Quasigroups and Related Systems **15** (2007), 109 – 140

Four lectures on quasigroup representations

Jonathan D. H. Smith

Abstract

These are notes for lectures in the Workshops Loops '07 series, held at the Czech Agricultural University, Prague, 13 August – 17 August, 2007. The initial lecture covers elementary topics and examples of quasigroups. The following lectures then introduce the three main branches of quasigroup representation theory: characters, permutation representations, and modules.

1. Quasigroups

1.1. Basic definitions.

1.1.1. *Combinatorial quasigroups.* A (*combinatorial*) *quasigroup* Q or $(Q,\cdot)$ is a set Q equipped with a binary operation of *multiplication*

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

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.

1.1.2. *Equational quasigroups.* An (*equational*) *quasigroup*, written as Q or $(Q,\cdot,/,\backslash)$, is a set Q equipped with three binary operations of multiplication, *right division* $/$ and *left division* $\backslash$, satisfying the identities:

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

Note the left-right symmetry of these identities.

2000 Mathematics Subject Classification: 20N05
Keywords: quasigroup, loop, multiplication group, centrality, character, association scheme, permutation representation, permutation group, transfomation group, split extension, module, group in category, combinatorial differentiation

1.1.3. *Quasigroups.* Suppressing the divisions, each equational quasigroup is a combinatorial quasigroup. For example, the unique solution y to $x \cdot y = z$ is $x\backslash z$. Conversely, each combinatorial quasigroup is equational: define $x\backslash z$ as the unique solution y to $x \cdot y = z$, and so on. We speak simply of *quasigroups.*

A subset P of a quasigroup $(Q, \cdot)$ is a *subquasigroup* of Q if P is closed under the multiplication and the divisions. If Q_1 and Q_2 are quasigroups, then their (*direct*) *product* is the product set $Q_1 \times Q_2$ equipped with componentwise multiplication and divisions.

1.1.4. *Homomorphisms and homotopies.* A map

$$f : (Q_1, \cdot, /, \backslash) \to (Q_2, \cdot, /, \backslash)$$

between quasigroups is a *homomorphism* if

$$xf \cdot yf = (x \cdot y)f$$

for all x, y in Q_1. It is an *isomorphism* if it is bijective. We then say that Q_1 and Q_2 are *isomorphic*, notation $Q_1 \cong Q_2$.

In quasigroup theory, the usual algebraic notion of homomorphism is often too strong. A triple of maps

$$(f, g, h) : (Q_1, \cdot, /, \backslash) \to (Q_2, \cdot, /, \backslash)$$

between quasigroups is a *homotopy* if

$$xf \cdot yg = (x \cdot y)h \tag{1.2}$$

for all x, y in Q_1. The triple is an *isotopy* if the maps f, g, h are bijective. We then say that Q_1 and Q_2 are *isotopic*, notation $Q_1 \sim Q_2$. (The concept of isotopy is often too weak. The right concept seems to be "central isotopy," as described in §1.5.5. Compare [5, §§4.2–3].)

1.1.5. *Exercises.*

1. If $f : Q_1 \to Q_2$ is a homomorphism between quasigroups, show $xf/yf = (x/y)f$ and $xf\backslash yf = (x\backslash y)f$ for all x, y in Q_1.

2. Show that a function $f : Q_1 \to Q_2$ between quasigroups is a homomorphism if and only if its *graph*

$$\{(x_1, x_2) \in Q_1 \times Q_2 \mid x_1 f = x_2\}$$

is a subquasigroup of the product $Q_1 \times Q_2$.

3. Show that isotopy is an equivalence relation.

4. Show that, if one of the three components f, g, h of a homotopy is bijective, then (f, g, h) is an isotopy.

5. Show that isotopic groups are isomorphic.

1.2. Basic examples.

1.2.1. *Groups.* Each group is a quasigroup, with $x/y = xy^{-1}$ and $x\backslash y = x^{-1}y$. The multiplication satisfies the associative law (although the divisions do not). Conversely, with the exception of the empty quasigroup, each associative quasigroup is a group. A quasigroup is *abelian* if it is commutative and associative, so is either empty or an abelian group.

1.2.2. *Subtraction.* If $(A, +)$ is an additive (abelian) group, then the set A forms a quasigroup $(A, -)$ under the nonassociative operation of subtraction. This operation is more fundamental than the associative operation of addition. For example, the integer 1 generates all integers using subtraction, since $0 = 1 - 1$, $-n = 0 - n$, $m + n = m - (-n)$. But 1 only generates the positive integers using addition.

1.2.3. *Isotopes.* If Q_2 is a quasigroup, and the maps $f, g, h : Q_1 \to Q_2$ are bijections, then there is a unique quasigroup structure on Q_1 so that (f, g, h) forms an isotopy. Using (1.2), we have $x \cdot y = (xf \cdot yg)h^{-1}$ for elements x, y in Q_1. For example, if $Q_1 = Q_2 = \mathbb{R}$, with Q_2 as the additive group $(\mathbb{R}, +, 0)$ of the real numbers, and the bijective maps $f, g, h : \mathbb{R} \to \mathbb{R}$ are the respective scalar multiplications by the invertible elements 1/2, 1/2, and 1, then the multiplication

$$x \cdot y = \frac{x + y}{2}$$

is the operation of taking arithmetic means.

1.2.4. *Latin squares.* A *Latin square*, such as that displayed on the left side of Figure 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. The body of the multiplication table of a (finite) quasigroup is a Latin square, while each Latin square may be bordered to yield the multiplication table of a quasigroup. For example, labelling the rows and columns of the Latin square on the left side of Figure 1 by $1, \dots, 6$ in order yields the multiplication table of a quasigroup Q with $3 \cdot 2 = 1$, etc., as displayed on the right side of Figure 1.

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

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: A Latin square yields a multiplication table.

1.2.5. *Exercises.*

1. Define a multiplication operation $\circ$ on the additive group $\mathbb{Z}/3\mathbb{Z}$ of integers modulo 3 by $x \circ y = -x - y$. Set up the body of the multiplication table of $(\mathbb{Z}/3\mathbb{Z}, \circ)$ as a Latin square.

2. Show that the quasigroups $(\mathbb{Z}/3\mathbb{Z}, -)$, $(\mathbb{Z}/3\mathbb{Z}, +)$, and the quasigroup $(\mathbb{Z}/3\mathbb{Z}, \circ)$ of Exercise (1) are all isotopic.

3. Verify the nonassociativity of the quasigroup Q whose multiplication table appears in Figure 1.

1.3. Steiner systems.

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

1.3.2. *Projective spaces over* $\mathsf{GF}(2)$. Suppose that S is the projective space $\mathsf{PG}(d, 2)$ of dimension d over the 2-element field $\mathsf{GF}(2)$. As a set, S consists of the nonzero elements of the $(d+1)$-dimensional vector space $\mathsf{GF}(2)^{d+1}$. The lines in the projective space are the intersection with S of 2-dimensional linear subspaces of $\mathsf{GF}(2)^{d+1}$. Taking $\mathcal{B}$ to be the set of lines yields a Steiner triple system $(S, \mathcal{B})$ which is also described as $\mathsf{PG}(d, 2)$. The points of S are specified by their coordinate vectors in $\mathsf{GF}(2)^{d+1}$, 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, illustrated in Figure 2, 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. Note the curved "line" 356 in the figure.

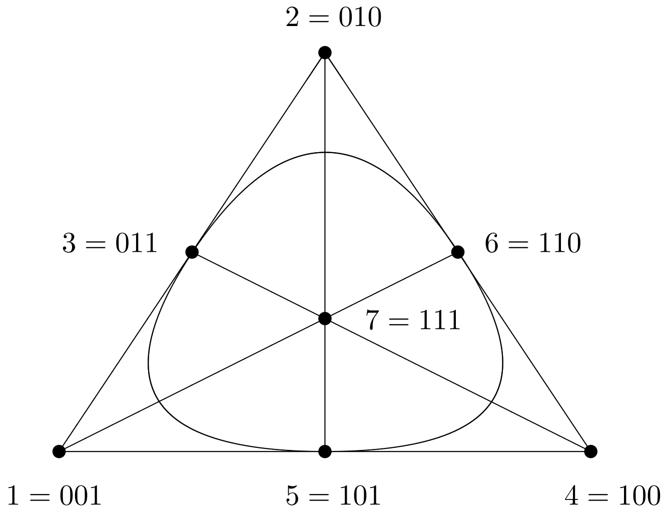

Figure 2: The projective space $\mathsf{PG}(2, 2)$.

Suppose that S is the projective space $\mathsf{PG}(d, 2)$ of dimension d over the 2-element field $\mathsf{GF}(2)$. As a set, S consists of the nonzero elements of the $(d+1)$-dimensional vector space $\mathsf{GF}(2)^{d+1}$. The lines in the projective space are the intersection with S of 2-dimensional linear subspaces of $\mathsf{GF}(2)^{d+1}$. Taking $\mathcal{B}$ to be the set of lines yields a Steiner triple system $(S, \mathcal{B})$ which is also described as $\mathsf{PG}(d, 2)$. The points of S are specified by their coordinate vectors in $\mathsf{GF}(2)^{d+1}$, 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, illustrated in Figure 2, 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. Note the curved "line" 356 in the figure.

1.3.2. *Affine spaces over* $\mathsf{GF}(3)$. Suppose that S is the affine space $\mathsf{AG}(d, 3)$ of dimension d over the 3-element field $\mathsf{GF}(3)$. As a set, S is the vector space $\mathsf{GF}(3)^d$. The lines in the affine geometry are the cosets $L + v$ of 1-dimensional linear subspaces L of $\mathsf{GF}(3)^d$, with v as a vector from $\mathsf{GF}(3)^d$. Taking $\mathcal{B}$ to be the set of lines again yields a Steiner triple system $(S, \mathcal{B})$, which is also 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.

1.3.4. *Totally symmetric quasigroups.* 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*, satisfying the identity

$$x\cdot x=x\,. \tag{1.3}$$

It also possesses the property of *total symmetry* expressed by the identities

$$x\cdot y=x/y=x\backslash y. \tag{1.4}$$

Conversely, 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 $(S,\cdot)$.

1.3.5. *Exercises.*

1. Construct the multiplication table for the idempotent, totally symmetric quasigroup $\mathsf{PG}(2,2)$.
2. Describe the quasigroup of Exercise 1.2.5 (1) as a Steiner triple system.
3. Show that for positive integers m and n, the totally symmetric quasigroups $\mathsf{AG}(m+n,3)$ and $\mathsf{AG}(m,3)\times\mathsf{AG}(n,3)$ are isomorphic.

1.4. Multiplication groups.

1.4.1. *Multiplications.* Let p be an element of a subquasigroup P of a quasigroup $(Q,\cdot)$. The (*relative*) *left multiplication* $L_Q(p)$ or $L(p)$ by p in Q is the map

$$L(p):Q\to Q;\quad x\mapsto p\cdot x\,.$$

Note that $L(p)$ is a permutation (bijective self-map) of Q. Indeed, the identity (IL) gives the injectivity of $L(p)$, while the identity (SL) gives the surjectivity. Similarly, the (*relative*) *right multiplication* $R_Q(p)$ or $R(p)$ by p in Q is the map

$$R(p) : Q \to Q; \quad x \mapsto x \cdot p\,.$$

1.4.2. *Multiplication groups.* Let P be a subquasigroup of a quasigroup Q. Let $Q!$ be the group of all permutations of the set Q. The (*relative*) *left multiplication group* of P in Q is the subgroup

$$\mathrm{LMlt}_Q P = \langle L_Q(p) \mid p \in P \rangle_{Q!}$$

of $Q!$ generated by all the relative left multiplications $L(p)$ by elements p of P. The (*relative*) *right multiplication group*

$$\mathrm{RMlt}_Q P = \langle R_Q(p) \mid p \in P \rangle_{Q!}$$

is defined similarly. The (*relative*) *multiplication group* of P in Q is the subgroup

$$\mathrm{Mlt}_Q P = \langle L_Q(p), R_Q(p) \mid p \in P \rangle_{Q!}$$

generated by both the left and right multiplications from P. Note that P is invariant under $\mathrm{Mlt}_Q P$. Finally, define the (*combinatorial*) *multiplication group* $\mathrm{Mlt}\, Q$ of Q as the relative multiplication group of Q in itself. (The adjective "combinatorial" distinguishes from the groups of §4.2.2.)

1.4.3. *Multiplication groups of groups.* Suppose that the quasigroup Q is a group (compare §1.2.1), with centre $Z(Q)$. The combinatorial multiplication group G of Q is given by the exact sequence

$$1 \to Z(Q) \xrightarrow{\Delta} Q \times Q \xrightarrow{T} G \to 1 \tag{1.5}$$

of groups with $\Delta : z \mapsto (z, z)$ and $T : (x, y) \mapsto L(x)^{-1}R(y)$. If the group Q is abelian, then the right multiplication map

$$R : Q \to G; \quad q \mapsto R(q)$$

is a group isomorphism.

1.4.4. *Multiplication groups as permutation groups.* Suppose that G is a relative multiplication group of a quasigroup Q. For elements x and y of Q, define

$$\rho(x, y) = R(x\backslash x)^{-1} R(x\backslash y) \tag{1.6}$$

in G. Note that $\rho(x,x)=1$ for x in Q. The action of G on Q is transitive: given elements x and y of Q, we have

$$x\rho(x,y)=xR(x\backslash x)^{-1}R(x\backslash y)=xR(x\backslash y)=x(x\backslash y)=y$$

since $xR(x\backslash x)=x(x\backslash x)=x$. Consider the stabiliser

$$G_x=\{g\in G\mid xg=x\}$$

of each element x in Q. The stabilisers are all conjugate in G, indeed

$$(G_x)^{\rho(x,y)}=G_{x\rho(x,y)}=G_y$$

for x and y in Q.

1.4.5. *Exercises.*

1. Verify that Δ and T in (1.5) are group homomorphisms.

2. Verify the exactness of the sequence (1.5) — at each of the three interior nodes, the image of the arrow coming in is the group kernel of the arrow going out.

3. Let G be the combinatorial multiplication group of a group Q with identity element e. Show that the stabiliser G_e is the inner automorphism group $\operatorname{Inn} Q$ of Q.

4. For an integer $n>1$, show that the dihedral group D_n of degree n is the multiplication group of the quasigroup $(\mathbb{Z}/n\mathbb{Z},-)$ of integers modulo n under subtraction.

5. Let e be an element of a subquasigroup P of a quasigroup Q. Let G be the relative multiplication group of P in Q, and let G_e be the stabiliser of e in G. Using the notation (1.6), show that G decomposes as the disjoint union

$$G=\bigcup_{x\in P}G_e\rho(e,x)\,.$$

6. Let e be an element of a quasigroup Q with combinatorial multiplication group G. Show that Q is an abelian group if and only if the stabiliser G_e is a normal subgroup of G [7, III Prop.2.5.3].

1.5. Centrality.

1.5.1. *Congruences.* If $f : Q_1 \to Q_2$ is a quasigroup homomorphism, consider the kernel relation $\ker f$ of f, defined by

$$(x, y) \in \ker f \Leftrightarrow xf = yf\,.$$

This is a *congruence* (*relation*) on Q_1, an equivalence relation which, as a subset of $Q_1 \times Q_1$, is a subquasigroup of $Q_1 \times Q_1$. Conversely, given a congruence relation V on a quasigroup Q, the natural projection

$$\operatorname{nat} V : Q \to Q^V; \quad x \mapsto x^V\,,$$

mapping x in Q to its equivalence class $x^V = \{y \in Q \mid (x, y) \in V\}$ in the set $Q^V = \{x^V \mid x \in Q\}$ of all equivalence classes, is a quasigroup homomorphism.

1.5.2. *Uniformity of congruences.* Let V be a congruence on a quasigroup Q. Then for elements x and y of Q, the map $\rho(x, y) : x^V \to y^V$ is a well-defined bijection. To see that it is well defined, consider an element x' of x^V. Then

$$(y, x'\rho(x, y)) = \big(x\rho(x, y), x'\rho(x, y)\big) = \big((x, x')/(x\backslash x, x\backslash x)\big) \cdot (x\backslash y, x\backslash y)$$

is an element of V, since V is both a reflexive relation and a subquasigroup of Q^2. Summarizing, a quasigroup congruence is determined by any one of its congruence classes.

1.5.3. *Normal subquasigroups.* A subquasigroup P of a quasigroup Q is said to be a *normal* subquasigroup of Q, written $P \triangleleft Q$, if there is a congruence V on Q having P as a single congruence class. By the uniformity (§1.5.2), the congruence V is uniquely determined by P. Write Q/P for the quotient Q^V. Note that a normal subgroup N of a group Q is a class of the kernel congruence of the natural projection $Q \to Q/N$; $x \mapsto Nx$.

1.5.4. *Central congruences.* For a quasigroup Q, the *diagonal*

$$\widehat{Q} = \{(x, x) \in Q^2 \mid x \in Q\}$$

is a subquasigroup of Q^2. The diagonal is a subquasigroup of each congruence V on Q, since V is reflexive. The congruence V is said to be *central* if $\widehat{Q} \triangleleft V$. Each central congruence on Q is a subcongruence of a maximal central congruence, the *centre congruence* $\zeta(Q)$ of Q. For a group Q, the centre $Z(Q)$ is the $\zeta(Q)$-class of the identity element. A quasigroup Q is said to be *central* if $\zeta(Q) = Q^2$. The class of central quasigroups is denoted by $\mathfrak{Z}$. Central groups are precisely the abelian groups.

1.5.5. *Central isotopy.* For a quasigroup Q, suppose that the diagonal $\widehat{Q}$ is a congruence class of a congruence W on $\zeta(Q)$. A quasigroup P is *centrally isotopic* to Q, written $P \simeq Q$, if there is a bijection $t : P \to Q$, a so-called *central shift*, and a pair (q, q') of elements of Q such that

$$(q, q')\ W\ \big((x \cdot y)t, xt \cdot yt\big) \tag{1.7}$$

for all x, y in P. In particular, it follows that the triple $\big(t, t, t\rho(q, q')\big)$ is an isotopy — Exercise 1.5.6 (4). Central isotopy is an equivalence relation, and centrally isotopic quasigroups have similar multiplication group actions (so in particular, their multiplication groups are isomorphic). A central quasigroup Q is centrally isotopic to the central quasigroup $Q^2/\widehat{Q}$. Note that the quotient $Q^2/\widehat{Q}$ has the class $\widehat{Q}$ as an idempotent element.

1.5.6. *Exercises.*

1. Show that a group Q is abelian if and only if $\widehat{Q} \triangleleft Q^2$.
2. Let $(A, +, 0)$ be an abelian group. For automorphisms R and L of $(A, +, 0)$, define $x \cdot y = xR + yL$. Show that $(A, \cdot)$ is a central quasigroup with 0 as an idempotent element. (In fact, each central quasigroup with an idempotent element is obtained in this way [1, Th. III.5.2], [6, §3.5].)
3. For the quasigroup $(A, \cdot)$ of Exercise (2), show that $\mathrm{Mlt}(A, \cdot)$ is the split extension of the abelian group $(A, +, 0)$ by the subgroup $\langle R, L\rangle$ of the automorphism group $\mathrm{Aut}(A, +, 0)$ generated by the automorphisms R and L.
4. Let a quasigroup P be centrally isotopic to a quasigroup Q. Use (1.7) to deduce that $\big(t, t, t\rho(q, q')\big) : P \to Q$ is an isotopy.
5. Amongst the quasigroups of Exercise 1.2.5 (2), determine which pairs are centrally isotopic.

2. Characters

2.1. The Bose-Mesner algebra.

2.1.1. *Conjugacy classes.* Let Q be a quasigroup, with multiplication group G. Recall that the action of G on Q is transitive, with a single orbit Q

(§1.4.4). The group G acts on $Q \times Q$ with the *diagonal action*

$$(q_1, q_2)g = (q_1 g, q_2 g)$$

for q_1, q_2 in Q and g in G. There are several orbits. In the general theory of transitive group actions, these orbits are described as *orbitals*. Here, they are defined as the (*quasigroup*) *conjugacy classes*. Since G acts transitively on Q, one orbital is the diagonal $\widehat{Q} = C_1$, the relation $\{(q_1, q_2) \mid q_1 = q_2\}$ of equality on Q. The complement of $\widehat{Q} = C_1$ in Q^2 is the *diversity relation* $\{(q_1, q_2) \mid q_1 \neq q_2\}$. If the diversity relation forms a single orbital, then Q is described as a *rank* 2 *quasigroup*. For a general finite quasigroup Q of order n, there is a finite set Γ or

$$\Gamma(Q) = \{\widehat{Q} = C_1, C_2, \ldots, C_s\} \tag{2.1}$$

of conjugacy classes, known as the *conjugacy class partition* of Q^2. The integer s is known as the *rank* of the quasigroup Q. For $1 \leqslant i \leqslant s$, the cardinality of the i-th conjugacy class is a multiple $|C_i| = nn_i$ of n. The factor n_i, known as the *valency* of C_i, is the cardinality of $C_i(x) := \{q \mid (x, q) \in C_i\}$ for each x in Q — Exercise 2.1.5 (1). Note that $n_1 = 1$ and $n_1 + \cdots + n_s = n$.

2.1.2. *Incidence matrices.* Suppose that Q is a finite quasigroup, with a positive order n. Then the elements of Q may be used to index the rows and columns of each $n \times n$ matrix (with entries from the field $\mathbb{C}$ of complex numbers). For a relation R on Q, the *incidence matrix* of R is the $n \times n$ matrix having an entry of 1 in the row labelled q_1 and column labelled q_2 whenever $(q_1, q_2) \in R$. The other entries of the incidence matrix of R are zero. Thus the incidence matrix of the universal relation $Q \times Q$ is the $n \times n$ matrix J or J_n, all of whose entries are 1. The incidence matrix of the equality relation $\widehat{Q} = C_1$ is the $n \times n$ identity matrix I or I_n. The incidence matrix of the diversity relation is $J_n - I_n$. If the incidence matrix of a relation R is A, then the incidence matrix of the converse relation

$$R^{-1} = \{(q_1, q_2) \mid (q_2, q_1) \in R\}$$

is the (conjugate) transpose A^* of A.

2.1.3. *The Bose-Mesner algebra.* Let Q be a quasigroup of positive finite order n, with conjugacy class partition (2.1). The converse of each conjugacy class C_i is a conjugacy class C_{i^*}. The respective incidence matrices

$$I_n = A_1, A_2, \ldots, A_s \tag{2.2}$$

of the quasigroup conjugacy classes are the *adjacency matrices.* Note that $A_i^* = A_{i^*}$ (for $1 \leqslant i \leqslant s$) and

$$\sum_{i=1}^{s} A_i = J_n \,.$$

The adjacency matrices (2.2) generate a subalgebra of the complex algebra $\mathbb{C}_n^n$ of all complex $n \times n$ matrices. This algebra is known as the *Bose-Mesner algebra.* If the multiplication group of Q is G, then the Bose-Mesner algebra is also known as the *centraliser ring* (or Vertauschungsring) $V(G,Q)$ of G on Q.

2.1.4. *Primitive idempotents.* The Bose-Mesner algebra $V(G,Q)$ of a finite quasigroup turns out to be just the s-dimensional $\mathbb{C}$-linear span of the set (2.2) of adjacency matrices, and moreover, $V(G,Q)$ is a commutative subalgebra of the complex matrix algebra [6, Th. 6.1]. Thus there are *structure constants* c_{ij}^k for $1 \leqslant i,j,k \leqslant s$ with

$$A_i A_j = \sum_{k=1}^{s} c_{ij}^k A_k$$

and $c_{ij}^k = c_{ji}^k$. Simultaneous diagonalisation of the set (2.2) of mutually commuting matrices shows that the vector space $V(G,Q)$ has a basis

$$\frac{1}{n} J_n = E_1, E_2, \ldots, E_s \tag{2.3}$$

of mutually orthogonal *primitive idempotent* matrices, satisfying

$$E_i E_j = \delta_{ij} E_i \qquad \text{and} \qquad \sum_{i=1}^{s} E_i = I_n \,.$$

Thus the Wedderburn decomposition of $V(G,Q)$ as a direct sum of matrix rings is

$$V(G,Q) \cong V(G,Q)E_1 \oplus \cdots \oplus V(C,Q)E_s \cong \mathbb{C} \oplus \cdots \oplus \mathbb{C} \,.$$

The matrices (2.3) are the projections onto the common eigenspaces of the adjacency matrices (2.2). They are also uniquely determined as the set of atoms of the finite Boolean algebra of idempotent elements of $V(G,Q)$. For $1 \leqslant i \leqslant s$, the traces f_i of the matrices E_i are the *multiplicities.* Note that $f_1 = 1$ and $f_1 + \cdots + f_s = n$.

2.1.5. *Exercises.*

1. Let C_i be a conjugacy class of a finite quasigroup of order n. For elements x, y of Q, show that $\rho(x,y) : C_i(x) \to C_i(y)$ is a bijection.
2. Let Q be a group with identity element e. Show that
$$\{e\} = C_1(e), C_2(e), \dots, C_s(e)$$
are the usual group conjugacy classes — see Exercise 1.4.5 (3).
3. If Q is a group with identity element e, show that
$$C_{i^*}(e) = \{x^{-1} \mid x \in C_i(e)\}\,.$$
4. Show that a finite, nonempty quasigroup is abelian if and only if all the valencies are 1.
5. Show that, up to isomorphism, the additive group $(\mathbb{Z}/2\mathbb{Z}, +, 0)$ is the only finite rank 2 group. (HNN-extensions of countable torsion-free groups yield infinite rank 2 groups [2].)
6. Let Q be the additive group $(\mathbb{Z}/3\mathbb{Z}, +, 0)$ of integers modulo 3. Show that the adjacency matrices are
$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$
and the primitive idempotents are
$$E_1 = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \; E_2 = \frac{1}{3}\begin{bmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \\ \omega & \omega^2 & 1 \end{bmatrix}, \; E_3 = \frac{1}{3}\begin{bmatrix} 1 & \omega^2 & \omega \\ \omega & 1 & \omega^2 \\ \omega^2 & \omega & 1 \end{bmatrix}$$
with $\omega = \exp(2\pi i/3)$ as a primitive cube root of unity.

2.2. The character table.

2.1.1. *Change of basis.* For a quasigroup Q of finite order n, with multiplication group G, the Bose-Mesner algebra $V(G,Q)$ has two bases: the adjacency matrices (2.2), and the primitive idempotents (2.3). Each matrix from one basis is expressed uniquely as a linear combination of the matrices from the other:

$$A_i = \sum_{j=1}^{s} \xi_{ij} E_j \,, \qquad E_i = \sum_{j=1}^{s} \eta_{ij} A_j \,.$$

The coefficients in these linear combinations form mutually inverse $s \times s$ matrices

$$\Xi = [\xi_{ij}] \quad \text{and} \quad H = [\eta_{ij}] \,. \tag{2.4}$$

2.2.2. *Character tables.* The *character table* of Q is the $s \times s$ matrix $\Psi(Q)$ or $\Psi = [\psi_{ij}]$ with entries given as the normalised versions

$$\psi_{ij} = \tfrac{\sqrt{f_i}}{n_j}\, \xi_{ji} = \tfrac{n}{\sqrt{f_i}}\, \overline{\eta}_{ij}$$

of the entries of the change-of-basis matrices (2.4). This normalisation is used in the theory of finite groups. With a different normalisation, the *unitary character table* of Q is the $s \times s$ matrix $\Upsilon(Q)$ or $\Upsilon = [\upsilon_{ij}]$ with entries given as

$$\upsilon_{ij} = \sqrt{\frac{f_i}{nn_j}} \xi_{ji} = \sqrt{\frac{nn_j}{f_i}} \overline{\eta}_{ij}$$

in terms of the entries of the change-of-basis matrices (2.4). The so-called *orthogonality relations* satisfied by the character tables Ψ and Υ are best summarised by saying that the unitary character table Υ is a unitary $s \times s$ matrix: $\Upsilon^* \Upsilon = I_s$ — Exercise 2.2.5 (1).

2.2.3. *Duality.* In order to keep track of all the notation, see Table 1,

adjacency matrix A_i	primitive idempotent E_i
valency n_i	multiplicity f_i
$n_1 = 1$	$f_1 = 1$
$n_1 + \cdots + n_s = n$	$f_1 + \cdots + f_s = n$
$A_1 = I_n$	$E_1 = \frac{1}{n} J_n$
$\sum_{i=1}^{s} A_i = J_n$	$\sum_{i=1}^{s} E_i = I_n$
$A_i \circ A_j = \delta_{ij} A_i$	$E_i \cdot E_j = \delta_{ij} E_i$
$A_i = \sum_{j=1}^{s} \xi_{ij} E_j$	$E_i = \sum_{j=1}^{s} \eta_{ij} A_j$

Table 1: Duality.

illustrating the duality present. For two matrices $B = [b_{ij}]$ and $C = [c_{ij}]$ of the same shape, recall the *Hadamard product* $B \circ C = [b_{ij}c_{ij}]$.

2.2.4. *Class functions.* For a quasigroup Q with multiplication group G, a complex-valued function $\theta : Q \times Q \to \mathbb{C}$ is a *class function* if $\theta(q_1 g, q_2 g) = \theta(q_1, q_2)$ for all q_i in Q and g in G. In other words, θ is constant on each conjugacy class. The class functions form a complex vector space $\mathbb{C}\mathrm{Cl}(Q)$ under componentwise addition and scalar multiplication. If Q has finite order n, then an inner product $\langle\ |\ \rangle$ is defined on $\mathbb{C}\mathrm{Cl}(Q)$ by

$$\langle\theta|\varphi\rangle = \frac{1}{n^2} \sum_{(x,y)\in Q^2} \theta(x,y)\varphi(y,x)\,.$$

For $1 \leqslant i \leqslant s$, the i-th row $\psi_i = [\psi_{i1}, \dots, \psi_{is}]$ of the character table $\Psi(Q)$ determines a class function ψ_i with $\psi_i(x,y) = \psi_{ij}$ for $(x,y) \in C_j$, known as a *basic character* of Q. As a result of the orthogonality relations, and the choice of the normalisation for Ψ, the basic characters $\psi_1, \dots, \psi_s$ form an orthonormal basis for the space $\mathbb{C}\mathrm{Cl}(Q)$ of class functions. In particular, the *principal character* ψ_1 is the *zeta function* $\zeta : Q^2 \to \mathbb{C}$ taking the constant value 1 — Exercise 2.2.5 (3).

2.2.5. *Exercises.*

1. For a finite nonempty quasigroup Q, use $\mathit{\Xi} H = I_s$ to prove that $\Upsilon(Q)$ is a unitary matrix.

2. For a quasigroup Q of positive order n, show that $f_i = n\eta_{i1}$ for $1 \leqslant i \leqslant s$. Conclude that $\psi_{i1} = \sqrt{f_i}$ for $1 \leqslant i \leqslant s$.

3. For a quasigroup Q of positive order n, show that $\xi_{1j} = 1$ for $1 \leqslant j \leqslant s$. Conclude that $\psi_{1j} = 1$ for $1 \leqslant j \leqslant s$.

4. Compute the character table and the unitary character table for the additive group $(\mathbb{Z}/3\mathbb{Z}, +, 0)$ of integers modulo 3 — compare Exercise 2.1.5 (6).

5. Show that a finite nonempty quasigroup is abelian if and only if all the multiplicities are 1.

2.3. Examples and computations.

2.3.1. *Rank* 2 *quasigroups.* Let Q be a rank 2 quasigroup of finite order n. Now $f_2 = n_2 = n - 1$, so $\Psi(Q)$ has the form

$$\begin{bmatrix} 1 & 1 \\ (n-1)^{1/2} & ? \end{bmatrix} .$$

Using the orthogonality relations, this is completed to

$$\Psi(Q) = \begin{bmatrix} 1 & 1 \\ (n-1)^{1/2} & -(n-1)^{-1/2} \end{bmatrix} .$$

In particular — compare Exercise 2.1.5 (5),

$$\Psi(\mathbb{Z}/2\mathbb{Z}, +) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} . \qquad (2.5)$$

Almost all finite quasigroups are rank 2 quasigroups [7, Cor.6.5].

2.3.2. *Groups.* Suppose that Q is a finite group of order n, with identity element e. By Exercise 2.1.5 (2), the valencies n_i are the orders of the group conjugacy classes $C_i(e)$ for $1 \leqslant i \leqslant s$. Consider the complex vector space $\mathbb{C}Q$ spanned by Q. Extending the multiplication of Q by linearity (including the distributive law) yields $\mathbb{C}Q$ as the (*complex*) *group algebra* of Q. The right and left multiplications of Q act as endomorphisms of the vector space $\mathbb{C}Q$, making $\mathbb{C}Q$ a faithful module over $\mathbb{C}G$. The centraliser ring $V(G,Q)$, as the ring $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q$ of endomorphisms of the vector space $\mathbb{C}Q$ that commute with the action of G, is the centre $Z(\mathbb{C}Q)$ of the group algebra. Choose a set $\{V_1, V_2, \dots V_s\}$ of mutually nonisomorphic representatives for the ordinary irreducible Q-modules, with V_1 trivial. Suppose $\dim V_i = d_i$ for $1 \leqslant i \leqslant s$. The group algebra $\mathbb{C}Q$ decomposes as

$$\begin{aligned} \mathbb{C}Q &\cong \mathrm{End}_{\,\mathbb{C}Q}\mathbb{C}Q \\ &\cong \mathrm{End}_{\,\mathbb{C}Q}V_1 \oplus \mathrm{End}_{\mathbb{C}Q}(d_2V_2) \oplus \cdots \oplus \mathrm{End}_{\mathbb{C}Q}(d_sV_s) \\ &\cong \mathbb{C} \oplus \mathrm{Mat}_{d_2}(\mathbb{C}) \oplus \mathrm{Mat}_{d_s}(\mathbb{C}) \,, \end{aligned}$$

a direct sum of matrix rings. (The latter isomorphism holds by Schur's Lemma). The centre decomposes as

$$V(G,Q) = Z(\mathbb{C}Q) \cong \mathbb{C}\pi_1 \oplus \mathbb{C}\pi_2 \oplus \cdots \oplus \mathbb{C}\pi_s$$

with the primitive idempotent π_i or E_i as the idempotent projection from $\mathbb{C}Q$ onto the d_i^2-dimensional subspace $\mathrm{Mat}_{d_i}(\mathbb{C})$. Thus the multiplicities are $f_i = d_i^2$ for $1 \leqslant i \leqslant s$. It turns out that for $1 \leqslant i, j \leqslant s$, the basic character value ψ_{ij} is the value of the irreducible group character χ_i (the character of the irreducible module V_i) at elements of the group conjugacy class $C_j(e)$. The character table of the symmetric group S_3 of degree 3 is

$$\Psi = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -1 & 0 \end{bmatrix} . \tag{2.6}$$

As usual for groups, the entries $\sqrt{f_i}$ in the first column, namely the dimensions d_i of the irreducible modules, are integral.

2.3.3. *Subtraction modulo* 4. By Exercise 1.4.5 (4), the multiplication group G of the quasigroup $Q = (\mathbb{Z}/4\mathbb{Z}, -)$ of the integers modulo 4 under subtraction is the 8-element dihedral group D_4 of degree 4. The adjacency matrices are

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} , \quad A_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} , \quad A_3 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} ,$$

corresponding to the three respective relations of equality, diametric opposition, and adjacency in the square graph of Figure 3.

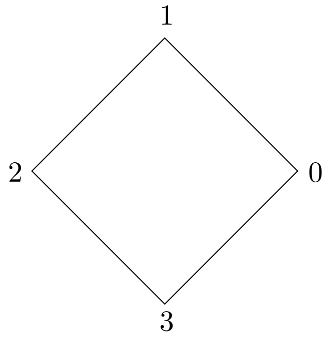

Figure 3: The square.

The centraliser ring $V(G,Q)$ is generated as a commutative complex algebra by the element $X = A_3$, since $A_3^2 = 2A_1 + 2A_2$, so $A_2 = \frac{1}{2}X^2 - 1$ (and, of course, $A_1 = 1$). Now $A_3^3 = 4A_3$, so

$$\begin{aligned} V(G,Q) &\cong \mathbb{C}[X]/\langle X^3 - 4X\rangle \\ &\cong \mathbb{C}[X]/\langle X-2\rangle \oplus \mathbb{C}[X]/\langle X+2\rangle \oplus \mathbb{C}[X]/\langle X\rangle \,. \end{aligned}$$

The isomorphism is obtained by the First Isomorphism Theorem for $\mathbb{C}$-algebras from the homomorphism

$$\mathbb{C}[X] \to \mathbb{C}^3;\quad f(X) \mapsto \big(f(2), f(-2), f(0)\big)\,.$$

Thus in the isomorphism $V(G,Q) \cong \mathbb{C}^3$,

$$\begin{aligned} A_1 = 1 &\mapsto (1,1,1)\,; \\ A_2 = \frac{X^2}{2} - 1 &\mapsto (1,1,-1)\,; \\ A_3 = X &\mapsto (2,-2,0)\,. \end{aligned}$$

The idempotent $E_1 = J/4 = (A_1 + A_2 + A_3)/4$, mapping to $(1,0,0)$, is projection onto the first component corresponding to $f(2)$. Let E_2 project to the second component $f(-2)$, and E_3 to the third $f(0)$. Then

$$\varXi = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{bmatrix} \quad \text{and} \quad H = \begin{bmatrix} 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & -1/4 \\ 1/2 & -1/2 & 0 \end{bmatrix}\,,$$

so $f_1 = f_2 = 1$ and $f_3 = 2$ — Exercise 2.2.5 (2). Finally

$$\Psi = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ \sqrt{2} & -\sqrt{2} & 0 \end{bmatrix} \tag{2.7}$$

— compare with the character table (2.6) of the symmetric group S_3.

2.3.4. *Exercises.*

1. Compute the character table of the Klein 4-group.

2. Compute the character table of the quasigroup $Q = (\mathbb{Z}/5\mathbb{Z}, -)$ of integers modulo 5 under subtraction. In your answer, use trigonometric functions rather than radicals as much as you can.

3. The character table (2.7) has the irrational entry $\sqrt{2}$ in the first column. Does the character table of a finite, nonassociative quasigroup always have at least one irrational entry somewhere in the first column?

4. (a) Using Exercise 1.5.6 (2) or otherwise, construct a central rank 2 quasigroup of order 5.

   (b) From the existence of non-central rank 2 quasigroups of order 5, conclude that the character table of a finite quasigroup Q cannot determine whether Q is central or not.

   (c) Since $\Psi(Q^2)$ does determine the centrality of Q [7, Cor. 7.2], conclude that $\Psi(Q)$ does not determine $\Psi(Q^2)$.

5. (a) Give an example of two isotopic quasigroups with distinct character tables.

   (b) Show that centrally isotopic quasigroups have the same character table.

3. Permutation representations

3.1. Cosets.

3.1.1. *Symmetry.* Consider a group Q, for example the group D_4 of symmetries of the square as illustrated in Figure 3. Let P be a *point stabiliser*, a subgroup of Q. In the square example, take the subgroup P to be the stabiliser $\{(0), (1\ 3)\}$ of the vertex 0. The subgroup P determines a (*group*) *homogeneous space*, the set

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

of cosets. The cosets (including P itself) are considered as *points* of the homogeneous space. The group Q acts on the homogeneous space $P\backslash Q$ by

$$R_{P\backslash Q}(q) : P\backslash Q \to P\backslash Q; \quad Px \mapsto Pxq \tag{3.1}$$

for q in Q. Now in Figure 3, for a vertex v of the square, choose an element x of Q taking 0 to v. Each vertex v of the square corresponds to the coset Px, the set of permutations taking 0 to $0x = v$. The action of Q on the square is then similar (in the technical sense!) to the action of Q on the homogeneous space $P\backslash Q$.

3.1.2 *Cosets.* As described in §3.1.1., symmetry reduces to the action of a group on a homogeneous space, the set of cosets of a subgroup. Our goal is to examine symmetry within the theory of quasigroups. Let P be a subquasigroup of a quasigroup Q. The (*right*) *cosets* of P in Q are defined as the orbits of the relative left multiplication group $\mathrm{LMlt}_Q P$ (compare §1.4.2) in its action on Q. The (*quasigroup*) *homogeneous space* $P\backslash Q$ is defined as the set of cosets of P in Q. For a finite quasigroup Q, the *type* of a 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. 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.

If P is a subgroup of a group Q, then the right cosets

$$Px = \{px \mid p \in P\}$$

in the group sense are exactly the right cosets $x\mathrm{LMlt}_Q P$ in the quasigroup sense. Now in the group case, the maps (3.1) are bijections between the various right cosets. Thus for a finite group Q, every homogeneous space $P\backslash Q$ is uniform.

3.1.3. *The quasigroup case.* To see what can happen in the quasigroup case, it is helpful to consider an example: the quasigroup Q whose multiplication table is displayed in Figure 1. Let P be the singleton subquasigroup $\{1\}$. Note that $\mathrm{LMlt}_Q P$ is the cyclic subgroup of $Q!$ generated by $(23)(456)$. Thus

$$P\backslash Q = \big\{\{1\}, \{2,3\}, \{4,5,6\}\big\} . \tag{3.2}$$

The space (3.2) is certainly not uniform, its type being the partition $3 + 2 + 1$ of 6. On the other hand, the homogeneous space determined by the subquasigroup $N = \{1, 2, 3\}$ is

$$N\backslash Q = \big\{\{1,2,3\}, \{4,5,6\}\big\} .$$

This space is uniform, of type $3 + 3$.

In a general quasigroup Q, the *regular* homogeneous space is defined as $\varnothing\backslash Q$. The relative left multiplication group of the empty subquasigroup just consists of the identity permutation, so the regular space is the set $\big\{\{x\} \bigm| x \in Q\big\}$ of singletons, isomorphic to (and often identified with) the set Q itself. If Q is a group or a *loop* (a quasigroup with identity element 1 satisfying $1 \cdot x = x = x \cdot 1$), the regular space may also be realised as the homogeneous space $\{1\}\backslash Q$.

3.1.4. *Exercises.*

1. Let Q be the quasigroup of integers modulo 4 under subtraction. For each subquasigroup P of Q, determine the homogeneous space $P\backslash Q$ and its type.
2. Let P be a subgroup of a group Q. Show that the orbits of the relative right multiplication group $\mathrm{RMlt}_Q P$ of P in Q are the left cosets of P.
3. Let P be a subgroup of a group Q. Show that the orbits of the relative multiplication group $\mathrm{Mlt}_Q P$ of P in Q are the double cosets PxP of P.
4. Let e be an element of a quasigroup Q with multiplication group G, and let G_e be the stabiliser of e in G. Show that the double cosets $G_e x G_e$ of G_e in G are in 1–1 correspondence with the quasigroup conjugacy classes of Q.

3.2. Action on homogeneous spaces.

3.2.1. *Markov matrices.* If q is an element of a group Q with subgroup P, the action of q on the homogeneous space $P\backslash Q$ is given by the map $R_{P\backslash Q}(q)$ of (3.1). Under right multiplication by q in Q, each element of a given coset Px is taken to the same coset Pxq.

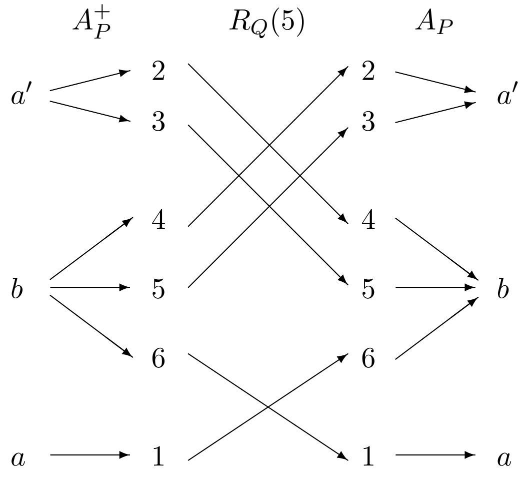

Figure 4: The action $R_{P\backslash Q}(5)$.

Now consider the quasigroup Q whose multiplication table is given in Figure 1, with the subquasigroup $P = \{1\}$. The homogeneous space $P\backslash Q$ is displayed in (3.2), and again on each side of Figure 4. Here the respective cosets are labelled as $a = \{1\}$, $a' = \{2, 3\}$, and $b = \{4, 5, 6\}$. Under the action of right multiplication by the element 5 of Q, the elements of the coset b are not all sent to the same coset. The elements 4 and 5 go to a', while 6 goes to a. The action is described by the Markov matrix

$$\begin{array}{c} \\ a \\ a' \\ b \end{array} \begin{array}{c} \begin{array}{ccc} a & a' & b \end{array} \\ \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix} \end{array} = R_{P\backslash Q}(5) \tag{3.3}$$

indexed by the points of the homogeneous space. Under the uniform probability distribution on Q, and hence on each coset, an element of the coset b is sent to a with probability $\frac{1}{3}$, and to a' with probability $\frac{2}{3}$. The Markov chain specified by the Markov matrix $R_{P\backslash Q}(5)$ has the homogeneous space $P\backslash Q = \{a, a', b\}$ as its state space. Each element of the state space on the left of Figure 4 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.

3.2.2. *Moore-Penrose inverses.* The analytical specification of Markov matrices such as (3.3) relies on the concept of the *(Moore-)Penrose inverse* or *pseudoinverse* A^+ of a (not necessarily square) complex matrix A. This is the unique matrix A^+ satisfying the equations

$$\begin{aligned} AA^+A &= A\ , \\ A^+AA^+ &= A^+, \\ (A^+A)^* &= A^+A\,, \\ (AA^+)^* &= AA^+ \end{aligned}$$

in which * denotes the conjugate transpose [4].

For a subquasigroup P of a finite, nonempty quasigroup Q, let A or A_P denote the incidence matrix for the homogeneous space $P\backslash Q$ of Q. This is a rectangular matrix, with rows indexed by Q and columns indexed by $P\backslash Q$. An entry indexed by an element q of Q and a coset X in $P\backslash Q$ is 1 if q lies in X, and 0 otherwise. The pseudoinverse A^+ or A_P^+ has its rows indexed by $P\backslash Q$ and columns indexed by Q. An entry indexed by a coset X in $P\backslash Q$ and an element q of Q is $|X|^{-1}$ if q lies in X, and 0 otherwise. For the singleton subquasigroup $P = \{1\}$ of the quasigroup Q from Figure 1, these matrices become

$$A_P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } A_P^+ = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix} . \qquad (3.4)$$

— compare the right and left sides of Figure 4.

3.2.3. *Action matrices.* If q is an element of a finite quasigroup Q with subquasigroup P, the action of q on the homogeneous space $P\backslash Q$ is given by the Markov matrix

$$R_{P\backslash Q}(q) = A_P^+ R_Q(q) A_P \qquad (3.5)$$

obtained using the incidence matrix A_P described in §3.2.2. The matrix (3.5) is called the *action matrix* of the element q on the homogeneous space $P\backslash Q$. Note how Figure 4 illustrates the composition of the action matrix $R_{P\backslash Q}(5)$ in the example under consideration. If Q is a finite group, then (3.5) recovers the permutation matrix describing the action (3.1) of q on $P\backslash Q$ — Exercise 3.2.4 (4).

3.2.4. *Exercises.*

1. Confirm that the matrices in (3.4) are mutual pseudoinverses.
2. 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,

$$R_{P\backslash Q}(q) = \begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \text{if } q \in P\,; \\ \\ \begin{bmatrix} 0 & 1 \\ \frac{m}{n-m} & \frac{n-2m}{n-m} \end{bmatrix} & \text{otherwise.} \end{cases}$$

3. (a) If $(Q, \cdot)$ is a quasigroup, show that $(Q, \backslash)$ is a quasigroup.

   (b) Show that the multiplication table of a finite quasigroup $(Q, \cdot)$ is the formal sum $\sum_{q \in Q} qR_S(q)$ of action matrices of the regular homogeneous space S of the quasigroup $(Q, \backslash)$.

4. If q is an element of a finite group Q with subgroup P, show that (3.5) recovers the permutation matrix describing the action (3.1) of q on $P\backslash Q$.

4. Modules

4.1. Groups in categories.

4.1.1. *Split extensions.* If Q is a group, a *Q-module* M is an abelian group $(M, +, 0)$ with a group homomorphism

$$Q \to \mathrm{Aut}(M, +, 0); \quad q \mapsto (m \mapsto mq)$$

from Q to the automorphism group of the abelian group $(M, +, 0)$. Since the composition of automorphisms is associative, this definition gives no possibility of extension to general quasigroups. Instead, it will be recast in more suitable form. Given a Q-module M, the *split extension* $E = Q \ltimes M$ is the set $Q \times M$ equipped with the product

$$(q_1, m_1)(q_2, m_2) = (q_1 q_2, m_1 q_2 + m_2)\,. \tag{4.1}$$

The split extension comes equipped with the projection

$$p : E \to Q; \quad (q, m) \mapsto q \tag{4.2}$$

and the insertion η_Q or

$$\eta : Q \to E; \quad q \mapsto (q, 0), \tag{4.3}$$

both of which are group homomorphisms.

4.1.1. *Slice categories.* If Q is an object of a category $\mathbf{C}$, an object in the *slice category* (or "comma category") $\mathbf{C}/Q$ is a $\mathbf{C}$-morphism $p : E \to Q$. For example, the projection (4.2) from the split extension is an object in the slice category $\mathbf{Gp}/Q$ of groups over Q, with $\mathbf{Gp}$ as the category of groups. A morphism in a slice category $\mathbf{C}/Q$ between two objects $p_1 : E_1 \to Q$ and $p_2 : E_2 \to Q$ is a $\mathbf{C}$-morphism $f : E_1 \to E_2$ for which the diagram

$$\begin{tikzcd}
E_1 \arrow[r, "f"] \arrow[d, "p_1"'] & E_2 \arrow[d, "p_2"] \\
Q \arrow[r, "1_Q"'] & Q
\end{tikzcd}$$

commutes. Such $\mathbf{C}/Q$-morphisms are often just denoted simply by the $\mathbf{C}$-morphism $f : E_1 \to E_2$. The identity morphism $1_Q : Q \to Q$ is the terminal object of $\mathbf{C}/Q$. If the category $\mathbf{C}$ has pullbacks, then the slice category $\mathbf{C}/Q$ has finite products. The product of two objects $p_1 : E_1 \to Q$ and $p_2 : E_2 \to Q$ is the pullback

$$\begin{tikzcd}
E_1 \times_Q E_2 \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & E_2 \arrow[d, "p_2"] \\
E_1 \arrow[r, "p_1"'] & Q
\end{tikzcd} \tag{4.4}$$

with the composite morphism $\pi_1 p_1 = \pi_2 p_2$ to Q. Recall that for categories of sets (possibly with algebraic structure), the pullback $E_1 \times_Q E_2$ is realised as $\{(e_1, e_2) \in E_1 \times E_2 \mid e_1 p_1 = e_2 p_2\}$, with the projections $\pi_i : E_1 \times_Q E_2 \to E_i;\ (e_1, e_2) \mapsto e_i$.

4.1.2. *Abelian groups.* The category **Set** of sets has all finite products, including the empty product as the terminal object T (the codomain of a unique morphism from each object). An abelian group $(A, +, 0)$ is an object A of **Set** with an addition morphism $+ : A^2 \to A$, a negation morphism $-1 : A \to A$, and a zero morphism $0 : A^0 \to A$ from the terminal object $T = A^0$, for which diagrams such as

$$\begin{tikzcd}
A \arrow[r, "(1,-1)"] \arrow[d] & A^2 \arrow[d, "+"] \\
A^0 \arrow[r, "0"'] & A
\end{tikzcd} \tag{4.5}$$

(expressing the identities for abelian groups, in this case $a + (-a) = 0$) commute. An *abelian group A in a category* $\mathbf{C}$ with finite products is an object A of $\mathbf{C}$ with an addition morphism $+ : A^2 \to A$, a negation morphism $-1 : A \to A$, and a zero morphism $0 : A^0 \to A$ from the terminal object $T = A^0$, for which the diagrams (4.5) commute.

If M is a module over a group Q, the projection $p : E \to Q$ (4.2) is an abelian group in the slice category $\mathbf{Gp}/Q$. The addition is

$$+ : E \times_Q E \to E; \quad \big((q, m_1), (q, m_2)\big) \mapsto (q, m_1 + m_2)$$

and the zero morphism is given by the group homomorphism η of (4.3), determining the morphism

$$\begin{tikzcd} Q \arrow[r, "\eta"] \arrow[d, "1_Q"'] & E \arrow[d, "p"] \\ Q \arrow[r, "1_Q"'] & Q \end{tikzcd} \tag{4.6}$$

from the terminal object $1_Q : Q \to Q$ of the slice category $\mathbf{Gp}/Q$.

4.1.3. *Modules.* Given a module M over a group Q, the split extension $p : Q \ltimes M \to Q$ (4.2) is an abelian group in the slice category $\mathbf{Gp}/Q$. For q in Q, the conjugation action of the element q^η on the normal subgroup $p^{-1}\{1\}$ of $Q \ltimes M$ is given by

$$(q,0)\backslash(1,m)(q,0) = (mq,0), \tag{4.7}$$

thereby reflecting the action of Q on the module M.

Conversely, suppose that $p : E \to Q$ is an abelian group in the slice category $\mathbf{Gp}/Q$, with addition $+ : E \times_Q E \to E$ and zero morphism as in (4.6). Let M denote the inverse image $p^{-1}\{1\}$ of the identity element 1 of Q under p. For elements m_1 and m_2 of M, the pair (m_1, m_2) lies in the pullback $E \times_Q E$, and the image $m_1 + m_2$ of the pair (m_1, m_2) under the addition again lies in M. In this way, the set M receives an abelian group structure. In analogy with (4.7), each element q of Q acts on M by

$$q : m \mapsto q^\eta \backslash m q^\eta ,$$

making M a right Q-module.

In summary, it is seen that modules over a group Q are equivalent to abelian groups $p : E \to Q$ in the slice category $\mathbf{Gp}/Q$ of groups over Q. It is this module concept which allows itself to be extended to arbitrary quasigroups (§4.2.1).

4.1.5. *Exercises.*

1. Using the definition (4.1) of the product in the split extension, verify the formula (4.7).

2. The group $\mathbb{Z}/3\mathbb{Z}$ of integers modulo 3 acts as a nontrivial group of automorphisms of the Klein 4-group. The corresponding split extension is a group of order 12. Can you recognise this group?

3. Produce a full set of commuting diagrams like (4.5) to define abelian groups (associativity, commutativity, etc.).

4.2. Modules over quasigroups

4.2.1. *Quasigroup modules.* Let $\mathbf{V}$ be a *variety* of quasigroups, a class of quasigroups closed under homomorphic images, subquasigroups, and products. Equivalently (by Birkhoff's Theorem [7, IV Th. 2.3.3]), V is the class of all quasigroups satisfying a given set of identities. As examples, consider the variety $\mathbf{G}$ of associative quasigroups (§1.2.1), the variety $\mathbf{A}$ of abelian quasigroups, the variety $\mathbf{Q}$ of all quasigroups, or the variety $\mathbf{STS}$ of Steiner triple systems — idempotent (1.3) and totally symmetric (1.4) quasigroups (§1.3). The variety $\mathbf{V}$ may also be considered as a category. The class of quasigroups is the object class of the category, while the morphisms are the quasigroup homomorphisms between the quasigroups in the class. As a category, $\mathbf{V}$ has all limits and colimits, in particular all pullbacks, products and coproducts (free products) [7, IV §2.2].

For a quasigroup Q in $\mathbf{V}$, a *Q-module* in the variety $\mathbf{V}$ is defined as an abelian group $p : E \to Q$ in the slice category $\mathbf{V}/Q$ of $\mathbf{V}$-quasigroups over Q. If Q is a group, it is apparent from §4.1.4 that Q-modules in the variety $\mathbf{G}$ are equivalent to Q-modules in the usual sense.

Given two Q-modules $p_i : E_i \to Q$ in $\mathbf{V}$ (with $i = 1, 2$), a Q-module homomorphism is a $\mathbf{V}/Q$-morphism $f : E_1 \to E_2$ that commutes with the abelian group structures: $0f = 0$, $(-1)f = f(-1)$, and $+f = (f \times_Q f)+$. The Q-modules in $\mathbf{V}$ form a category $\mathbb{Z} \otimes \mathbf{V}/Q$.

4.2.2. *Universal multiplication groups.*The definition of modules over a quasigroup given in §4.2.1 is rather abstract. A direct description depends on certain groups associated with a quasigroup Q in a variety $\mathbf{V}$. Let $Q[X]_{\mathbf{V}}$ or $Q[X]$ be the free product (coproduct) of Q in $\mathbf{V}$ with the free quasigroup in $\mathbf{V}$ on a single generator X. The $\mathbf{V}$-quasigroup $Q[X]$ is analogous to a ring of polynomials, and is characterised by a similar universal property: for every quasigroup E in $\mathbf{V}$ that is the codomain of a $\mathbf{V}$-morphism $\eta : Q \to E$, and for every element x of E, there is a unique quasigroup homomorphism $Q[X] \to E$ restricting to η on the subquasigroup Q of $Q[X]$, and mapping the indeterminate X to x in E.

The *universal multiplication group* $\widetilde{G}$ or $U(Q, \mathbf{V})$ of Q in $\mathbf{V}$ is the relative multiplication group of Q in $Q[X]$. If Q is a subquasigroup of a quasigroup E in $\mathbf{V}$, the relative multiplication group of Q in E is a quotient of $\widetilde{G}$. In particular, the combinatorial multiplication group G of Q is a quotient of $\widetilde{G}$. In this way $\widetilde{G}$ acts on Q, and an element e of Q has its stabiliser in $\widetilde{G}$, the *universal stabiliser* $\widetilde{G}_e$.

4.2.3. *Examples of universal multiplication groups.*

1. The universal multiplication group $U(Q,\mathbf{Q})$ of a quasigroup Q in the variety $\mathbf{Q}$ of all quasigroups is the free group on the set $L(Q)+R(Q)$, the disjoint union of two copies of the set Q.

2. The universal multiplication group $U(Q,\mathbf{G})$ of a group Q in the variety $\mathbf{G}$ of all associative quasigroups is the direct square $Q \times Q$. Compare with §1.4.4, where the combinatorial multiplication group of Q is obtained from the direct square $Q \times Q$ by dividing out the diagonal copy of the centre $Z(Q)$.

3. For an abelian group Q in the variety $\mathbf{A}$ of all abelian quasigroups, $U(Q,\mathbf{A}) \cong Q$ — Exercise 4.2.6 (1).

4. The universal multiplication group $U(Q,\mathbf{STS})$ of a Steiner triple system Q in the variety $\mathbf{STS}$ of all Steiner triple systems is the free product (in the variety of groups) of $|Q|$ copies of the cyclic group of order 2. It is also described as the set $Q^\times$ of words in the alphabet Q without adjacent letters repeated. Each letter q from Q corresponds to $R(q)$ in $U(Q,\mathbf{STS})$. The product in the group is obtained from concatenation of words followed by cancellation of adjacent pairs of identical letters. For example, $q_1q_2q_3 \cdot q_3q_2 = q_1$. The identity element is the empty word.

4.2.4. *The Fundamental Theorem.* Let Q be a quasigroup, considered in the variety $\mathbf{Q}$ of all quasigroups. Let $\widetilde{G}$ be the universal multiplication group $U(Q,\mathbf{Q})$ of Q in $\mathbf{Q}$. Let e be an element of Q, with corresponding universal stabiliser $\widetilde{G}_e$. The *Fundamental Theorem of Quasigroup Representations* [6, Th. 10.1] states that modules over the quasigroup Q are equivalent to modules over the group $\widetilde{G}_e$.

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. 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. This action consists of automorphisms of the abelian group M. Thus the Q-module $p : E \to Q$ yields a $\widetilde{G}_e$-module $M = p^{-1}\{e\}$.

Conversely, for a $\widetilde{G}_e$-module M, a corresponding abelian group in $\mathbf{Q}/Q$ has to be constructed. 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

$$s(q,g)\rho(e,qg) = \rho(e,q)g \tag{4.8}$$

— Exercise 1.4.5 (5). Note that

$$s(e,g_e) = g_e \tag{4.9}$$

for g_e in $\widetilde{G}_e$. Now consider the $\widetilde{G}$-set $E = M \times Q$ with action

$$(m,q)g = \bigl(ms(q,g), qg\bigr)\,. \tag{4.10}$$

— compare Exercise 4.2.6 (2). Define local abelian group structures on E by

$$(m_1,q) - (m_2,q) = (m_1 - m_2, q) \tag{4.11}$$

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

$$\begin{cases} a \cdot b = aR(b\pi) + bL(a\pi)\,; \\ a/b = (a - bL(a\pi/b\pi))R(b\pi)^{-1}\,; \\ a\backslash b = (b - aR(a\pi\backslash b\pi))L(a\pi)^{-1}\,. \end{cases} \tag{4.12}$$

With this structure, $\pi : E \to Q$ becomes an abelian group object in the category $\mathbf{Q}/Q$. Note that by (4.9), the $\widetilde{G}_e$-modules M and $\pi^{-1}\{e\}$ are isomorphic.

4.2.5. *Differential calculus.* The Fundamental Theorem of Quasigroup Representations provides a *differentiation* process applying 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 (4.12), the action of a quasigroup word $x_1 \dots x_n w$ on this object is given by

$$(m_1,q_1)\dots(m_n,q_n)w = \Bigl(\sum_{h=1}^{n} m_h \rho(e,q_h)\frac{\partial w}{\partial x_h}\rho(e,w)^{-1}, q_1 \dots q_n w\Bigr) \tag{4.13}$$

for certain elements

$$\frac{\partial w}{\partial x_h} = \frac{\partial w}{\partial x_h}(q_1,\dots,q_n) \tag{4.14}$$

of $\mathbb{Z}\widetilde{G}$. Notational conventions similar to those of calculus are used. The functions

$$\frac{\partial w}{\partial x_h} : Q^n \to \mathbb{Z}\widetilde{G}; (q_1, \ldots, q_n) \mapsto \frac{\partial w}{\partial x_h}(q_1, \ldots, q_n) \tag{4.15}$$

for $1 \leqslant h \leqslant n$ are known as the *partial derivatives* of the quasigroup word $x_1 \ldots x_n w$. They are computed inductively using the parsing of the word $x_1 \ldots x_n w$. For $xw = x$, (4.13) simply gives

$$\frac{\partial x}{\partial x} = 1\,. \tag{4.16}$$

More generally, the derivatives of the projection $x_1 \ldots x_i \ldots x_n \pi_i = x_i$ are given by

$$\frac{\partial \pi_i}{\partial x_j} = \delta_{ij}\,.$$

For $x_1 \ldots x_k x_{k+1} \ldots x_{k+l} w = x_1 \ldots x_k u \cdot x_{k+1} \ldots x_{k+l} v$, (4.12) and (4.13) give

$$\begin{aligned}
(m_1, q_1) \ldots (m_{k+l}, q_{k+l}) w &= \Big(\sum_{h=1}^{k+l} m_h \rho(e, q_h) \frac{\partial w}{\partial x_h} \rho(q_h, w)^{-1}, w \Big) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1}, u \Big) \cdot \Big(\sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1}, v \Big) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1}, u \Big) R(q_{k+1} \ldots q_{k+l} v) \\
&\quad + \Big(\sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1}, q_{k+1} \ldots q_{k+l} v \Big) L(q_1 \ldots q_k u) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1} s\big(u, R(v)\big) + \\
&\qquad \sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1} s\big(v, L(u)\big), w \Big)\,,
\end{aligned}$$

leading to the *Product Rules*

$$\frac{\partial w}{\partial x_i} = \frac{\partial u}{\partial x_i} R(x_{k+1} \ldots x_{k+l} v)$$

for $1 \leqslant i \leqslant k$ and

$$\frac{\partial w}{\partial x_j} = \frac{\partial v}{\partial x_j} L(x_1 \dots x_k u)$$

for $k < j \leqslant k + l$. These may be summarized as

$$\frac{\partial(u \cdot v)}{\partial x_i} = \frac{\partial u}{\partial x_i} R(v)\,; \tag{4.17}$$

$$\frac{\partial(u \cdot v)}{\partial x_j} = \frac{\partial v}{\partial x_j} L(u)\,. \tag{4.18}$$

Note that if there are repeated arguments in the word w, say $q_i = q_j$ with $i \leqslant k < j$, then $\partial w / \partial x_i$ will include the sum of $\partial(u \cdot v)/\partial x_i$ as given by (4.17) and $\partial(u \cdot v)/\partial x_j$ as given by (4.18).

4.2.6. *Exercises.*

1. Let Q be an abelian group, considered in the variety $\mathbf{A}$ of abelian quasigroups.

   (a) Show that $Q[X]_{\mathbf{A}} = Q \oplus \mathbb{Z}$.

   (b) Show that $U(Q, \mathbf{A}) \cong Q$.

2. In the context of §4.2.4, let M be a $\widetilde{G}_e$-module.

   (a) Show that $s(q,g)s(qg,h) = s(q,gh)$ for $q \in Q$ and $g, h \in \widetilde{G}$.

   (b) Show that (4.10) does give a group action: for m in M, q in Q and g_1, g_2 in $\widetilde{G}$, show $(m,q)(g_1 g_2) = \big((m,q)g_1\big)g_2\,.$

3. In the context of §4.2.4, let M be a $\widetilde{G}_e$-module. Show that (4.12) defines a quasigroup structure on $E = M \times Q$.

4. Show that

$$\frac{\partial x^2}{\partial x} = R(x) + L(x)\,.$$

5. For nonassociative powers x^l and x^r, show that

$$\frac{\partial(x^l \cdot x^r)}{\partial x} = \frac{\partial x^l}{\partial x} R(x) + \frac{\partial x^r}{\partial x} L(x)\,.$$

   Conclude that nonassociative powers of x are indexed by their derivatives, which are noncommutative polynomials in $R(x)$ and $L(x)$ — the “index ψ-polynomials” of [3].

6. Derive the *Right Quotient Rules*

$$\frac{\partial(u/v)}{\partial x_i} = \frac{\partial u}{\partial x_i} R(v)^{-1}\,;$$
$$\frac{\partial(u/v)}{\partial x_j} = -\frac{\partial v}{\partial x_j} L(u/v) R(v)^{-1}\,;$$

and the *Left Quotient Rules*

$$\frac{\partial(u\backslash v)}{\partial x_i} = -\frac{\partial u}{\partial x_i} R(u\backslash v) L(u)^{-1}\,;$$
$$\frac{\partial(u\backslash v)}{\partial x_j} = \frac{\partial v}{\partial x_j} L(u)^{-1}\,.$$

7. Let Q be a group, with identity element e. Take $\widetilde{G}$ to be the universal multiplication group $U(Q, \mathbf{G})$ of Q in the variety $\mathbf{G}$ of associative quasigroups. Show that Q-modules are equivalent to $\widetilde{G}_e$-modules.

References

[1] **O. Chein et al.:** *Quasigroups and Loops: Theory and Applications*, Heldermann, Berlin, 1990.

[2] **G. Higman, B.H. Neumann and H. Neumann:** *Embedding theorems for groups*, J. London Math. Soc. **24** (1949), 247 – 254.

[3] **H. Minc:** *Index polynomials and bifurcating root-trees*, Proc. Roy. Soc. Edin., A **65** (1957), 319 – 341.

[4] **R. Penrose:** *A generalised inverse for matrices*, Proc. Camb. Phil. Soc. **51** (1955), 406 – 413.

[5] **J. D. H. Smith:** *Mal'cev Varieties*, Springer, Berlin, 1976.

[6] **J. D. H. Smith:** *An Introduction to Quasigroups and their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.

[7] **J. D. H. Smith and A. B. Romanowska:** *Post-Modern Algebra*, Wiley, New York, NY, 1999.

Department of Mathematics
Iowa State University Ames, Iowa 50011-2064
U.S.A.
E-mail: jdhsmith@math.iastate.edu
http://www.orion.math.iastate.edu/jdhsmith/

Received April 24, 2007