q(Q \setminus \{q\}) = \{0\}$. Let $f = \delta_0$. Then $T_2 f = \{\delta_0, -\delta_1, \delta_2, -\delta_3\}$. The closed convex hull of this set of translates is a geometric 3-simplex. For g in $L^1(Q)$, the effect $\Delta_2 g$ of the Laplace operator Δ_2 is defined by

$$\Delta_2 g(y) = \frac{3}{4}g(y) - \frac{1}{4}g(y+2) + \frac{1}{4}g(y+1) + \frac{1}{4}g(y+3)$$

for y in Q. Thus 3 solutions u of $\Delta_2 u = 0$ on the closed convex hull of $T_2 f$ are $\frac{1}{4}\delta_0 - \frac{3}{4}\delta_1$, $\frac{1}{4}\delta_0 - \frac{3}{4}\delta_3$, and $\frac{1}{4}\delta_0 + \frac{3}{4}\delta_2$. The full set of solutions is the geometric 2-simplex spanned by these three solutions. ∎

12.6 Proof of the Existence Theorem

This section is devoted to the proof of Theorem 12.8. Fix i in the range $1 \le i \le s$. Let f be an almost-periodic function on $\widetilde{G}$. If $f = 0$, then $u = o \in \{0\} = T_i f$ solves $\Delta_i u = 0$. If $f \neq 0$, say $f(x^{-1}) \neq 0$ for some element x of $\widetilde{G}$, then $T_i T_1^x f = T_i f$ and $T_1^x f(1) = f(x^{-1}) \neq 0$, so without loss of generality one may assume $f(1) \neq 0$.

For a subset S of $\widetilde{G}$, let $\chi_S : \widetilde{G} \to \mathbb{C}$ denote the characteristic function with $\chi_S(S) = \{1\}$ and $\chi_S(\widetilde{G} \setminus S) = \{0\}$. Set $|Q| = n$, and let $\{H = H_1, \ldots, H_n\}$ be the set of cosets Ht of $H = \widetilde{G}_e$. Then $1 = \sum_{j=1}^n \chi_{H_j}$ in $B(\widetilde{G})$. The χ_{H_j} are periodic (having the subgroup H of index n as left period), and so are almost-periodic on $\widetilde{G}$. Under the ring operations induced componentwise from $\mathbb{C}$, the set $AP(\widetilde{G})$ of almost-periodic functions forms a ring [106, 41A]. Set $f_j = \chi_{H_j} f$, so that

$$f = f_1 + \cdots + f_n \tag{12.14}$$

for almost-periodic f_j vanishing off H_j. Suppose that f_j is nonzero, say $f_j(h_j) \neq 0$ for some $h_j \in H_j$. In particular, take $h_1 = 1$. Define a function $\phi_j : \widetilde{G} \to \mathbb{C}; x \mapsto f(xh_j)$. By Theorem 12.5, ϕ_j is almost-periodic, and $\phi_j(1) = f_j(h_j) \neq 0$. Consider the finite, nonempty subset

$$Z = \{f_j(h_j) \mid f_j \neq 0\}$$

of $\mathbb{C} \setminus \{0\}$. Take $m = \min\{|z| \mid z \in Z\}$.

Given $0 < \varepsilon < mnM_i$, it will be shown that there is a finite convex combination of translates of f differing by less that ε from a fixed solution u of $\Delta_i u = 0$ in the uniform norm on $B(\widetilde{G})$. The function u is taken

to be $\mu_i * f/\mu_i(1)$. Recall the idempotence of μ_i under convolution (12.6) given by Proposition 12.2. Moreover, as a consequence of the associativity of $*$ on $L^1(\widetilde{G}^b)$ [106, 31B], the convolution on $AP(\widetilde{G})$ is associative. Then $\mu_i * u = \mu_i * \mu_i * f/\mu_i(1) = \mu_i * f/\mu_i(1) = u$, so that $\Delta_i u = 0$.

The almost-periodic function ϕ_j on $\widetilde{G}$ is the restriction of a unique continuous function ϕ_j^b on $\widetilde{G}^b$. Thus there is a neighborhood V_j of the identity in $\widetilde{G}^b$ such that $V_j = V_j^{-1}$ and

$$x/y \in V_j \quad \Rightarrow \quad \left|\phi_j^b(x) - \phi_j^b(y)\right| < \frac{\varepsilon}{nM_i}\,. \tag{12.15}$$

If $f_j = 0$, take V_j to be V_1. Then set $V = \bigcap_{j=1}^n V_j$. Note $V = V^{-1}$.

LEMMA 12.3
The neighborhood V is contained in the closure $\overline{H}$ of $\widetilde{G}_e$. Indeed, $V \cap \widetilde{G} \subseteq \widetilde{G}_e$.

PROOF For v in $V \subseteq V_1$, condition (12.15) gives

$$|f_1^b(v) - f_1(1)| = |\phi_1^b(v) - \phi_1^b(1)| < \frac{\varepsilon}{nM_i} < m < |f_1(1)|\,,$$

so $f_1^b(v) \neq 0$. Since f_1 vanishes off $\widetilde{G}_e$, the point v must lie in the closure of $\widetilde{G}_e$. If v also lies in $\widetilde{G}$, then $f_1(v) \neq 0$ gives $v \in \widetilde{G}_e$. ∎

LEMMA 12.4
For x/y in V, one has

$$|f^b(x) - f^b(y)| < \frac{\varepsilon}{M_i}\,.$$

PROOF Suppose $x/y \in V$. If $f_j = 0$, the inequality

$$|f_j^b(x) - f_j^b(y)| < \frac{\varepsilon}{nM_i} \tag{12.16}$$

is automatic. Otherwise, write $x = \xi h_j$ and $y = \eta h_j$. Then

$$|f_j^b(x) - f_j^b(y)| = |f_j^b(\xi h_j) - f_j^b(\eta h_j)| = |\phi_j^b(\xi) - \phi_j^b(\eta)| < \frac{\varepsilon}{nM_i} \tag{12.17}$$

by (12.15), since $\xi/\eta = x/y \in V \subseteq V_j$. Now (12.14) yields $f^b = \sum_{j=1}^n f_j^b$. Then

$$\begin{aligned} |f^b(x) - f^b(y)| &= \Big|\sum_{j=1}^n f_j^b(x) - \sum_{j=1}^n f_j^b(y)\Big| \\ &\leq \sum_{j=1}^n \Big|f_j^b(x) - f_j^b(y)\Big| < \frac{\varepsilon}{M_i}\,, \end{aligned}$$

on summing the inequalities (12.16) and (12.17) over $j = 1, \ldots, n$. □

LEMMA 12.5
The function μ_i^b is constant on all translates aV of V with a in $\widetilde{G}$.

PROOF Consider a given translate aV. Lemma 12.3 shows that $aV \cap \widetilde{G}$ is contained in $a\widetilde{G}_e$. Since the function μ_i has $\widetilde{G}_e$ as a right period, it is constant on the dense subset $aV \cap \widetilde{G}$ of aV. Thus the continuous function μ_i^b is constant on aV. □

In the free group $\widetilde{G}$, the intersection of all the subgroups K of finite index is the singleton consisting of the identity element. Thus in $\widetilde{G}^b$, the intersection of all the closures $\overline{K}$ of the subgroups K of finite index is again the singleton consisting of the identity element. This means that the topological group $\widetilde{G}^b$ forms a Fréchet or T_1-space. It follows [106, 28D] that $\widetilde{G}^b$ forms a Hausdorff or T_2-space. Since $\widetilde{G}^b$ is also compact, it is normal [106, 3B], and thus Urysohn's Lemma applies [106, 3C]. Taking the complement of V and the singleton $\{v\}$ of a point v of V as the closed sets F_0, F_1, one may use Urysohn's Lemma to construct a continuous function $h : \widetilde{G} \to [0, 1]$ to the closed unit interval, vanishing outside V and with $h(v) = 1$. Consider the nonempty open subset $U = h^{-1}(]0, 1])$ of V. The set $\{aU \mid a \in \widetilde{G}\}$ of all translates of U covers the compact space $\widetilde{G}^b$, and thus contains a finite subcover $\{a_1U, \ldots, a_rU\}$. Now $\sum_{k=1}^r T_1^{a_k} h(x) > 0$ for all x in $\widetilde{G}^b$, so that $g_k = \big(T_1^{a_k} h\big) / \sum_{l=1}^r T_1^{a_l} h$ is a well-defined continuous nonnegative function on $\widetilde{G}^b$ for $1 \le k \le r$. Define $c_k = \int g_k(x)dx$. The nonnegative coefficients $c_1, \ldots, c_r$ satisfy $\sum_{k=1}^r c_k = 1$. It will be shown that for each element y of $\widetilde{G}^b$, the value $u^b(y)$ of the solution of the generalized Laplace equation differs by less than ε from the convex combination $\sum_{k=1}^r c_k \big(T_i^{a_k} f\big)^b$ of twisted translates of f.

Now

$$\begin{aligned}
&\Big| u^b(y) - \sum_{k=1}^r c_k \big(T_i^{a_k} f\big)^b(y) \Big| \\
&\quad = \mu_i(1)^{-1} \Big| \mu_i^b * f^b(y) - \sum_{k=1}^r \int g_k(x) \mu_i^b(a_k) f^b(a_k \backslash y) dx \Big| \\
&\quad = \mu_i(1)^{-1} \Big| \sum_{k=1}^r \int g_k(x) \big(\mu_i^b(x) f^b(x \backslash y) - \mu_i^b(a_k) f^b(a_k \backslash y) \big) dx \Big| .
\end{aligned}$$

The k-th integrand is only nonzero where $g_k(x)$ is nonzero, namely for x within the translate a_kV. Since such x and a_k both lie in a_kV, Lemma 12.5 shows that $\mu_i^b(x) = \mu_i^b(a_k)$. Further, since $(x\backslash y)/(a_k\backslash y) = x\backslash a_k \in V^{-1} = V$, Lemma 12.4 shows that $|f^b(x\backslash y) - f^b(a_k\backslash y)| < \varepsilon / M_i$. But $|\mu_i^b(x)/\mu_i(1)| < M_i$,

so that

$$\begin{aligned}
&\Big|u^b(y) - \sum_{k=1}^{r} c_k \big(T_i^{a_k} f\big)^b(y)\Big| \\
&\quad = \Big|\sum_{k=1}^{r} \int g_k(x) \frac{\mu_i^b(x)}{\mu_i(1)} \big(f^b(x\backslash y) - f^b(a_k\backslash y)\big) dx\Big| \\
&\quad \le \sum_{k=1}^{r} \int g_k(x) \Big|\frac{\mu_i^b(x)}{\mu_i(1)}\Big| \cdot \big|f^b(x\backslash y) - f^b(a_k\backslash y)\big| dx \\
&\quad < \sum_{k=1}^{r} \int g_k(x) M_i(\varepsilon/M_i) dx = \varepsilon \int \Big(\sum_{k=1}^{r} g_k(x)\Big) dx = \varepsilon\,,
\end{aligned}$$

as required to complete the proof of the theorem.

12.7 Exercises

1. For a finite group G, show that the $\mathbb{C}$-algebra $P(G)$ under the convolution (12.6) is isomorphic to the complex group algebra $\mathbb{C}G$.

2. For an infinite group G, show that the formal convolution unit δ is not periodic.

3. Show that for almost all finite quasigroups Q, there is a periodic function on $\widetilde{G}$, with normal period K, that has exactly $|K\backslash\widetilde{G}|!$ translates.

4. Show that $t \mapsto T_1^t$ yields a representation of $\widetilde{G}$.

5. Under what circumstances does $t \mapsto T_i^t$ (for $1 < i \le s$) yield a representation of $\widetilde{G}$?

12.8 Problems

1. Given a quasigroup Q in a variety $\mathbf{V}$, determine to what extent the generalized Laplace operators of Q discriminate between the various irreducible unitary Q-modules in $\mathbf{V}$. Two particular cases of interest are:

   (a) $\mathbf{V}$ the variety of Moufang loops;

   (b) $\mathbf{V}$ a universally finite variety.

2. A finite-dimensional unitary Q-module $p : E \to Q$ with $M = p^{-1}\{e\}$ furnishes a finite-dimensional unitary representation $M^{\widetilde{G}}$ of $\widetilde{G}$. This representation has a character (according to [44, 15.3.6]) which restricts to an almost-periodic function on $\widetilde{G}$. How does this function behave under the generalized Laplace operators Δ_i on $AP(\widetilde{G})$?

3. Is the converse of Proposition 12.6 false for those i for which the signed measure μ_i may take the value zero?

4. In the context of Theorem 12.8, find a general method to determine the shape of the full set of solutions u of $\Delta_i u = 0$ on the closed convex hull of $T_i f$. Note that for f in $L^1(Q)$ or $P(\widetilde{G})$, this is a purely combinatorial problem.

5. Give a treatment of the material of this chapter using Hopf algebra techniques.

12.9 Notes

Section 12.4

Loomis [106, §41] takes property (b) of Theorem 12.5 as a definition of a ("left") almost-periodic function, and then constructs a realization of the Bohr compactification as the maximal ideal space of the commutative C^*-algebra formed by these functions.

Section 12.5

The Existence Theorem first appeared in [149].

Section 12.6

The proof of the Existence Theorem given here is modeled on the proof of the existence part of Theorem 12.7 given in [106, 41D].

Appendix A

CATEGORICAL CONCEPTS

A.1 Graphs and categories

A *directed graph* or *quiver* $C = (C_0, C_1, \partial_0, \partial_1)$ consists of two classes C_0, C_1 and two maps $\partial_0 : C_1 \to C_0$, $\partial_1 : C_1 \to C_0$. Elements of C_0 are called *vertices*, *points*, or *objects*. Elements of C_1 are called *edges*, *arrows*, or *morphisms*. The map ∂_0 is variously called the *tail* or *domain map*. The map ∂_1 is variously called the *head* or *codomain map*. An edge f is often depicted in the form $f : x \to y$ or $x \xrightarrow{f} y$ to indicate that $f\partial_0 = x$ and $f\partial_1 = y$. For a given pair (x, y) of vertices, set

$$C(x, y) = \{f \in C_1 \mid f\partial_0 = x\,, f\partial_1 = y\}. \tag{A.1}$$

A vertex or object t of C is said to be *terminal* if $C(x, t)$ is a singleton for each object x of C. The graph C is said to be *small* if the classes C_0 and C_1 are sets. The graph is *locally small* if the class (A.1) is a set for each pair (x, y) of vertices. Usually, graphs are implicitly assumed to be locally small. A pair (f, g) of edges is said to be *composable* if $f\partial_1 = g\partial_0$, i.e., if the head of f is the tail of g:

$$f\partial_0 \xrightarrow{f} f\partial_1 = g\partial_0 \xrightarrow{g} g\partial_1\,.$$

The class of composable pairs of edges, denoted by $C_1 \times_{C_0} C_1$, is the domain of projections $\pi_i : (f_0, f_1) \mapsto f_i$ for $i = 0, 1$. The *opposite* or *dual* of the directed graph $C = (C_0, C_1, \partial_0, \partial_1)$ is the graph $C^{\mathrm{op}} = (C_0, C_1, \partial_1, \partial_0)$. Thus duality of graphs reverses arrows. If (f, g) is a composable pair in C, then (g, f) is a composable pair in C^{op}.

A *category* $C = (C_0, C_1, \partial_0, \partial_1, 1, \mu)$ is a graph $(C_0, C_1, \partial_0, \partial_1)$ equipped with a *composition*

$$\mu : C_1 \times_{C_0} C_1 \to C_1; (f, g) \mapsto fg$$

satisfying $\mu\partial_0 = \pi_0\partial_0\,, \mu\partial_1 = \pi_1\partial_1$, and an *identity map*

$$1 : C_0 \to C_1; x \mapsto 1_x$$

retracting ∂_0 and ∂_1, such that

$$1_x f = f = f1_y \tag{A.2}$$

for all $x, y \in C_0\,, f \in C(x, y)$. The associative law $(fg)h = f(gh)$ is required to hold for composable pairs (f, g) and (g, h). The *opposite* or *dual* of the category C is the dual graph C^{op} equipped with the identity (A.2) and the multiplication $(g, f) \mapsto g \circ f := fg$. (Recall that composable pairs (g, f) in C^{op} correspond to composable pairs (f, g) in C.) Thus duality of categories reverses the order of composition.

A morphism $m : y \to z$ in a category C is a *monomorphism* if for all morphisms $f : x \to y$ and $g : x \to y$ in C, the equation $fm = gm$ implies $f = g$. Dually, a morphism $e : z \to y$ is an *epimorphism* if for all morphisms $f : y \to x$ and $g : y \to x$ in C, the equation $ef = eg$ implies $f = g$. (Note the reversal of the order of composition.) A morphism $f : x \to y$ is said to be an *isomorphism* if there is a morphism $g : y \to x$ such that $fg = 1_x$ and $gf = 1_y$. In this case, the objects x and y are said to be *isomorphic* in C. Isomorphism in C is an equivalence relation.

Given objects x and y of a category C, their *product* is an object $x \times y$ of C, equipped with *projection* arrows $p : x \times y \to x$ and $q : x \times y \to y$, such that for each object z and arrows $f : z \to x$, $g : z \to y$, there is a unique arrow $f \times g$ or $(f, g) : z \to x \times y$ such that $(f, g)p = f$ and $(f, g)q = g$. This so-called *universality property* of the product may be expressed in the form of a diagram

$$\begin{array}{ccccc} x & \xleftarrow{\ p\ } & x \times y & \xrightarrow{\ q\ } & y \\ \| & & \uparrow{\scriptstyle (f,g)} & & \| \\ x & \xleftarrow{\ f\ } & z & \xrightarrow{\ g\ } & y \end{array} \tag{A.3}$$

known as the *product diagram*. The *coproduct* or *sum* of x and y in C is an object $x + y$ of C, equipped with *insertion* arrows $i : x \to x + y$ and $j : y \to x + y$, such that for each object z and arrows $f : x \to z$, $g : y \to z$, there is a unique arrow $f + g : x + y \to z$ such that $i(f + g) = f$ and $j(f + g) = g$. Products and coproducts are dual: the coproduct of x and y in C is the product of x and y in C^{up}. Note that products and coproducts are only determined to within isomorphism. For example, in the category **Set** of sets and functions, the product of two sets X and Y may be realized by the "set-theoretical" construction

$$X \times Y = \{\{x, \{x, y\}\} \mid x \in X\,, y \in Y\}$$

or by the Cartesian construction

$$X \times Y = \{(x, y) \mid x \in X\,, y \in Y\}$$

of ordered pairs. The sum or coproduct $X+Y$ is the disjoint union, which may be realized as $(X \times \{0\}) \cup (Y \times \{1\})$ with insertions $i : X \to X+Y; x \mapsto (x, 0)$ and $j : Y \to X + Y; y \mapsto (y, 1)$.

For a map $I \to C_0; i \mapsto x_i$ from a set I to the object class of a category C, the *product* $\prod_{i \in I} x_i$ is an object of C, coming equipped with *projections*

$\pi_i : \prod_{i\in I} x_i \to x_i$ for each i in I, such that for each object z of C and arrow $f_i : z \to x_i$ for each i in I, there is a unique arrow $f = \prod_{i\in I} f_i : z \to \prod_{i\in I} x_i$ such that $f\pi_i = f_i$ for each i in I. If $I = \{0, 1\}$, then $\prod_{i\in I} x_i$ is just $x_0 \times x_1$. If I is empty, then the product object $\prod_{i\in I} x_i$ is terminal in C. If the map $I \to C_0$ takes the constant value x, then $\prod_{i\in I} x_i$ is called the *power* x^I. The zeroth power X^0 of any object of the category of sets is the empty product, a terminal object or arbitrary singleton $\{*\}$.

Given arrows $f : x \to z$ and $g : y \to z$ in a category C, their *pullback* is an object $x \times_z y$ of C, equipped with *projection* arrows $p : x \times_z y \to x$ and $q : x \times_z y \to y$, such that for each object t of C and arrows $h : t \to x$, $k : t \to y$ satisfying $tf = tg$, there is a unique arrow $h \times_z k$ or $(h, k) : t \to x \times_z y$ such that $(h, k)p = h$ and $(h, k)q = k$. The pullback is usually displayed as in the following diagram:

$$\begin{array}{ccc} x \times_z y & \xrightarrow{\ q\ } & y \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle g} \\ x & \xrightarrow[\ f\ ]{} & z \end{array} \tag{A.4}$$

In a small category C, the set $C_1 \times_{C_0} C_1$ of composable pairs is the pullback of the head and tail maps of C in the category **Set**.

A.2 Natural transformations and functors

A *graph map* $F : D \to C$ from a directed graph D to a directed graph C consists of two functions, a *vertex map* or *object part* $F_0 : D_0 \to C_0$ and an *edge map* or *morphism part* $F_1 : D_1 \to C_1$, such that for each pair x, y of vertices of D, the map F_1 restricts to

$$F_1 : D(x, y) \to C(xF_0, yF_0).$$

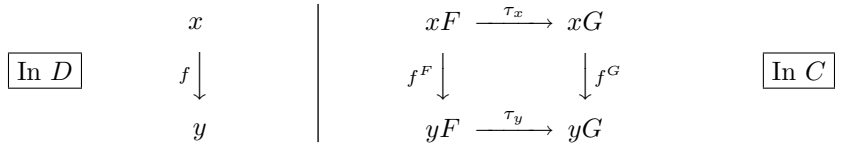
The respective suffices 0 and 1 on the object and morphism parts are usually suppressed. Here are two examples:

- The *identity map* $1_D : D \to D$ on a graph D comprises the respective identity maps 1_{D_0} and 1_{D_1} on the vertex and edge classes.
- If C is a category, and c is an object of C, then the *constant map* $[c] : D \to C$ takes each vertex of the graph D to c and each arrow of the graph D to 1_c.

A *path* in a directed graph D is a sequence $e_1, \ldots, e_l$ of edges such that each pair (e_1, e_2), $\ldots$, (e_{l-1}, e_l) is composable. A *diagram* in a category C is a graph map $F : D \to C$ with codomain C. The diagram is said to *commute*

if for each pair of paths $(e_1, \ldots, e_l)$, $(f_1, \ldots, f_m)$ in D with common starting point $e_1\partial_0 = f_1\partial_0$ and end point $e_l\partial_1 = f_m\partial_1$, the composite morphisms $e_1^F \ldots e_l^F$ and $f_1^F \ldots f_m^F$ in C agree. For example, the universality property of the product is expressed by the commuting of the diagram (A.3).

Given two diagrams $F : D \to C$ and $G : D \to C$ with common domain graph D and codomain category C, a *natural transformation* $\tau : F \to G$ is a vector having a component $\tau_x : xF \to xG$ in $C(xF, xG)$ for each vertex x of D, such that the *naturality property* $f^F\tau_y = \tau_x f^G$ is satisfied for each edge $f : x \to y$ of D. The naturality corresponds to the commuting of the diagram in C on the right-hand side of the picture



for every arrow $f : x \to y$ in D displayed on the left-hand side of the picture.

A (*covariant*) *functor* $F : D \to C$ from a category D to a category C is a graph map satisfying the *functoriality properties* $1_xF = 1_{xF}$ for all objects x of D and

$$(fg)^F = f^F g^F \tag{A.5}$$

for all composable pairs (f, g) of D. A *contravariant functor* $F : D \to C$ from a category D to a category C is a covariant functor from D to C^{op}.

An *adjunction* $(F, G, \eta, \varepsilon)$ consists of a *left adjoint* functor $F : D \to C$, a *right adjoint* functor $G : C \to D$, a *unit* natural transformation $\eta : 1_D \to FG$, and a *counit* natural transformation $\varepsilon : GF \to 1_C$, such that $\eta_x^F \varepsilon_{xF} = 1_{xF}$ for all objects x of D and $\eta_{yG}\varepsilon_y^G = 1_{yG}$ for all objects y of C. Such an adjunction is often summarized by the isomorphism

$$C(xF, y) \cong D(x, yG) \tag{A.6}$$

for objects x of D and y of C. under which a morphism $g : xF \to y$ maps to $\eta_x g^G$, while a morphism $f : x \to yG$ maps to $f^F\varepsilon_y$. In particular, η_x corresponds to 1_{xF} and ε_y corresponds to 1_{yG}. The adjunction provides an *equivalence* between the categories C and D if the components η_x and ε_y of the unit and counit are always (natural) isomorphisms.

Example A.1

For a characteristic example of an adjunction, take C to be the category **Mon** of monoids and monoid homomorphisms, with D as the category **Set** of sets. The right adjoint is the underlying set functor $G : \mathbf{Mon} \to \mathbf{Set}$, while the left adjoint $F : \mathbf{Set} \to \mathbf{Mon}$ takes a set X, considered as an alphabet, to the free monoid X^* of words in the alphabet X (with the empty word as the identity element). Words are multiplied by concatenation. The component

$\eta_X : X \to X^*$ at a set X embeds letters (elements) from X into X^* as one-letter words. For a monoid Y, the counit $\varepsilon_Y : Y^* \to Y$ takes a word in the alphabet Y to the product of its letters computed in the monoid Y. Under the isomorphism (A.6), a function $f : X \to Y$ from a set X to (the underlying set of) a monoid Y is mapped to its canonical extension to a monoid homomorphism from X^* to Y. Conversely, a monoid homomorphism $g : X^* \to Y$ is mapped to its restriction to the set X of one-letter words. □

A.3 Limits and colimits

Let $F : D \to C$ be a functor with small domain D. Then the *limit* $\varprojlim F$ of F is an object of C, equipped with a natural transformation $\pi : [\varprojlim F] \to F$ from its constant map to F, such that the following *limit property* holds:

> For all objects t of C and natural transformations $\kappa : [t] \to F$, there is a unique morphism $\varprojlim \kappa : t \to \varprojlim F$ such that $(\varprojlim \kappa)\pi_v = \kappa_v$ for all vertices v of D.

The natural transformation π, together with its components, are known as *projections* from the limit $\varprojlim F$. Limits have also been known as *projective limits* or *inverse limits*.

The pullback (A.4) is a typical example of a limit. The domain category consists of

$$u \to w \leftarrow v \tag{A.7}$$

together with the identity arrows at each of its vertices. The image of (A.7) under F is

$$x \xrightarrow{f} z \xleftarrow{g} y\,.$$

Then $\varprojlim F = x \times_z y$, while $\pi_u = p$ and $\pi_v = q$. By naturality, it follows that $\pi_w = pf = qg$. If $\kappa_u = h$ and $\kappa_v = k$, then $\varprojlim \kappa = h \times_z k$.

Dually, the *colimit* $\varinjlim F$ of F is an object of C, equipped with a natural transformation $\iota : F \to [\varinjlim F]$ from F to its constant map, such that the following *colimit property* holds:

> For all objects t of C and natural transformations $\kappa : F \to [t]$, there is a unique morphism $\varinjlim \kappa : \varinjlim F \to t$ such that $\iota_v(\varinjlim \kappa) = \kappa_v$ for all vertices v of D.

The natural transformation ι, together with its components, are known as *insertions* into the colimit $\varinjlim F$. Colimits have also been known as *inductive limits* or *direct limits* (sometimes under restrictions on the domain D of the functor F).

A category C is said to be *complete* if it has all limits, and *cocomplete* if it has all colimits. It is *bicomplete* if it is both complete and cocomplete.

Appendix B

UNIVERSAL ALGEBRA

B.1 Combinatorial universal algebra

A *type* $\tau : \Omega \to \mathbb{N}$ is a function whose codomain is the set of natural numbers. (Note that $\mathbb{N}$, as the set of cardinalities of finite sets, includes the cardinality 0 of the empty set. The set of positive integers is denoted by $\mathbb{Z}^+$.) Elements of the domain of τ are called the *basic operators* of the type. An *algebra of type* τ or τ*-algebra* A or (A, Ω) is a set A equipped with *basic operations*

$$\omega : A^{\omega\tau} \to A; (a_1, \ldots, a_{\omega\tau}) \mapsto a_1 \ldots a_{\omega\tau}\omega \tag{B.1}$$

for each basic operator. The class of all such algebras is denoted by $\underline{\tau}$. A subset B of A is a *subalgebra* of (A, Ω) if

$$\forall \omega \in \Omega,\ (\forall 1 \leq i \leq \omega\tau,\ x_i \in B) \Rightarrow x_1 \ldots x_{\omega\tau}\omega \in B. \tag{B.2}$$

Since intersections of subalgebras are subalgebras, each subset X of A determines a smallest subalgebra $\langle X \rangle$ of A containing X, known as the *subalgebra generated by* X. Given a family of algebras (A_i, Ω), their product $\prod A_i$ forms an algebra $\prod(A_i, \Omega)$ or $(\prod A_i, \Omega)$, the *product algebra*, under componentwise operations. A function $f : (A, \Omega) \to (B, \Omega)$ between algebras is said to be a *homomorphism* if its *graph*

$$\{(a, b) \in A \times B \mid af = b\} \tag{B.3}$$

is a subalgebra of $(A \times B, \Omega)$. (Note that it is often convenient to identify a function with its graph.) Bijective homomorphisms are called *isomorphisms*. An equivalence relation V on an algebra A is a *congruence* if it is a subalgebra of $(A \times A, \Omega)$. This implies that the *natural projection*

$$\operatorname{nat} V : A \to A^V; a \mapsto a^V, \tag{B.4}$$

mapping an element a of A to its equivalence class $a^V = \{b \in A \mid a\, V\, b\}$ in the *quotient* $A^V = \{a^V \mid a \in A\}$, is a homomorphism. Conversely, the *kernel*

$$\ker f = \{(a, a') \in A^2 \mid af = a'f\} \tag{B.5}$$

of a homomorphism $f : A \to B$ is a congruence on the domain of the homomorphism. An algebra (A, Ω) is *simple* if it is not the domain of a nontrivial,

noninjective homomorphism. In other words, its only congruences are the *diagonal* $\widehat{A} = \{(a, a) \mid a \in A\}$ and the *universal* or improper congruence $A \times A$.

Given a set L, the *free monoid* L^* over L is the set of all *words* $l_1 l_2 \dots l_n$ with l_i in L and n in $\mathbb{N}$ (compare Example A.1). Words are multiplied by concatenation; the unit element is the empty word ($n = 0$). Given a set X, let $X + \Omega$ be the disjoint union of X with Ω. The free monoid $(X + \Omega)^*$ over $X + \Omega$ becomes a τ-algebra under

$$\omega : (w_1, \dots, w_{\omega\tau}) \mapsto w_1 \dots w_{\omega\tau}\omega \tag{B.6}$$

for each basic operator ω. Define $X\Omega$, the *word algebra* or *algebra of τ-words in X*, to be the subalgebra of $((X + \Omega)^*, \Omega)$ generated by X.

PROPOSITION B.1

Each function $f : X \to A$ from a set X to the underlying set of a τ-algebra (A, Ω) extends to a unique homomorphism $\overline{f} : (X\Omega, \Omega) \to (A, \Omega)$.

PROOF The graph of $\overline{f}$ is the subalgebra of $(X\Omega \times A, \Omega)$ generated by the graph of f. □

Now fix a set D of *variables* or *arguments* by a bijection

$$\beta : \mathbb{Z}^+ \to D; n \mapsto x_n. \tag{B.7}$$

Make the power set 2^D into a τ-algebra by

$$\omega : (A_1, \dots, A_{\omega\tau}) \mapsto A_1 \cup \dots \cup A_{\omega\tau} \tag{B.8}$$

for ω in Ω. By Proposition B.1, there is a homomorphism

$$\arg : D\Omega \to 2^D; x_n \mapsto \{x_n\}, \tag{B.9}$$

called the *argument map*. Note $\arg(x_1 \dots x_{\omega\tau}\omega) = \{x_1, \dots, x_{\omega\tau}\}$. Since the argument map sends each element of $D\Omega$ to a finite subset of D, there is a well-defined function

$$\tau' : D\Omega \to \mathbb{N}; w \mapsto \max(\beta^{-1}(\arg w)) \tag{B.10}$$

called the *derived type* of τ. Elements of $D\Omega$ are called *derived operators* of τ. Given a τ-algebra (A, Ω), one obtains a τ'-algebra $(A, D\Omega)$ with *derived operations*

$$u : A^{u\tau'} \to A; (a_1, \dots, a_{u\tau'}) \mapsto u\overline{(x_i \mapsto a_i)}. \tag{B.11}$$

In other words, u acts on A by sending $(a_1, \dots, a_{u\tau'})$ to the image of u under the homomorphic extension $\overline{f} : D\Omega \to A$ of the function $f : D \to A; x_i \mapsto a_i$.

It is convenient to write a derived operator u in the form $x_1 \dots x_{u\tau'} u$, so that (B.11) becomes

$$u : A^{u\tau'} \to A; (a_1, \dots, a_{u\tau'}) \mapsto a_1 \dots a_{u\tau'} u. \tag{B.12}$$

One may identify a basic operator ω with the corresponding derived operator $x_1 \dots x_{\omega\tau}\omega$.

Finally, fix a τ-algebra (A, Ω). For a subset Δ of $D\Omega$, and restriction $\sigma : \Delta \to \mathbb{N}$ of $\tau' : D\Omega \to \mathbb{N}$, the σ-algebra (A, Δ) is called a *reduct* of the τ-algebra (A, Ω). Subalgebras of such reducts are called *subreducts* of the original algebra (A, Ω).

B.2 Categorical universal algebra

Given a class $\mathbf{V}$ of algebras of type τ, the category $\mathbf{V}$ (same symbol) will denote the category whose object class is the class $\mathbf{V}$, and such that, for given $\mathbf{V}$-algebras A and B, the set $\mathbf{V}(A, B)$ of morphisms from A to B is the set of all homomorphisms from A to B. The category $\mathbf{V}$ is the domain of two forgetful functors, the *inclusion*

$$G : \mathbf{V} \hookrightarrow \underline{\underline{\tau}} \tag{B.13}$$

and the *underlying set functor*

$$U : \mathbf{V} \longrightarrow \mathbf{Set}; \big(f : (A, \Omega) \to (B, \Omega)\big) \mapsto (f : A \to B) \tag{B.14}$$

to the category **Set** of sets and functions. Proposition B.1 shows that the functor $U : \underline{\underline{\tau}} \to \mathbf{Set}$ has a left adjoint $\Omega : \mathbf{Set} \to \underline{\underline{\tau}}$. For a set X, the unit $\eta_X : X \to X\Omega U$ just construes an element x of X as a one-letter word. For a τ-algebra (A, Ω), the counit

$$\varepsilon_A : AU\Omega \to A \tag{B.15}$$

is the homomorphic extension of the identity function $AU \to A; a \mapsto a$ given by Proposition B.1. In particular, for each basic operator ω, the counit ε_A maps a word $a_1 \dots a_{\omega\tau}\omega$ in $AU\Omega$ to the corresponding element $a_1 \dots a_{\omega\tau}\omega$ of A given by the image of (B.1).

A class $\mathbf{V}$ of algebras of type τ is a *prevariety* if isomorphic copies, subalgebras, and products of $\mathbf{V}$-algebras are again $\mathbf{V}$-algebras. If $\mathbf{V}$ is a prevariety, then the forgetful functors (B.13) and (B.14) each have left adjoints. The left adjoint of the inclusion $G : \mathbf{V} \hookrightarrow \underline{\underline{\tau}}$ is the *replication functor* R_V or $R : \underline{\underline{\tau}} \to \mathbf{V}$. The unit of the adjunction, for a τ-algebra A, is the surjective corestriction $\eta_A : A \to ARG$ of the product of the set of natural projections $\operatorname{nat} \alpha : A \to A^\alpha$

of congruences α on A whose quotient lies in $\mathbf{V}$. In other words, η_A is the natural projection of the smallest congruence ρ_V or ρ on A whose quotient A^ρ lies in $\mathbf{V}$. The congruence ρ is called the $\mathbf{V}$-*replica congruence* of A, and the corresponding quotient A^ρ in $\mathbf{V}$ is called the $\mathbf{V}$-*replica* of A.

The left adjoint of $U : \mathbf{V} \to \mathbf{Set}$ is the *free* $\mathbf{V}$-*algebra functor* $V : \mathbf{Set} \to \mathbf{V}$. The unit $\eta_X : X \to XVU$ of the adjunction, for a set X, is the composite of the unit $\eta_X : X \to X\Omega U$ of the adjunction

$$(\Omega : \mathbf{Set} \to \underline{\underline{\tau}}, U : \underline{\underline{\tau}} \to \mathbf{Set}, \eta, \varepsilon)$$

and (the image under $U : \mathbf{V} \to \mathbf{Set}$ of) the unit $\eta_{X\Omega} : X\Omega \to X\Omega RG$ of the adjunction

$$(R : \underline{\underline{\tau}} \to \mathbf{V}, G : \mathbf{V} \to \underline{\underline{\tau}}, \eta, \varepsilon).$$

In other words, the adjunction

$$(V : \mathbf{Set} \to \mathbf{V}, U : \mathbf{V} \to \mathbf{Set}, \eta, \varepsilon)$$

is the composite of these two given adjunctions. Two τ-words in X are said to be $\mathbf{V}$-*synonymous* if they are related by the replica congruence ρ_V on $X\Omega$. Thus the free $\mathbf{V}$-algebra on a set X is the algebra of $\mathbf{V}$-synonymy classes.

Fix a type $\tau : \Omega \to \mathbb{N}$. An *identity* in the type τ is a pair (u, v) of derived operators of τ. It is often convenient to write the identity (u, v) in the form $x_1 \dots x_{u\tau'} u = x_1 \dots x_{v\tau'} v$. For example, in the type $\{(\mu, 2)\}$ of a binary "multiplication" μ, the associative law is $x_1 x_2 \mu x_3 \mu = x_1 x_2 x_3 \mu\mu$, or equivalently $(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3)$ using infix notation for the multiplication. A τ-algebra (A, Ω) is said to *satisfy* the identity (u, v) if the derived operations u and v coincide on A.

For a class $\mathbf{V}$ of τ-algebras, let $\mathsf{H}\mathbf{V}$ denote the class of homomorphic images of algebras in $\mathbf{V}$. Similarly, let $\mathsf{S}\mathbf{V}$ and $\mathsf{P}\mathbf{V}$ denote the respective classes of subalgebras and products of algebras in $\mathbf{V}$. The most famous theorem in universal algebra is the following [15].

THEOREM B.1 (***Birkhoff's Theorem***)
A class $\mathbf{V}$ *of* τ*-algebras is the class of all* τ*-algebras satisfying a given set of identities if and only if* $\mathbf{V} = \mathsf{HSP}\mathbf{V}$.

A *variety* is a class $\mathbf{V}$ of τ-algebras satisfying the two equivalent conditions of Birkhoff's Theorem. Note that a variety is a prevariety. The full set of identities satisfied by each algebra from a variety $\mathbf{V}$ is the $\mathbf{V}$-replica congruence ρ_V on the algebra $D\Omega$ of derived operators.

Appendix C

COALGEBRAS

C.1 Coalgebras and covarieties

This appendix summarises the basic facts about coalgebras. For details, readers may consult [68], [69], or [136]. Crudely speaking, coalgebras are just the duals of algebras: coalgebras in a category C are algebras in the dual category C^{op}. To understand algebras in the right context for this duality, consider the case of monoids as discussed in Example A.1. There, the composite FG or ${}^*G : \mathbf{Set} \to \mathbf{Set}$ is an *endofunctor* on the category of sets, a functor from the category to itself. The monoid structure on the underlying set M of a monoid M (informal notation!) is then specified by the image

$$\eta^G_M : M^*G \to M \tag{C.1}$$

of the counit at M under the functor G. The function (C.1) is considered as the *structure map* of the monoid M.[1] Note that a function $f : M \to N$ between two monoids is then a monoid homomorphism if and only if the equation

$$\eta^G_M f = f^{*G}\eta^G_N \tag{C.2}$$

is satisfied.

Let $F : \mathbf{Set} \to \mathbf{Set}$ be an endofunctor on the category of sets and functions. Then an *F-coalgebra*, or simply a *coalgebra* if the endofunctor is implicit in the context, is a set X equipped with a function α_X or

$$\alpha : X \to XF$$

— note the duality with (C.1). This function is known as the *structure map* of the coalgebra X. (Of course, for complete precision, one may always denote a coalgebra by its structure map.) A function $f : X \to Y$ between coalgebras is a *homomorphism* if and only if the equation

$$f\alpha_Y = \alpha_X f^F \tag{C.3}$$

[1] For a more general example of an algebraic structure map, one might consider the image of the counit (B.15) under the functor $U : \underline{\underline{\tau}} \to \mathbf{Set}$.

is satisfied. Again, note how (C.3) is dual to (C.2). A subset S of a coalgebra X is a *subcoalgebra* if it is itself a coalgebra such that the embedding of S in X is a homomorphism. A coalgebra Y is a *homomorphic image* of a coalgebra X if there is a surjective homomorphism $f : X \to Y$. A *bisimulation* between coalgebras X and Y is a binary relation $R \subseteq X \times Y$ affording a coalgebra structure such that the two set product projections $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ restrict to respective coalgebra homomorphisms $R \to X$ and $R \to Y$.

Let $(X_i \mid i \in I)$ be a family of coalgebras. The *sum* of the family is the disjoint union of the sets of the family, equipped with a coalgebra structure map α given as follows. Let $\iota_i : X_i \to X$ insert X_i as a summand in the disjoint union X of the family. For each i in I, let α_i be the structure map of X_i. Then the restriction of α to the subset X_i of X is given by $\alpha_i \iota_i^F$. (More generally, the forgetful functor from coalgebras to sets creates colimits — compare [8, Prop. 1.1].)

A *covariety* of coalgebras is a class of coalgebras closed under the operations H of taking homomorphic images, S of taking subcoalgebras, and Σ of taking sums. If $\mathbf{\Lambda}$ is a class of F-coalgebras, then the smallest covariety containing $\mathbf{\Lambda}$ is given by $\mathsf{SH}\Sigma\mathbf{\Lambda}$ — compare [68, Th. 7.5] or [69, Th. 3.3]. Since homomorphic images are dual to sub(co)algebras, while sums are dual to products, this result is dual to Birkhoff's Theorem B.1.

C.2 Set functors

Suppose that $F : \mathbf{Set} \to \mathbf{Set}$ is an endofunctor on the category of sets and functions. Many of the standard theorems about F-coalgebras depend on certain properties of the endofunctor F. This section summarizes the two properties needed for the results quoted in Chapter 5.

Given arrows $f : x \to z$ and $g : y \to z$ in a category D, their *weak pullback* is an object $x \times_z y$ of D, equipped with projection arrows $p : x \times_z y \to x$ and $q : x \times_z y \to y$, such that for each object t of D and arrows $h : t \to x$, $k : t \to y$ satisfying $tf = tg$, there is an arrow $h \times_z k$ or $(h, k) : t \to x \times_z y$ such that $(h, k)p = h$ and $(h, k)q = k$. (For $x \times_z y$ to be a pullback, the arrow $h \times_z k$ would be required to be unique.) Let $F : D \to C$ be a functor from a category D to a category C. Then F is said to *preserve weak pullbacks* if $xF \times_{zF} yF$ with projection arrows $pF : xF \times_{zF} yF \to xF$ and $qF : xF \times_{zF} yF \to yF$ is a weak pullback in C whenever $x \times_z y$ with projection arrows $p : x \times_z y \to x$ and $q : x \times_z y \to y$ is a weak pullback in D.

An endofunctor $F : \mathbf{Set} \to \mathbf{Set}$ on the category of sets is said to be *bounded* if there is a cardinal number κ such that for each F-coalgebra X and for each element x of X, the element x lies in a subalgebra S of X with $|S| < \kappa$.

References

[1] Adyan, S.I., *The Burnside Problem and Identities in Groups* (Russian), Nauka, Moscow, 1975.

[2] Albert, A.A., Quasigroups I, II, *Trans. Amer. Math. Soc.*, 54, 507–519, 1943; 55, 401–409, 1944.

[3] Albert, A.A., Ed., *Studies in Modern Algebra*, Prentice-Hall, Englewood Cliffs, NJ, 1963.

[4] Aschbacher, M., *Finite Group Theory*, Cambridge University Press, Cambridge, 1986.

[5] Baer, R., Nets and groups I, *Trans. Amer. Math. Soc.*, 46, 110–141, 1939.

[6] Bannai, E. and Ito, T., *Algebraic Combinatorics*, Benjamin-Cummings, Menlo Park, CA, 1984.

[7] Barnsley, M.F., *Fractals Everywhere*, Academic Press, San Diego, CA, 1988.

[8] Barr, M., Terminal coalgebras in well-founded set theory, *Theoret. Comput. Sci.*, 114, 299–315, 1993.

[9] Beck, J.M., Triples, Algebras, and Cohomology, Ph.D. thesis, Columbia University 1967, *Reprints in Theory and Applications of Categories*, 2, 1–59, 2003.

[10] Bělohlávek, R., A characterization of congruence classes of quasigroups, *Math. Slovaca*, 50, 377–380, 2000.

[11] Bělohlávek, R. and Chajda, I., Congruences and ideals in semiloops, *Acta Math. (Szeged)*, 59, 43–47, 1994.

[12] Belousov, V.D., On the structure of distributive quasigroups (Russian), *Mat. Sb.*, 50, 267–298, 1960.

[13] Belousov, V.D., *Foundations of the Theory of Quasigroups and Loops* (Russian), Nauka, Moscow, 1967.

[14] Billingsley, P., *Probability and Measure*, Wiley, New York, NY, 1979.

[15] Birkhoff, G., On the structure of abstract algebras, *Proc. Camb. Phil. Soc.*, 31, 433–454, 1935.

[16] Bodnarchuk, V.G., Kaluzhnin, L.A., Kotov, V.N., and Romov, B.A., Galois theory for Post algebras I, II, *Cybernetics*, 5, 243–252, 531–539, 1969.

[17] Bose, R.C. and Shimamoto, T., Classification and analysis of partially balanced designs with two associate classes, *J. Amer. Statist. Assoc.*, 47, 151–190, 1952.

[18] Boullion, T.L. and Odell, P.L., *Generalized Inverse Matrices*, Wiley, New York, NY, 1971.

[19] Bruck, R.H., Some results in the theory of quasigroups, *Trans. Amer. Math. Soc.*, 55, 19–52, 1944.

[20] Bruck, R.H., Contributions to the theory of loops, *Trans. Amer. Math. Soc.*, 60, 245–354, 1946.

[21] Bruck, R.H., *A Survey of Binary Systems*, Springer, Berlin, 1958.

[22] Burnside, W., On an unsettled question in the theory of discontinuous groups, *Quart. J. Pure and Appl. Math.*, 33, 230–238, 1902.

[23] Burnside, W., *Theory of Groups of Finite Order*, Dover, New York, NY, 1955.

[24] Cameron. P.J., *Permutation Groups*, Cambridge University Press, Cambridge, 1999.

[25] Cameron, P.J., Goethals, J.M., and Seidel, J.J., The Krein condition, spherical designs, Norton algebras and permutation groups, *Indag. Math.*, 81, 196–206, 1978.

[26] Chari, V. and Pressley, A.N., *A Guide to Quantum Groups*, Cambridge University Press, Cambridge, 1994.

[27] Chein, O., Lagrange's Theorem for M_k-loops, *Arch. Math.*, 24, 121–122, 1973.

[28] Chein, O. et al., *Quasigroups and Loops: Theory and Applications*, Heldermann, Berlin, 1990.

[29] Chernoff, H., A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, *Ann. Math. Stat.*, 23, 493–509, 1952.

[30] Choi, D.-H. and Smith, J.D.H., Greedy loop transversal codes for correcting error bursts, *Discrete Math.*, 264, 37–43, 2003.

[31] Connor, W.S., The uniqueness of the triangular association scheme, *Ann. Math. Statist.*, 29, 262–266, 1958.

[32] Conway, J.H., A simple construction of the Fischer-Griess monster group, *Inv. Math.*, 79, 513–540, 1985.

[33] Conway, J.H. and Smith, D.A., *On Quaternions and Octonions*, Peters, Natick, MA, 2002.

[34] Crowell, R.H., The derived group of a permutation representation, *Adv. in Math.*, 53, 99–124, 1984.

[35] Curtis, C.W. and Reiner, I., *Representation Theory of Finite Groups and Associative Algebras*, Interscience, New York, NY, 1962.

[36] Curtis, C.W. and Reiner, I., *Methods of Representation Theory I*, Wiley, New York, NY, 1981.

[37] Delsarte, P., An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.*, 10, 1973.

[38] Dershowitz, N. and Jouannaud, J.P., Rewrite systems, in *Handbook of Theoretical Computer Science, Vol. B: Formal Models and Semantics*, van Leeuwen, J., Ed., Elsevier, Amsterdam, 1990, 245–320.

[39] Dharwadker, A. and Smith, J.D.H., Split extensions and representations of Moufang loops, *Comm. in Alg.*, 23, 4245–4255, 1995.

[40] Diaconis, P., *Group Representations in Probability and Statistics*, Institute of Mathematical Statistics Lecture Notes-Monograph Series Vol. 11, Institute of Mathematical Statistics, Hayward, CA, 1988.

[41] Dijkgraaf, R. et al., The operator algebra of orbifold models, *Comm. Math. Phys.*, 123, 485–526, 1989.

[42] DiPaola, J.W. and Nemeth, E., Generalized triple systems and medial quasigroups, in *Proceedings of the Seventh Southeastern Conference on Combinatorics, Graph Theory and Computing, 1976*, Congressus Numerantium, No. XVII, Utilitas Math., Winnipeg, Manitoba, 1976, 289–306.

[43] Divinsky, N.J., Rings and Radicals, University of Toronto Press, Toronto, 1965.

[44] Dixmier, J., *Les C^*-Algèbres et leurs Représentations*, Gauthiers-Villars, Paris, 1964.

[45] Dixon, G.M., *Division Algebras: Octonions, Quaternions, Complex Numbers and the Algebraic Design of Physics*, Kluwer, Dordrecht, 1994.

[46] Doro, S., Simple Moufang loops, *Math. Proc. Camb. Phil. Soc.*, 83, 377–392, 1978.

[47] Drápal, A., On multiplication groups of relatively free quasigroups isotopic to abelian groups, *Czechoslovak Math. J.*, 55, 61–86, 2005.

[48] Dunkl, C. and Ramirez, D.E., *Topics in Harmonic Analysis*, Appleton-Century-Crofts, New York, NY, 1971.

[49] Duskin, J., Simplicial methods and the interpretation of "triple" cohomology, *Memoirs of the American Mathematical Society*, No. 163, 1975.

[50] Ebbinghaus, H.-D. et al., *Zahlen*, Springer, Berlin, 1983. English translation: *Numbers*, Springer, New York, NY, 1991.

[51] Eilenberg, S., Extensions of general algebras, *Ann. Soc. Polon. Math.*, 21, 125–134, 1948.

[52] Erdős, P. and Spencer, J., *Probabilistic Methods in Combinatorics*, Academic Press, New York, NY, 1974.

[53] Etherington, I.M.H., Non-associative arithmetics, *Proc. Roy. Soc. Edin.*, 62, 442–453, 1949.

[54] Euler, L., Recherches sur une nouvelle espèce de carrés magiques, *Mém. de la Societé de Vlissingue*, 9, pp. 85 ff., 1779.

[55] Evans, T., Homomorphisms of non-associative systems, *J. London Math. Soc.*, 24, 254–260, 1949.

[56] Evans, T., On multiplicative systems defined by generators and relations, *Proc. Camb. Phil. Soc.*, 47, 637–649, 1951.

[57] Evans, T., Identical relations in loops I, *J. Austral. Math. Soc.*, 12, 275–286, 1971.

[58] Feit, W., Some consequences of the classification of finite simple groups, *Proc. Sympos. Pure Math.* 37, 175–182, 1980.

[59] Feller, W., *An Introduction to Probability Theory and its Applications, Vol. I*, 2nd. Ed., Wiley, New York, NY, 1957.

[60] Figà-Talamanca, A. and Picardello, M.A., *Harmonic Analysis on Free Groups*, Dekker, New York, NY, 1983.

[61] Fox, R.H., Free differential calculus, *Ann. of Math.*, 57, 547–560, 1953.

[62] Gibson, C.G., *Elementary Geometry of Algebraic Curves*, Cambridge University Press, Cambridge, 1998.

[63] Glauberman, G., On loops of odd order II, *J. Alg.*, 8, 393–414, 1968.

[64] Glauberman, G. and Wright, C.R.B., Nilpotence of finite Moufang 2-loops, *J. Alg.*, 8, 415–417, 1968.

[65] Gluck, D., Idempotent formula for the Burnside algebra with applications to the p-subgroup simplicial complex, *Illinois J. Math.*, 25, 63–67, 1981.

[66] Grätzer, G. and Padmanabhan, R., On idempotent commutative and nonassociative groupoids, *Proc. Amer. Math. Soc.*, 29, 249–264, 1973.

[67] Griess, R.L., Jr., Code loops, *J. Alg.*, (100), 224–234, 1986.

[68] Gumm, H.-P., *Elements of the General Theory of Coalgebras*, LUATCS'99, Rand Afrikaans University, Johannesburg, 1999.

[69] Gumm, H.-P., Birkhoff's variety theorem for coalgebras, *Contributions to General Algebra*, 13, 159–173, 2001.

[70] Gumm, H.-P. and Schröder, T., Covarieties and complete covarieties, in *Coalgebraic Methods in Computer Science*, Jacobs, B. et al., Eds., Electronic Notes in Theoretical Computer Science, Vol. 11, Elsevier Science, 1998, 43–56.

[71] Gumm, H.-P. and Schröder, T., Products of coalgebras, *Alg. Univ.*, 46, 163–185, 2001.

[72] Gvaramiya, A.A. and Plotkin, B.I., The homotopies of quasigroups and universal algebras, in *Universal Algebra and Quasigroup Theory*, Romanowska, A. and Smith, J.D.H., Eds., Heldermann, Berlin, 1992, 89–99.

[73] Hagemann, J. and Herrmann, C., A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity, *Arch. Math.*, 32, 234–245, 1979.

[74] Häggkvist, R. and Janssen, J.C.M., All-even Latin squares, *Discrete Math.*, 157, 199–206, 1996.

[75] Hartley, B., A note on the normalizer condition, *Proc. Camb. Phil. Soc.*, 74, 11–15, 1973.

[76] Heineken, H. and Mohamed, I.J., A group with trivial centre satisfying the normalizer condition, *J. Alg.*, 10, 368–376, 1968.

[77] Heineken, H. and Mohamed, I.J., Groups with normalizer condition, *Math. Ann.*, 198, 179–188, 1972.

[78] Herrmann, C., Affine algebras in congruence modular varieties, *Acta Sci. Math.*, 41, 119–123, 1979.

[79] Heyer, H., Convolution semigroups of probability measures of Gel'fand pairs, *Expo. Math.*, 1, 3–45, 1983.

[80] Higman, G., Neumann, B.H., and Neumann, H., Embedding theorems for groups, *J. London Math. Soc.*, 24, 247–254, 1949.

[81] Hsu, F.-L., Hummer, F.A., and Smith, J.D.H., Logarithms, syndrome functions, and the information rates of greedy loop transversal codes, *J. Comb. Math. Comb. Comp.*, 22, 33–49, 1996.

[82] Hummer, F.A. and Smith, J.D.H., Greedy loop transversal codes, metrics, and lexicodes, *J. Comb. Math. Comb. Comp.*, 22, 143–155, 1996.

[83] Huppert, B., *Endliche Gruppen I*, Springer, Berlin, 1967.

[84] Ihringer, T., On multiplication groups of quasigroups, *Eur. J. Combinatorics*, 5, 137–141, 1984.

[85] Izbash, V.I., Isomorphisms of quasigroups isotopic to groups, *Quasigroups and Related Systems*, 2, 34–50, 1995.

[86] James, I.M., Quasigroups and topology, *Math. Zeitschr.*, 84, 329–342, 1964.

[87] Ježek, J., Normal subsets of quasigroups, *Comment. Math. Univ. Carol.*, 16, 77–85, 1975.

[88] Johnson, K.W., Loop transversals and the centralizer ring of a permutation group, *Math. Proc. Camb. Phil. Soc.*, 94, 411–416, 1983.

[89] Johnson, K.W., Some historical aspects of the representation theory of groups and its extension to quasigroups, in *Universal Algebra and Quasigroup Theory*, Romanowska, A. and Smith, J.D.H., Eds., Heldermann, Berlin, 1992, 101–117.

[90] Johnson, K.W. and Leedham-Green, C.R., Loop cohomology, preprint, 1978.

[91] Johnson, K.W. and Smith, J.D.H., Characters of finite quasigroups, *Europ. J. Combinatorics*, 5, 43–50, 1984.

[92] Johnson, K.W. and Smith, J.D.H., Characters of finite quasigroups II: induced characters, *Europ. J. Combinatorics*, 7, 131–137, 1986.

[93] Johnson, K.W. and Smith, J.D.H., Characters of finite quasigroups III: quotients and fusion, *Europ. J. Combinatorics*, 10, 47–56, 1989.

[94] Johnson, K.W. and Smith, J.D.H., Characters of finite quasigroups IV: products and superschemes, *Europ. J. Combinatorics*, 10, 257–263, 1989.

[95] Johnson, K.W. and Smith, J.D.H., Characters of finite quasigroups V: linear characters, *Europ. J. Combinatorics*, 10, 449–456, 1989.

[96] Johnson, K.W. and Smith, J.D.H., Characters of finite quasigroups VII: permutation characters, *Comment. Math. Univ. Carol.*, 45, 265–273, 2004.

[97] Johnson, K.W., Smith, J.D.H., and Song, S.Y., Characters of finite quasigroup VI: critical examples and doubletons, *Europ. J. Combinatorics*, 11, 267–275, 1990.

[98] Karras, A., Magnus, W., and Solitar, D., *Combinatorial Group Theory*, Wiley, New York, NY, 1966.

[99] Kepka, T. and Rosendorf, D., Quasigroups which are unions of three proper subquasigroups, *Acta Univ. Carolin. Math. Phys.*, 45, 55–66, 2004.

[100] Klin, M., Pöschel, R., and Rosenbaum, K., *Angewandte Algebra*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1988.

[101] Knuth, D.E. and Bendix, P.B., Simple word problems in universal algebras, in *Computational Problems in Abstract Algebra*, Leech, J., Ed., Pergamon, Oxford, 1970, 263–297.

[102] Krasner, M., Une généralisation de la notion de corps, *J. Math. Pures et Appl.*, 17, 367–385, 1938.

[103] Kurosh, A.G., *Theory of Groups*, Chelsea, New York, NY, 1958

[104] Liebeck, M.W., The classification of finite simple Moufang loops, *Math. Proc. Camb. Phil. Soc.*, 102, 33–47, 1987.

[105] Loginov, E.K., On linear representations of Moufang loops, *Comm. in Alg.*, 21, 2527–2536, 1993.

[106] Loomis, L.H., *An Introduction to Abstract Harmonic Analysis*, Van Nostrand, New York, NY, 1953.

[107] Loos, O., *Symmetric Spaces I: General Theory.* Benjamin, New York, NY, 1969.

[108] Łuczak, T. and Pyber, L., On random generation of the symmetric group, *Combin. Probab. Comput.*, 2, 505–512, 1993.

[109] Mack, G. and Schomerus, V., Conformal field algebras with quantum symmetry from the theory of superselection sectors, *Comm. Math. Phys.* 134, 139–196, 1990.

[110] Mal'tsev, A.I., On the general theory of algebraic systems (Russian), *Mat. Sb. N.S.*, 35 (77), 3–20, 1954. English translation by Alderson, H: *Amer. Math. Soc. Transl.*, 27, 125–140, 1963.

[111] Manin, Yu.I., *Cubic Forms* (Russian), Nauka, Moscow, 1972. English translation: *Cubic Forms*, North-Holland, Amsterdam, 1974.

[112] Meldrum, J.D.P., On the Heineken-Mohamed groups, *J. Alg.*, 27, 437–444, 1973.

[113] Mendelsohn, E., Every (finite) group is the automorphism group of a (finite) strongly regular graph, *Ars. Comb.*, 6, 75–86, 1978.

[114] Mendelsohn, N.S., Orthogonal Steiner systems, *Aequationes Math.*, 5, 268–272, 1970.

[115] Mendelsohn, N.S., A natural generalization of Steiner triple systems, in *Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969*, Academic Press, London, 1971, 323–338.

[116] Minc, H., Index polynomials and bifurcating root-trees, *Proc. Roy. Soc. Edin.*, A, 65, 319–341, 1957.

[117] Mitschke, A. and Werner, H., On groupoids representable by vector spaces over finite fields, *Arch. Math.*, 24, 14–20, 1973.

[118] Movsisyan, Yu.M., Hyperidentities in algebras and varieties (Russian), *Uspekhi Mat. Nauk* 53, 61–114, 1998.

[119] Murdoch, D.C., Structure of abelian quasigroups, *Trans. Amer. Math. Soc.*, 49, 392–409, 1941.

[120] Neumann, W.D., On the quasivariety of convex subsets of affine spaces, *Arch. Math.*, 21, 11–16, 1970.

[121] O'Nan, M.E., Sharply 2-transitive sets of permutations, in *Proceedings of the Rutgers Group Theory Year, 1983–1984*, Aschbacher, M. *et al.*, Eds., Cambridge University Press, Cambridge, 1984, 63–67.

[122] Osborn, J.M., New loops from old geometries, *Amer. Math. Monthly*, 68, 103–107, 1961.

[123] Paige, L.J., A class of simple Moufang loops, *Proc. Amer. Math. Soc.*, 7, 471–482, 1956.

[124] Penrose, R., A generalised inverse for matrices, *Proc. Camb. Phil. Soc.*, 51, 406–413, 1955.

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

[126] Phillips, J.D. and Smith, J.D.H., The endocenter and its applications to quasigroup representation theory, *Comm. Math. Univ. Carol.*, 32, 417–422, 1991.

[127] Phillips, J.D. and Smith, J.D.H., Quasiprimitivity and quasigroups, *Bull. Austral. Math. Soc.*, 59, 473–475, 1999.

[128] Pierce, R.S., *Associative Algebras*, Springer, New York, NY, 1982.

[129] Pigozzi, D. and Sichler, J., Homomorphisms of partial and of complete Steiner triple systems and quasigroups, in *Universal Algebra and Lattice Theory*, Comer, S.D., Ed., Springer, Berlin, 1985, 224–237.

[130] Pöschel, R. and Kalužnin, L.A., *Funktionen- und Relationenalgebren*, Deutscher Verlag der Wissenschaften, Berlin, 1979.

[131] Praeger, C., An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs, *J. London Math. Soc.*, 47, 227–239, 1993.

[132] Praeger, C., Quasiprimitivity: structure and combinatorial applications, *Discrete Math.*, 264, 211-224, 2003.

[133] Przytycki, J.H. and Traczyk, P., Conway algebras and skein equivalences of links, *Proc. Amer. Math. Soc.*, 100, 744–748, 1987.

[134] Romanowska, A.B. and Smith, J.D.H., *Modal Theory*, Heldermann, Berlin, 1985.

[135] Romanowska, A.B. and Smith, J.D.H., *Modes*, World Scientific, Singapore, 2002.

[136] Rutten, J.J.M.M., Universal coalgebra: a theory of systems, *Theoret. Comput. Sci.*, 249, 3–80, 2000.

[137] Sade, A., Quasigroupes obéissant à certaines lois, *Rev. Fac. Sci. Univ. Istanbul, Ser. A*, 22, 151–184, 1957.

[138] Sade, A., Quasigroupes demi-symétriques, *Ann. Soc. Sci. Bruxelles Ser. I*, 79, 133–143, 1965.

[139] Sade, A., Quasigroupes demi-symétriques II. Autotopies gauches, *Ann. Soc. Sci. Bruxelles Ser. I*, 79, 223–232, 1965.

[140] Sade, A., Quasigroupes demi-symétriques III. Constructions linéaires, *A*-maps, *Ann. Soc. Sci. Bruxelles Ser. I*, 81, 5–17, 1967.

[141] Sade, A., Quasigroupes demi-symétriques. Isotopies préservant la demi-symétrie, *Math. Nach.*, 33, 177–188, 1967.

[142] Serre, J.-P., *Représentations Linéaires des Groupes Finies*, Hermann, Paris, 1978.

[143] Serre, J.-P., *Trees*, Springer, Berlin, 1980.

[144] Sherman, G., A lower bound for the number of conjugacy classes in a finite nilpotent group, *Pacific J. Math.*, 80, 253–254, 1979.

[145] Shrikande, S.S., On a characterization of the triangular association scheme, *Ann. Math. Statist.*, 30, 39–47, 1959.

[146] Smith, J.D.H., Centraliser rings of multiplication groups on quasigroups, *Math. Proc. Camb. Phil. Soc.*, 79, 427–431, 1976.

[147] Smith, J.D.H., *Mal'cev Varieties*, Springer, Berlin, 1976.

[148] Smith, J.D.H., *Representation Theory of Infinite Groups and Finite Quasigroups*, Université de Montréal, Montreal, 1986.

[149] Smith, J.D.H., Quasigroups, association schemes, and Laplace operators on almost periodic functions, in *Algebraic, Extremal and Metric Combinatorics 1986*, Deza, M.-M., Frankl, P., and Rosenberg, I.G., Eds., Cambridge University Press, Cambridge, 1988, 205–218.

[150] Smith, J.D.H., Induced class functions are conditional expectations, *Eur. J. Combinatorics*, 10, 293–296, 1989.

[151] Smith, J.D.H., Entropy, character theory and centrality of finite quasigroups, *Math. Proc. Camb. Phil. Soc.*, 108, 435–443, 1990.

[152] Smith, J.D.H., Combinatorial characters of quasigroups, in *Coding Theory and Design Theory, Part I: Coding Theory*, Ray-Chaudhuri, D., Ed., Springer, New York, NY, 1990, 163–187.

[153] Smith, J.D.H., Skein polynomials and entropic right quasigroups, *Demonstr. Math.* 24, 241–246, 1991.

[154] Smith, J.D.H., Loop transversals to linear codes, *J. Comb., Info. and System Sciences*, 17, 1–8, 1992.

[155] Smith, J.D.H., Association schemes, superschemes, and relations invariant under permutation groups, *Eur. J. Combinatorics*, 15, 285–291, 1994.

[156] Smith, J.D.H., Homotopy and semisymmetry of quasigroups, *Alg. Univ.*, 38, 175–184, 1997.

[157] Smith, J.D.H., Quasigroup actions: Markov chains, pseudoinverses, and linear representations, *Southeast Asia Bull. of Math.*, 23, 719–729, 1999.

[158] Smith, J.D.H., Classical and quantum statistical mechanics of permutation representations, in *Groups Korea '98, Proceedings of the International Conference, Pusan National University, Pusan, Korea, August 10–16, 1998*, Baik, Y.G., Johnson, D.L., and Kim, A.C., Eds., de Gruyter, Berlin, 2000, 337–348.

[159] Smith, J.D.H., Some observations on the concepts of information-theoretic entropy and randomness, *Entropy*, 3, 1–11 (electronic journal), 2001.

[160] Smith, J.D.H., Quasigroup homogeneous spaces and linear representations, *J. Alg.*, 241, 193–203, 2001.

[161] Smith, J.D.H., A coalgebraic approach to quasigroup permutation representations, *Alg. Univ.*, 48, 427–438, 2002.

[162] Smith, J.D.H., Permutation representations of loops, *J. Alg.*, 264, 342–357, 2003.

[163] Smith, J.D.H., Characters of central piques, *J. Alg.*, 279, 437–450, 2004.

[164] Smith, J.D.H., Symmetry and entropy: a hierarchical perspective, *Symmetry*, 16, 37–45, 2005.

[165] Smith, J.D.H. and Romanowska, A. B., *Post-Modern Algebra*, Wiley, New York, NY, 1999.

[166] Soublin, J.-P., Etude algébrique de la notion de moyenne. *J. Math. Pures et Appl.*, 50, 53–264, 1971.

[167] Spencer, J., *Ten Lectures on the Probabilistc Method*, SIAM, Philadelphia, PA, 1987.

[168] Stein, S.K., On the foundations of quasigroups, *Trans. Amer. Math. Soc.*, 85, 228–256, 1957.

[169] Suschkewitsch, A., On a generalization of the associative law, *Trans. Amer. Math. Soc.* 31, 204–214, 1929.

[170] Tamaschke, O., S-Ringe und verallgemeinerte Charaktere auf endlichen Gruppen, *Math. Z.* (84), 101–119, 1964.

[171] Terwilliger, P., The Johnson graph $J(d, r)$ is unique if $(d, r) \neq (2, 8)$, *Discr. Math.*, 58, 175–189, 1986.

[172] Vesanen, A., The group $\mathrm{PSL}(2, q)$ is not the multiplication group of a loop, *Comm. Alg.*, 22, 1177–1195, 1994.

[173] Vink, E.P. de, and Rutten, J.J.M.M., Bisimulation for probabilistic transition systems: a coalgebraic approach, *Theoret. Comput. Sci.*, 221, 271–293, 1999.

[174] Weisfeiler, B., *On Construction and Identification of Graphs*, Springer, Berlin, 1976.

[175] Wielandt, H., *Finite Permutation Groups*, Academic Press, New York, NY, 1964.

[176] Witherspoon, S.J,, The representation ring of the quantum double of a finite group, *J. Alg.*, 179, 305–329, 1996.

[177] Wojdyło, J., Relation algebras and t-vertex condition graphs, *Eur. J. Combinatorics*, 19, 981–986, 1998.

[178] Yoshida, T., Idempotents of Burnside rings and Dress induction theorem, *J. Alg.*, 80, 90–105, 1983.

[179] Zorn, M., Alternativkörper und quadratische Systeme, *Abh. Math. Sem. Hamburg*, 9, 395–402, 1933.