SYLOW THEORY FOR QUASIGROUPS

JONATHAN D. H. SMITH

Abstract. This paper is intended as a first step toward a general Sylow theory for quasigroups and Latin squares. A subset of a quasigroup lies in a *non-overlapping orbit* if its respective translates under the elements of the left multiplication group remain disjoint. In the group case, each non-overlapping orbit contains a subgroup, and Sylow's Theorem guarantees non-overlapping orbits on subsets whose order is a prime-power divisor of the group order. For the general quasigroup case, the paper investigates the relationship between non-overlapping orbits and structural properties of a quasigroup. Divisors of the order of a finite quasigroup are classified by the behavior of non-overlapping orbits. In a dual direction, Sylow properties of a subquasigroup P of a finite left quasigroup Q may be defined directly in terms of the homogeneous space $P\backslash Q$, and also in terms of the behavior of the isomorphism type $[P\backslash Q]$ within the so-called Burnside order, a labeled order structure on the full set of all isomorphism types of irreducible permutation representations.

This is a preprint version. Please cite the published version as: J.D.H. Smith, Sylow theory for quasigroups, *J. Combin. Designs* **23** (2015), 115–133.

1. Introduction

The goal of the present paper is to initiate a study of Sylow theory for general quasigroups and Latin squares, going beyond some recent developments for Moufang loops (compare [4] – [8], [10], [24]). It is to be expected that this theory will become much more diverse and ramified than its group-theoretical prototype.

Two approaches are adopted in the paper. The starting point for the first is the permutation representation proof of Sylow's theorems for finite groups ([11, §I.7] [16, 17] [22, §10.8] [25]), examining the behavior of subsets of a given size under left multiplication by group elements.

2010 *Mathematics Subject Classification.* 20N05.

Key words and phrases. Latin square, quasigroup, Sylow theorem, Moufang loop, Paige loop, permutation representation.

The orbit of a given subset is described as *non-overlapping* if its members are disjoint; otherwise, the orbit is said to be *overlapping*. Each subgroup lies in a non-overlapping orbit, and each non-overlapping orbit contains a subgroup (compare Proposition 5.1). For subsets whose order is a prime-power divisor of the group order, non-overlapping orbits are guaranteed to exist (in a number that is congruent to 1 modulo the prime in question). For general finite quasigroups, the much more richly varied behavior of overlapping and non-overlapping orbits on subsets of different sizes becomes the main concern. One may characterize this direction as a **bottom-up** approach to Sylow theory.

The second, **top-down** approach, primarily addresses issues related to analogues of the conjugacy, maximality, or number of Sylow subgroups of groups within the context of the permutation representation theory of (left) quasigroups. The fundamental concept of that theory is the notion of a *homogeneous space* $P\backslash Q$ for a subquasigroup P of a (left) quasigroup Q, defined as the set of orbits of the relative left multiplication group of P in Q as it acts on the set Q. The subquasigroup P is *right Lagrangean* if these orbits all have the same length. The (left) quasigroup Q acts on the space $P\backslash Q$ in stochastic fashion, with Markov matrices instead of permutation matrices. The *Burnside order* of Q keeps track of the isomorphism types of these stochastic actions, and forms the framework for the top-down approach.

Despite some ostensibly algebraic language, the current theory is really involved with the combinatorial structure of Latin squares, as the multiplication tables of finite quasigroups. In that light, the bottom-up approach to Sylow theory may be seen to play a role that is dual to the top-down approach. For example, consider a subquasigroup P of a finite quasigroup Q, and the bordered multiplication table of Q. If P lies in a non-overlapping orbit, then the part of the multiplication table consisting of **columns** labeled by elements of P has a special property: any two of its **rows** have either the same or completely disjoint sets of elements. Dually, if P is right Lagrangean, then the part of the multiplication table consisting of **rows** labeled by elements of P has the corresponding property: any two of its **columns** have either the same or completely disjoint sets of elements.

Readers are referred to [21] and [23] for quasigroup-theoretic and general algebraic concepts and conventions that are not otherwise explicitly clarified here.

2. Plan of the paper

After introductory sections recalling some basic concepts and notation, the definition of overlapping and non-overlapping orbits in the quasigroup context is presented in Section 5. Congruence classes, such as normal subquasigroups, lie in non-overlapping orbits. Theorem 5.5 establishes a converse for commutative quasigroups, where subsets that are not congruence classes are shown to lie in overlapping orbits. (The existence of proper, non-trivial subgroups of finite simple groups shows that the assumption of commutativity is essential.) In general quasigroups, non-overlapping orbits do not necessarily contain subquasigroups. Theorem 7.1 provides sufficient conditions under which one may expect to find a subquasigroup in a non-overlapping orbit. A geometrical application of some of these results appears in Section 6.

Definition 8.1 presents the basic classification of divisors of the order of a finite quasigroup by progressively stronger types, in terms of the existence of non-overlapping orbits, the presence of subquasigroups within them, and the Lagrangean behavior of those subquasigroups. Note that Lagrangean properties are understood here in the stronger sense provided by quasigroup permutation representation theory: a subquasigroup is (right) Lagrangean if its relative left multiplication group acts semitransitively (compare [21, §4.5] and Section 4 below). A divisor d has type J if non-overlapping orbits on subsets of size d exist. It has type I if at least one of those non-overlapping orbits contains a subquasigroup, and type H if each of the non-overlapping orbits contains a subquasigroup. It has type G ("group type") if the subquasigroups in non-overlapping orbits are Lagrangean. Examples 8.3–8.7 separate the types. Theorem 8.8 shows that if d has type G, then each non-overlapping orbit contains a unique subquasigroup.

Section 9 establishes a connection between the current theory and the Sylow theory developed by Gagola III, Grishkov, Zavaritsine *et al.* for finite Moufang loops. In the Paige loops $\mathsf{PSL}_{1,3}(q)$ (also denoted $P(q)$, $\mathrm{M}(q)$, or $\mathrm{SLL}(q)$) for prime powers q (the finite, non-associative simple Moufang loops), certain primes p (dividing q^2+1) are "bad" from the point of view of Sylow theory, in that there are no non-trivial p-subloops of $\mathsf{PSL}_{1,3}(q)$, even though these primes are divisors of $|\mathsf{PSL}_{1,3}(q)|$. For example, 5 is a "bad" prime for the smallest Paige loop $\mathsf{PSL}_{1,3}(2)$ of order 120. A general result about diassociative loops (Theorem 9.2) classifies these bad primes as not belonging to the weakest type J of Definition 8.1.

The second, top-down approach of the paper works in the broader context of left quasigroups. The class of left quasigroups, generalizing

quasigroups, ranges from groups at one extreme to sets (with projections) at the other. Section 4 describes the homogeneous space $P\backslash Q$ associated with a sub-(left)-quasigroup P of a left quasigroup Q. If Q is finite and p is a (rational) prime, then P is a *Sylow p-subquasigroup* if $|P|$ is a power of p, $|P\backslash Q|$ is coprime to Q, and $|P| \cdot |P\backslash Q| = |Q|$ (Definition 10.1). This definition just extends the usual group-theory concept, although it is more stringent than a definition that has been used previously for Moufang loops ([4] – [8], [10]), since the Paige loop of order 120 has no Sylow 2-subloops in the present sense (Corollary 10.5). Sylow p-subquasigroups are studied in Sections 10 and 11. Proposition 10.6 establishes the basic relationship with the preceding "bottom-up" Sylow theory. Section 11 then examines cyclic subgroups of diassociative loops, which are especially well-behaved. Theorem 11.4 shows that in a diassociative loop, the number of cyclic subgroups that are maximal p-subgroups for a prime p is congruent to 1 modulo p. As noted in Example 11.5, this result matches the known number 28 of Sylow 3-subgroups in the Paige loop of order 120.

A new, elementary survey of the permutation representation theory of (left) quasigroups is presented in Section 12. The presentation avoids mention of the coalgebras that are needed for deeper questions, and also uses $\mathbb{Q}$ as a more appropriate ground field for the current discussion (compare [21, Ch. 5]). Associated with each finite left quasigroup Q is a labeled, ordered set of isomorphism types $[P\backslash Q]$ of homogeneous spaces $P\backslash Q$, known as the *Burnside order* (Section 13). For a finite group, the Burnside order is the poset of conjugacy classes of subgroups. Within the Burnside order, Definition 13.3 defines a *Sylow p-type* for a prime p. If P is a Sylow p-subquasigroup, then $[P\backslash Q]$ is a Sylow p-type (Proposition 13.5). The converse holds if Q is a quasigroup (Proposition 13.7), but may fail in a proper left quasigroup (Example 13.8). The conjugacy and maximality of Sylow subgroups of finite groups are then captured by the respective concepts of *Sylowian* and *strongly Sylowian* prime numbers for a finite left quasigroup Q (Definition 13.9). If Q is a group, all primes are strongly Sylowian. The prime 3 is strongly Sylowian for the Paige loop of order 120 (Example 13.10). Finally, a general prime p is strongly Sylowian for a non-trivial projection quasigroup Q if $p \nmid |Q|$ (Proposition 13.11).

3. Left, right, and two-sided quasigroups

Quasigroups, left quasigroups, and right quasigroups may be defined combinatorially or equationally. Combinatorially, all three form

a structure $(Q, \cdot)$, embodying a set Q equipped with a binary *multiplication* operation denoted by $\cdot$ or simple juxtaposition of the two arguments. Then the *opposite* Q^{op} is the set Q taken with the operation

$$Q \times Q \to Q; (x, y) \mapsto y \cdot x \,.$$

The structure $(Q, \cdot)$ is a (*two-sided*) *quasigroup* if specification of any two of x, y, z in the equation

$$x \cdot y = z \tag{3.1}$$

determines the third uniquely. In a *left quasigroup*, specification of x and z in (3.1) determines y uniquely. Then $(Q, \cdot)$ is a *right quasigroup* if its opposite is a left quasigroup. In other words, specification of y and z in (3.1) determines x uniquely.

Equationally, a quasigroup $(Q, \cdot, /, \backslash)$ is a set Q equipped with three binary operations of multiplication, *right division* $/$ and *left division* $\backslash$, satisfying the identities:

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

These identities correspond to the existence and uniqueness of the solutions of (3.1). For example, (SL) says that $x\backslash z$ is a solution y to (3.1) for given x and z. On the other hand, given solutions y_1 and y_2, so that $x \cdot y_1 = z = x \cdot y_2$, the identity (IL) shows that $y_1 = x\backslash(x \cdot y_1) = x\backslash(x \cdot y_2) = y_2$, so any solution is unique.

A group forms a quasigroup, with $x\backslash z = x^{-1}z$ and $z/y = zy^{-1}$. Any set Q forms a left quasigroup $(Q, \cdot, \backslash)$, with the *right projection* operations $x \cdot y = x\backslash y = y$, or a right quasigroup $(Q, \cdot, /)$, with the *left projection* operations $x \cdot y = x/y = x$.

The body of the multiplication table of a two-sided quasigroup forms a Latin square, with each element appearing just once in each column and each row. In the multiplication table of a left quasigroup, each element appears just once in each row. Dually, in the multiplication table of a right quasigroup, each element appears just once in each column. These combinatorial conditions are conveniently symbolized by the respective multiplication tables on the set $\{0, 1\}$ of bits or residues modulo 2, given by the quasigroup of addition modulo 2, the left quasigroup with the right projection operation, and the right quasigroup with the left projection operation:

$$\begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}, \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 0 & 1 \end{array}, \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 1 & 1 \end{array}.$$

A subset P of a quasigroup $(Q, \cdot, /, \backslash)$ is a *subquasigroup* if it is closed under the multiplication and the two divisions. When considering subsets of a left quasigroup that are closed under the multiplication and left division operations, the term *subquasigroup* will again be used, in place of the cumbersome "sub-left-quasigroup." Thus the nonempty subquasigroups of a group are precisely the subgroups, while each subset of a right projection left quasigroup is a subquasigroup.

4. Lagrangean subquasigroups

For each element x of a set Q with a multiplication operation, consider the *right multiplication*

$$R(x)\colon Q \to Q; y \mapsto y \cdot x$$

and *left multiplication*

$$L(x)\colon Q \to Q; y \mapsto x \cdot y\,.$$

On a quasigroup, the right and left multiplications are elements of the group $Q!$ of bijections from the set Q to itself. For example, the identity (SL) says that each $L(x)$ surjects, while (IL) gives the injectivity of $L(x)$. On a left quasigroup, the left multiplications are bijections. Dually, the right multiplications on a right quasigroup are bijective.

The *left multiplication group* of a (left) quasigroup Q is the subgroup

$$\mathrm{LMlt}\, Q = \langle L(q) \mid q \in Q \rangle_{Q!}$$

of $Q!$ generated by the left multiplications. The (*two-sided*) *multiplication group* of a quasigroup Q is defined as the subgroup

$$\mathrm{Mlt}\, Q = \langle L(q), R(q) \mid q \in Q \rangle_{Q!}$$

of $Q!$ generated by all the left and right multiplications. If Q is commutative, then $\mathrm{LMlt}\, Q = \mathrm{Mlt}\, Q$.

For a subquasigroup P of a (left) quasigroup Q, the *relative left multiplication group* of P in Q is the subgroup $\mathrm{LMlt}_Q(P)$ of $\mathrm{LMlt}\, Q$ generated by $L_Q(P) = \{L(p) : Q \to Q \mid p \in P\}$. If Q is a group and P is nonempty, then the set of orbits of $\mathrm{LMlt}_Q P$ on Q is the set

$$P\backslash Q = \{Px \mid x \in Q\} \tag{4.1}$$

of cosets of P.

Let P be a subquasigroup of a finite (left) quasigroup Q. Let $P\backslash Q$ denote the set of orbits of the permutation group $\mathrm{LMlt}_Q P$ on the set Q. This set is known as a *homogeneous space*. If Q is a group, the notation is consistent with (4.1). In the group case, $\mathrm{LMlt}_Q P$ always acts semitransitively on Q, in the sense that each orbit has size $|P|$. In the general (left) quasigroup case, the subquasigroup P is said to be

(*right*) *Lagrangean* in Q if $\mathrm{LMlt}_Q P$ acts semitransitively on Q (compare [21, §4.5]). Dually, a subquasigroup P of a (right) quasigroup Q is said to be *left Lagrangean* in Q if P is right Lagrangean in Q^{op}. A subquasigroup P of a quasigroup Q is *Lagrangean* in Q if it is both right and left Lagrangean.

Lagrange's Theorem implies that each subgroup of a finite group is right Lagrangean. In any left quasigroup Q, the relative left multiplication group of the empty subquasigroup $\varnothing$ is trivial. Since the orbits are all singletons, $\varnothing$ is right Lagrangean. Similarly, in a right projection quasigroup, each subquasigroup (each subset) is right Lagrangean.

5. Non-overlapping orbits

Let Q be a quasigroup. For each natural number $r \leq |Q|$, the left multiplication group $\mathrm{LMlt}\, Q$ of Q acts on the set $\binom{Q}{r}$ of subsets of Q of size r. An orbit of this action is said to be *overlapping* if it contains pairs of elements which are not disjoint. Otherwise, the orbit is described as *non-overlapping*. If Q is finite, then a non-overlapping orbit will only appear if r is a divisor of $|Q|$, since the equal-sized sets in such an orbit partition Q. The following two propositions exhibit the occurrence of non-overlapping orbits.

Proposition 5.1. *Let Q be a finite group.*

(a) *If P is a subgroup of Q, then P lies in a non-overlapping orbit.*
(b) *Each non-overlapping orbit of Q contains a subgroup of Q.*

Proof. (a): The orbit of P is the set $\{xP \mid x \in Q\}$ of left cosets of P.

(b): Let P be that member of a non-overlapping orbit which contains the identity element 1 of Q. The set-wise stabilizer $(\mathrm{LMlt}\, Q)_P$ of P is $\{L(x) \mid x \in Q \text{ and } xP = P\}$. Now for x in Q, the relation $xP = P$ implies $x = x1 \in P$, so the group isomorphism $L\colon Q \to \mathrm{LMlt}\, Q$ restricts to a group isomorphism $L\colon P \to (\mathrm{LMlt}\, Q)_P$, and in particular P is a subgroup of Q. □

Proposition 5.2. *Let V be a congruence on a finite quasigroup Q. Then the set of V-classes constitutes a non-overlapping orbit.*

Proof. Let S be a congruence class of V, with elements s and s'. Then for each element x of Q, the relations $x\ V\ x$ and $s\ V\ s'$ imply $xs\ V\ xs'$, so $SL(x)$ is again a congruence class of V. It follows that the orbit of S is the set of congruence classes of V. Since these classes are disjoint, the orbit of S is non-overlapping. □

Corollary 5.3. *Let P be a subquasigroup of a finite quasigroup Q. If P is normal, then it lies in a non-overlapping orbit.*

Corollary 5.4. *Let P be a subquasigroup of a finite quasigroup Q, with $0 < |P| = |Q|/2$. Then P lies in a non-overlapping orbit.*

The following theorem exhibits overlapping orbits involving subsets of certain quasigroups Q whose size may be a divisor of $|Q|$.

Theorem 5.5. *Let Q be a finite commutative quasigroup. Let P be a subset of Q that is not a congruence class in Q. Then P lies in an overlapping orbit.*

Proof. Let e be an element of P. If P was a congruence class, then it would be preserved by the stabilizer

$$(\mathrm{LMlt}\, Q)_e = \langle L(x/e)L(y)L(yx/e)^{-1} \mid x, y \in Q \rangle_{Q!}$$

of the element e in the (left) multiplication group of Q. Moreover, for elements a, b, c of Q, whenever $(a/e)b = c$ and two of a, b, c were in P, then the third would also lie in P. (Compare [13],[21, Cor. 2.6 and Ch. 3, Exer. 10].) Since P is not a congruence class, however, at least one of the following four cases applies.

Case (a): There are elements b, c of P such that $(a/e)b = c$ with $a = eL(c/b) \notin P$. Then the element $c = bL(c/b)$ lies in the intersection of the distinct subsets P and $PL(c/b)$, so the orbit of P is overlapping.

Case (b): There are elements a, c of P such that $(a/e)b = c$ with $b = cL(a/e)^{-1} \notin P$. Then the element $e = aL(a/e)^{-1}$ lies in the intersection of the distinct subsets P and $PL(a/e)^{-1}$, so the orbit of P is overlapping.

Case (c): There are elements a, b of P such that $(a/e)b \notin P$. Then the element $a = eL(a/e)$ lies in the intersection of the distinct subsets P and $PL(a/e)$, so the orbit of P is overlapping.

Case (d): There are elements x, y of Q with $PL(x/e)L(y)L(yx/e)^{-1} \neq P$. Then the element e lies in the intersection of the distinct subsets P and $PL(x/e)L(y)L(yx/e)^{-1}$, so the orbit of P is overlapping. □

Remark 5.6. The commutativity assumption is needed in Theorem 5.5. Suppose that Q is a finite simple (non-commutative) group. Then by Proposition 5.1(a), any proper, non-trivial subgroup P of Q lies in a non-overlapping orbit, even though P is not a congruence class in Q.

Corollary 5.7. *Let Q be a finite commutative quasigroup. Let P be a subquasigroup of Q that is not normal. Then P lies in an overlapping orbit.*

Corollaries 5.3 and 5.7 identify the structural significance of subquasigroups of commutative quasigroups that lie in non-overlapping orbits.

Corollary 5.8. *Let P be a subquasigroup of a finite commutative quasigroup Q. Then P lies in a non-overlapping orbit iff it is a normal subquasigroup of Q.*

6. Some affine geometry

Let n and d be positive integers, with n odd. Consider the power $Q = (\mathbb{Z}/_n)^d$ with the commutative, idempotent multiplication

$$x \cdot y = 2^{-1}(x + y)\,. \tag{6.1}$$

Now $(Q, \cdot, /, \backslash)$ is a quasigroup, with divisions

$$y/x = x\backslash y = 2y - x\,.$$

Since $(Q, \cdot)$ is entropic, each subquasigroup is normal [21, §3.10, Ex. 1]. Furthermore, a subset S of Q is a (normal) subquasigroup of Q if and only if it is an affine subspace of the affine geometry $\mathsf{AG}(d, \mathbb{Z}/_n)$ of dimension d over $\mathbb{Z}/_n$ (compare [19, Cor. 6.6.9], for example). By Corollary 5.3 and Theorem 5.5, this means that S is an affine subspace if and only if it lies in a non-overlapping orbit.

Within the quasigroup $(Q, \cdot)$ with multiplication (6.1), one has

$$L(x)\colon Q \to Q; y \mapsto 2^{-1}y + 2^{-1}x\,. \tag{6.2}$$

In particular, the *doubling map*

$$L(0)^{-1}\colon Q \to Q; y \mapsto 2y$$

and the *translation*

$$L(0)^{-1}L(2x)\colon Q \to Q; y \mapsto y + x$$

by each element x of Q lie in $\mathrm{LMlt}\, Q$. Indeed, $\mathrm{LMlt}\, Q$ is generated by the doubling and the full set of translations, since by (6.2), the left multiplication $L(x)$ by an element x of Q is the composition of the inverse of the doubling with the translation by $2^{-1}x$. In summary, one obtains the following combinatorial-geometrical consequence of the results of the previous section.

Theorem 6.1. *Let n and d be positive integers, with n odd. In the affine geometry $\mathsf{AG}(d, \mathbb{Z}/_n)$ of dimension d over the ring $\mathbb{Z}/_n$ of integers modulo n, let Γ be the group of affine transformations generated by the doubling and translations. Let S be a set of points in the geometry. Then S is an affine subspace if and only if $S \cap S\gamma$ is never a proper, non-empty subset of S for any affine transformation γ in Γ.*

7. Subquasigroups in non-overlapping orbits

Proposition 5.1(b) showed that in a finite, non-trivial associative quasigroup Q, each non-overlapping orbit contains a subquasigroup. The following theorem adapts that result to general quasigroups with idempotent elements.

Theorem 7.1. *Let e be an idempotent element of a finite quasigroup Q. Suppose that a subset P of Q satisfies the following conditions:*

(a) *$e \in P$;*
(b) *P lies in a non-overlapping orbit of Q;*
(c) *P lies in a non-overlapping orbit of Q^{op}.*

Then P is a subquasigroup of Q.

Proof. Since $Q = \{eR(q) \mid q \in Q\}$, there is a subset S of Q with $P = \{eR(s) \mid s \in S\}$ and $|S| = |P|$. Note that $P = SL(e)$, so $S = PL(e)^{-1}$ lies in the non-overlapping orbit of P in Q. Furthermore, $eR(e) = e \in P$, so $e \in S$ and $S = P$. Thus $P = PL(e)^{-1}$: For a given element p_2 of P, there is an element p_3 of P with $p_2 = p_3L(e)^{-1} = e\backslash p_3$.

Now $p_3 = eR(e\backslash p_3) \in PR(e\backslash p_3) \cap P$. Since $PR(e\backslash p_3)$ lies in the non-overlapping orbit of P in Q^{op}, the equality $P = PR(e\backslash p_3) = PR(p_2)$ holds. Thus for given elements p_1 and p_2 of P, one has $p_1p_2 \in PR(p_2) = P$. Since Q is finite, it follows that P is a subquasigroup of Q. □

Corollary 7.2. *Let e be an idempotent element of a finite quasigroup Q. Suppose that a subset P of Q satisfies the following conditions:*

(a) *$e \in P$;*
(b) *P lies in a non-overlapping orbit of Q;*
(c) *P is invariant under an isomorphism of Q with Q^{op}.*

Then P is a subquasigroup of Q.

Proof. An isomorphism of quasigroups induces an isomorphism of their left multiplication groups, and a similarity of the respective actions of these left multiplication groups on sets of subsets of given order. □

Corollary 7.3. *Suppose that e is an idempotent element of a finite, commutative quasigroup Q.*

(a) *If a subset P of Q contains e, and lies in a non-overlapping orbit of Q, then it is a subquasigroup of Q.*
(b) *Each non-overlapping orbit of Q contains a normal subquasigroup of Q.*

Proof. (a): Since Q is commutative, each non-overlapping orbit of Q is also a non-overlapping orbit of Q^{op}.

(b): In a non-overlapping orbit of Q, let P be the member that contains the idempotent element e of Q. By (a), P is a subquasigroup of Q. Corollary 5.8 then shows that P is a normal subquasigroup of Q. □

In Theorem 7.1 and Corollary 7.2, the respective conditions (c) are essential.

Example 7.4. Consider the quasigroup Q with multiplication table

(7.1)

Q	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	3	2	1	0
3	2	3	0	1

and idempotent element 0. Although the subset $P = \{0, 2\}$ satisfies the conditions (a) and (b) of Theorem 7.1 and Corollary 7.2, it is not a subquasigroup.

The necessity of condition (a) in Theorem 7.1 is demonstrated by the following.

Example 7.5. Let Q be the set of integers modulo 6, equipped with the commutative quasigroup product $x \circ y = 4 - x - y$. Then $yL_\circ(x) = y(-1) + (4 - x)$, so $\operatorname{LMlt} Q$ is the split extension of $(\mathbb{Z}/_6, +)$ with $\{\pm 1\}$. The unique non-overlapping orbit $\big\{\{0, 3\}, \{1, 4\}, \{2, 5\}\big\}$ on subsets of size 2 does not contain a subquasigroup.

8. Classifying divisors

Non-overlapping orbits provide the basis for a classification of the divisors of the order of a non-trivial finite quasigroup.

Definition 8.1. Let d be a positive integer, and let Q be a quasigroup whose (finite) order is a multiple of d. Consider the action of $\operatorname{LMlt} Q$ on the set $\binom{Q}{d}$ of subsets of Q of size d. For the quasigroup Q, the integer d is said to have ...

- ... *type J* if at least one non-overlapping orbit exists;
- ... *type I* if the action has at least one non-overlapping orbit which contains a subquasigroup of Q;
- ... *type H* if the action has non-overlapping orbits, each of which contains a subquasigroup of Q;
- ... *type G* if it has type H, and if each subquasigroup in a non-overlapping orbit is (right) Lagrangean.

Remark 8.2 (Informal mnemonics for the types of Definition 8.1)**.** If Q is a Group, then each prime power dividing $|Q|$ has type G (cf. [22, Prop. 10.51]). For type H, it is required that eacH non-overlapping orbit contain a subquasigroup. For type I, it is sufficient for I (Roman numeral!) non-overlapping orbit to contain a subquasigroup. Alternatively, 1 has type I for Q if and only if Q contains an Idempotent element (compare Example 8.4 below). For type J, one Just requires a non-overlapping orbit.

A series of examples serves to separate the types of Definition 8.1.

Example 8.3 (Divisors not of type J)**.** For a simple commutative quasigroup Q, Corollary 7.3(b) shows that no proper divisor of the order $|Q|$ may have type J for Q. As a concrete instance, one may consider the quasigroup Q with multiplication table

(8.1)

Q	0	1	2	3
0	0	2	3	1
1	2	0	1	3
2	3	1	0	2
3	1	3	2	0

and idempotent element 0. Since the stabilizer of 0 in the multiplication group of Q includes the 3-cycle $L(0) = (1\ 2\ 3)$, the multiplication group action is doubly transitive. While this certainly ensures that Q is simple, it also shows directly that 2 does not have type J for Q, since $\mathrm{Mlt}\, Q = \mathrm{LMlt}\, Q$ acts transitively on $\binom{Q}{2}$.

Example 8.4 (A divisor of type J, but not I)**.** The integer 1 has type J for any finite quasigroup Q. It has type I if and only if Q contains an idempotent element.

Example 8.5 (A divisor of type I, but not H)**.** Consider the quasigroup Q of (7.1). The non-overlapping orbit $\big\{\{0,1\},\{2,3\}\big\}$ contains the subquasigroup $\{0,1\}$, while the non-overlapping orbits $\big\{\{0,2\},\{1,3\}\big\}$ and $\big\{\{0,3\},\{1,2\}\big\}$ contain no subquasigroup. Thus 2 has type I, but not type H.

Example 8.6 (A divisor of type H, but not G)**.** Consider the quasigroup $Q = (\mathbb{Z}/_3, -)$ of integers modulo 3 under subtraction, with unique idempotent element 0. As noted in Example 8.4, 1 has type I for Q. It also has type H, since there is a unique (non-overlapping) orbit. However, since $\mathrm{LMlt}_Q\{0\}$ has orbits $\{0\}$ and $\{1,2\}$ on Q, the subquasigroup $\{0\}$ is not (right) Lagrangean, so 1 does not have type G.

Example 8.7 (Divisors of type G)**.** Proposition 5.1 shows that if Q is a group with subgroup P, then $|P|$ has type G for Q. For non-associative examples, consider a subquasigroup P of a quasigroup Q, with $0 < |P| = |Q|/2$. Note that P is a congruence class of the kernel of a surjective homomorphism from Q to a 2-element group. Then $|P|$ has type G for Q (compare Corollary 5.4 and [21, §4.6, Exer. 3]).

There are structural implications to the existence of divisors of type G for a given quasigroup Q.

Theorem 8.8. *Suppose that Q is a finite quasigroup of order dm, and that d has type G for Q. Then in the action of $\mathrm{LMlt}\, Q$ on $\binom{Q}{d}$, each non-overlapping orbit contains a unique subquasigroup of Q.*

Proof. Since d has type G, each non-overlapping orbit contains a right Lagrangean subquasigroup P. Let the orbit of P under the action of $\mathrm{LMlt}\, Q$ on $\binom{Q}{d}$ be $\{P\lambda_i \mid 1 \leq i \leq m\}$, with each λ_i in $\mathrm{LMlt}\, Q$ and $\lambda_1 = 1$.

Suppose that $P\lambda_h$ is a subquasigroup, for some index $1 < h \leq m$. Consider an element y of $P\lambda_h$. Then $x \cdot y = y$ for $x = y/y$ in $P\lambda_h$. On the other hand, since P is right Lagrangean, $(P\lambda_h)\mathrm{LMlt}_Q P = P\lambda_h$, so $\{yL(p) \mid p \in P\} = P\lambda_h$. Now $y \in P\lambda_h$, so there is an element p of P with $p \cdot y = y$. Then $p = y/y \in P \cap P\lambda_h$ contradicts the fact that the orbit of P is non-overlapping. □

Note that the statement of the following corollary (which may also be proved directly) makes no mention of Sylow theory.

Corollary 8.9. *Suppose that a finite quasigroup Q has more than one singleton subquasigroup. Then none of those singleton subquasigroups is (either right or left) Lagrangean.*

Proof. Consider an idempotent element x of Q. If the singleton subquasigroup $\{x\}$ was right Lagrangean, the integer 1 would have type G for Q. Theorem 8.8 would then imply that x was the only idempotent element of Q. Applying the same argument to the opposite of Q shows that $\{x\}$ cannot be left Lagrangean either. □

9. Diassociative loops

Recall that a *loop* is a quasigroup Q with an (*identity*) element 1 such that $1x = x = x1$ for all x in Q. A loop is *diassociative* if for each pair x, y of elements of Q, the subloop $\langle x, y\rangle$ of Q generated by x and y is associative. A loop Q is said to be a (*left*) *Bol loop* if

$$L(x)L(y)L(x) = L(x \cdot yx) \tag{9.1}$$

for all elements x and y of Q. *Right Bol loops* are defined dually. A loop is a *Moufang loop* if and only if it is both a left and a right Bol loop. Moufang's Theorem states that each Moufang loop is diassociative [3, §VII.4].

The goal of this brief section is to exhibit divisors that are not of type J for certain diassociative loops, and in particular for simple, nonassociative Moufang loops.

Lemma 9.1. *Let Q be a diassociative loop.*

(a) *Each element x of Q has an inverse x^{-1} with $L(x^{-1}) = L(x)^{-1}$.*
(b) *The inversion map*

$$Q \to Q^{\mathsf{op}}; x \mapsto x^{-1} \tag{9.2}$$

is an isomorphism of Q with Q^{op}.

Proof. (a): Each element x of Q has an inverse x^{-1} in the group $\langle 1, x\rangle$. Then for each element y of Q, one has $x^{-1}(xy) = y = x\,(x^{-1}y)$ in the group $\langle x, y\rangle$.

(b): For elements x and y of Q, the equation $(xy)^{-1} = y^{-1}x^{-1}$ holds in the subgroup $\langle x, y\rangle$ of Q generated by x and y, so the inversion (9.2) is a homomorphism. Furthermore, $(x^{-1})^{-1} = x$, so the inversion, being involutory, is bijective. □

Theorem 9.2. *Let Q be a finite, diassociative loop. For a divisor d of $|Q|$, suppose that there is no subloop of order d. Then d does not have type J for Q.*

Proof. Consider an orbit of the action of $\mathrm{LMlt}(Q)$ on $\binom{Q}{d}$. It must be shown that the orbit is overlapping. Let P be a member of the orbit that contains the identity element 1 of the loop Q.

If $P \neq P^{-1}$, say $x^{-1} \notin P$ for an element x of P, then

$$x^{-1} = 1L(x)^{-1} \in PL(x)^{-1} \neq P$$

but

$$1 = xL(x)^{-1} \in P \cap PL(x)^{-1}\,,$$

so the orbit of P is overlapping.

Otherwise, P is invariant under the inversion isomorphism (9.2) of Q with Q^{op}. Since there are no subloops of order d, Corollary 7.2 then implies that the orbit of P is overlapping. □

Let q be a non-trivial prime power. The set of elements of norm 1 in the split octonion algebra over the q-element field forms a diassociative loop under multiplication, and the quotient of that loop by the central scalar subloop $\{\pm 1\}$ forms a simple, non-associative

Moufang loop known as the *Paige loop* $\mathsf{PSL}_{1,3}(q)$ (compare [4, 18], [21, §1.7]). Suppose that p is an odd prime divisor of q^2+1. Note that p is congruent to 1 modulo 4 (and conversely, for each such p, there is a prime power q for which q^2+1 is a multiple of p) [4, Lemma 2.1]. Then p is also a divisor of $|\mathsf{PSL}_{1,3}(q)| = q^3(q^4-1)/\gcd\{q+1,2\}$.

Corollary 9.3. *Let p be an odd prime number that divides q^2+1 for a prime power q. Then in the Paige loop $\mathsf{PSL}_{1,3}(q)$, no non-trivial power of p dividing $|\mathsf{PSL}_{1,3}(q)|$ has type J.*

Proof. The Paige loop $\mathsf{PSL}_{1,3}(q)$ has no subloop whose order is a non-trivial power of p [4, Cor. 2.5]. □

10. Sylow subquasigroups

As a starting point for the top-down approach to Sylow theory, homogeneous spaces are used to formulate the definition of a (left) Sylow subquasigroup of a left quasigroup. (Dually, one may define right Sylow subquasigroups of right quasigroups.)

Definition 10.1. Let Q be a finite left quasigroup, and let p be a prime number. A subset P of Q is said to be a (*left*) *Sylow p-subquasigroup* of Q if

(a) P is a subquasigroup of Q;
(b) $|P|$ is a power of p;
(c) $|P\backslash Q|$ is coprime to p;
(d) $|P| \cdot |P\backslash Q| = |Q|$.

Remark 10.2. Earlier approaches to the extension of Sylow theory for groups (compare [4] – [8], [10], [24]) have disregarded the permutation-theoretical aspect, essentially using $|Q|/|P|$ as a substitute for $|P\backslash Q|$ in Definition 10.1, and rendering condition (d) redundant.

Example 10.3. Let P be a subquasigroup of a finite left quasigroup Q.

(a) If P is empty, then Definition 10.1(b) means that P cannot be a Sylow p-subquasigroup for any prime p.
(b) If Q is a group, and P is non-empty, then P is a Sylow p-subgroup of Q if and only if P is a Sylow p-subquasigroup of Q.
(c) Let Q be a projection left quasigroup, with $|P| > 1$. Then since $|P\backslash Q| = |Q|$, Definition 10.1(d) implies that P cannot be a Sylow p-subquasigroup for any prime p.

(d) Let Q be a projection left quasigroup, with $|P| = 1$. Then by Definition 10.1(c), P is a Sylow p-subquasigroup of Q if and only if p is not a divisor of $|Q| = |P\backslash Q|$.

The following proposition relates Definition 10.1 to the permutation-theoretic concept of a right Lagrangean subquasigroup.

Proposition 10.4. *Let Q be a quasigroup of order $p^r \cdot m$, for a prime number p with m coprime to p. Let P be a subquasigroup of order p^r. Then the following conditions are equivalent:*

(a) *P is a Sylow p-subquasigroup of Q;*
(b) *$|P\backslash Q| = |Q|/|P|$;*
(c) *P is right Lagrangean in Q.*

Proof. The equivalence of (b) and (c) is well known [21, Exercise 4.9]. Condition (b) of the proposition is a restatement of Definition 10.1(d) when P is nonempty, and also implies that $|P\backslash Q| = m$ is coprime to p — condition (c) of Definition 10.1 — under the assumptions of the proposition. □

Corollary 10.5. *There are no Sylow 2-subquasigroups in the Paige loop $\mathsf{PSL}_{1,3}(2)$ of order 120.*

Proof. The loop $\mathsf{PSL}_{1,3}(2)$ of order $120 = 2^3 \cdot 15$ does contain subloops of order 8, which are elementary abelian groups. However, a GAP [9] calculation performed by K.W. Johnson shows that these subloops are not Lagrangean. □

The following proposition establishes the basic relationship between Definition 10.1 and the classification of the divisors of the order of a finite quasigroup given in Definition 8.1.

Proposition 10.6. *Let Q be a quasigroup of order $p^r \cdot m$, for a prime number p with m coprime to p. Suppose that the divisor p^r of $|Q|$ has type G in the classification of Definition 8.1. Then Q contains at least one Sylow p-subquasigroup.*

Proof. Since the divisor p^r has type G, the action of $\mathrm{LMlt}\, Q$ on the set $\binom{Q}{p^r}$ of p^r-element subsets of Q has non-overlapping orbits, each of which contains a right Lagrangean subquasigroup P of Q. Then by Proposition 10.4, P is a Sylow p-subquasigroup of Q. □

11. Cyclic subgroups

An associative subloop P of a loop Q is often described as a *subgroup* of that loop. If Q is finite, and the size $|P|$ of the subgroup P is a power

of a prime number p, then P is said to be a *p-subgroup* of Q. Each element x of a Bol loop Q generates a cyclic subgroup of Q. Moreover, for each element x of a left Bol loop Q, induction on $|r|$ from (9.1) shows that

$$L(x^r) = L(x)^r \tag{11.1}$$

for each integer r [23, §I.4.2].

The following two results provide instances in which cyclic subgroups of loops become Lagrangean. Lagrangean subloops of Bol loops were treated earlier in [14, §7.1], [15, §5].

Proposition 11.1. *Suppose that P is a cyclic subgroup of a finite left Bol loop Q. Then P is right Lagrangean.*

Proof. Let P be generated by an element x, say $P = \{x^i \mid 0 \leq i < p\}$ for $p = |P|$. Consider an element y of Q. By (11.1), one has $\mathrm{LMlt}_Q(P) = \{L(x)^i \mid 0 \leq i < p\}$. Then $y\mathrm{LMlt}_Q(P) = \{yL(x)^i \mid 0 \leq i < p\}$ and $|y\mathrm{LMlt}_Q(P)| = p = |P|$, so P is right Lagrangean. □

Corollary 11.2. *Let P be a cyclic subgroup of a finite loop Q.*

(a) *If Q is a right Bol loop, then P is left Lagrangean.*
(b) *If Q is a Moufang loop, then P is Lagrangean.*

Corollary 11.2(b) may also be derived from the following.

Proposition 11.3. *Let P be a cyclic subgroup of a finite diassociative loop Q. Then P is (both right and left) Lagrangean.*

Proof. Suppose that P is generated by an element x. If $P = Q$, the result is immediate. Otherwise, let y be an element of Q that does not lie in P. Let G be the subgroup of Q generated by x and y. Then $y\mathrm{LMlt}_Q(P) = y\mathrm{LMlt}_G(P)$, and $|y\mathrm{LMlt}_G(P)| = |P|$ in the group G. It follows that P is right Lagrangean. Since diassociativity is a self-dual concept, P is also left Lagrangean. □

Cyclic subgroups of diassociative loops feature in the following counting theorem, an analogue of a result of Bruck for the case of nilpotent diassociative loops of odd prime-power order [3, Th. VI.3.2(a)].

Theorem 11.4. *Let Q be a finite diassociative loop. Let p be a prime divisor of $|Q|$. Suppose that P is a cyclic subgroup of Q which is a maximal p-subgroup of Q. Then the number of cyclic subgroups of Q of size $|P|$ is congruent to 1 modulo p.*

Proof. Let S be the set of cyclic subgroups of Q of size $|P|$. The group P acts on S by conjugation —

$$x : P' \mapsto P'T(x) = P'L(x)^{-1}R(x)$$

for $x \in P$ and $P' \in S$ — a process which takes place inside the subgroup $\langle P, P' \rangle$ of the diassociative loop Q generated by the cyclic groups P and P'. If P does not fix P', then the length of the orbit of P', the index of its proper stabilizer in the p-group P, is a multiple of p. Of course, the orbit of P itself is a singleton. Now suppose that P were to fix an element P' of S with $P' \neq P$, so that P' would be a normal subgroup of $\langle P, P' \rangle = PP'$. Then

$$|PP'| = |PP'/P'| \cdot |P'| = |P'/(P \cap P')| \cdot |P'| \,,$$

so PP' would be a p-subgroup of Q properly containing P, in contradiction to the maximality of P. Thus $|S| \equiv 1 \mod p$. □

Example 11.5. Let Q be the Paige loop $\mathsf{PSL}_{1,3}(2)$ of order $120 = 3 \cdot 40$. Then Q has exactly $28 = 3^3 + 1$ cyclic subgroups of order 3 (and no other 3-subgroups) [24, Lemma 5.13]. By Corollary 11.2(b), each of these cyclic subgroups is Lagrangean in Q. By Proposition 10.4, it follows that they are Sylow 3-subloops of Q.

12. Iterated function systems

If P is a subgroup of a group Q, then the group Q has a permutation representation on the homogeneous space (4.1) by the actions

$$R_{P\backslash Q}(q) : P\backslash Q \to P\backslash Q \,;\, Px \mapsto Pxq \tag{12.1}$$

for elements q of Q. Now let P be a subquasigroup of a left quasigroup Q. For each element q of the left quasigroup Q, consider the Markov chain with transition matrix $R_{P\backslash Q}(q)$ on the state space $P\backslash Q$, where the probability of transition from an orbit X to an orbit Y is given as

$$\big[R_{P\backslash Q}(q)\big]_{XY} = |X \cap R(q)^{-1}(Y)|/|X| \,. \tag{12.2}$$

If Q is a group, the transition matrix $R_{P\backslash Q}(q)$ is the permutation matrix given by the permutation action (12.1). With the uniform distribution on the left quasigroup Q, the quotient (12.2) becomes the conditional probability of the event $xq \in Y$ given $x \in X$. The set of convex combinations of the states from $P\backslash Q$ forms a complete metric space, and the actions $R_{P\backslash Q}(q)$ of the left quasigroup elements q form an iterated function system (IFS) in the sense of fractal geometry [1, 12].

Let Q be a finite set. Define a (*rational*) Q-IFS (X, Q) as a finite set X together with an *action map*

$$R\colon Q \to \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}X); q \mapsto R_X(q) \tag{12.3}$$

from Q to the set of endomorphisms of the rational vector space $\mathbb{Q}X$ with basis X (identified with their matrices with respect to the basis X), such that each *action matrix* $R_X(q)$ is stochastic. If P is a

subquasigroup of a finite non-empty left quasigroup Q, then the homogeneous space $P\backslash Q$ is a Q-IFS with the action map specified by (12.2). A *morphism* or (Q-)*homomorphism*

$$\phi\colon (X,Q) \to (Y,Q) \tag{12.4}$$

from a Q-IFS (X,Q) to a Q-IFS (Y,Q) is a function $\phi : X \to Y$, whose graph has incidence matrix F, such that the intertwining relation

$$R_X(q)F = FR_Y(q) \tag{12.5}$$

is satisfied for each element q of Q. It is readily checked that the class of morphisms (12.4), for a fixed finite set Q, forms a concrete category $\mathbf{IFS}_Q$. The following proposition serves to define homomorphic images.

Proposition 12.1. *Let $\phi\colon (X,Q) \to (Y,Q)$ be a Q-IFS homomorphism. Let $Z = X\phi$. Then the subspace $\mathbb{Q}Z$ of $\mathbb{Q}Y$ is invariant under the set $\{R_Y(q) \mid q \in Q\}$ of actions in (Y,Q).*

Proof. Consider an element z of Z, say $z = x\phi$ for $x \in X$, and an element q of Q. Suppose $xR_X(q) = \sum_{t\in X} r_t t$ for rational numbers r_t. Then (12.5) implies $zR_Y(q) = x\phi R_Y(q) = xFR_Y(q) = xR_X(q)F = \left(\sum_{t\in X} r_t t\right) F = \sum_{t\in X} r_t(tF) = \sum_{t\in X} r_t(t\phi) \in \mathbb{Q}Z$. □

Definition 12.2. In the context of Proposition 12.1, the Q-IFS (Z,Q) with action map $R\colon Q \to \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}Z); q \mapsto R_Y(q)\big|_{\mathbb{Q}Z}$ is known as:

(a) the *homomorphic image* of (the Q-IFS (X,Q) under) the Q-IFS homomorphism $\phi\colon (X,Q) \to (Y,Q)$, and as
(b) a *sub-Q-IFS* of the Q-IFS (Y,Q).

Group permutation representations appear in the IFS context as follows [21, Prop. 5.1].

Proposition 12.3. *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* (12.3) *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 $\mathbf{IFS}_Q$.*

Now let Q be a finite left quasigroup. Recall that for each subquasigroup P of Q, the homogeneous space $P\backslash Q$ is a Q-IFS with the action map specified by (12.2). In particular, the *regular space* is $\varnothing\backslash Q$. A Q-IFS is said to be a *basic Q-set* if it is a homomorphic image of a homogeneous space $P\backslash Q$ for a subquasigroup P of Q — compare Definition 12.2(a). Each basic Q-set is *irreducible* in the sense that it has no proper, non-empty subobjects [20, Cor. 8.2]. A Q-IFS is said to be

a (*finite*) Q-*set* if it is a finite sum of basic Q-sets. A finite Q-set (Z, Q) is said to be a Q-*subset* or *sub-*Q-*set* of a finite Q-set (Y, Q) if (Z, Q) is a sub-Q-IFS of (Y, Q) — compare Definition 12.2(b). The *category* $\underline{\underline{Q}}_{\mathrm{fin}}$ *of finite* Q-*sets* is the full subcategory of $\mathbf{IFS}_Q$ induced on the class of finite Q-sets. (Note that the alternative definitions here agree with the earlier definitions of [20, 21] — compare [21, Th. 5.4].)

13. Burnside orders

For a finite Q-set X, let $[X]$ denote its isomorphism type within the category $\underline{\underline{Q}}_{\mathrm{fin}}$. Let B be the set of so-called *basic* types, the isomorphism types of basic Q-sets. In particular, the *regular type* is $[\varnothing\backslash Q]$. Let $\underline{\underline{J}}$ be the full subcategory of $\underline{\underline{Q}}_{\mathrm{fin}}$ induced on the class of basic Q-sets. Define a new category $\widetilde{\underline{\underline{J}}}$ on the object class $\underline{\underline{J}}_0$ of $\underline{\underline{J}}$ by setting

$$\left|\widetilde{\underline{\underline{J}}}(X,Y)\right| = \begin{cases} 1 & \text{if } \underline{\underline{Q}}_{\mathrm{fin}}(X,Y) \neq \varnothing; \\ 0 & \text{otherwise.} \end{cases}$$

Then $\widetilde{\underline{\underline{J}}}$ is a pre-ordered class. It induces an order structure $(B, \sqsubseteq)$ on the set B (compare [23, I, Ex. 1.3H]) given explicitly by

$$[X] \sqsubseteq [Y] \quad \Leftrightarrow \quad \underline{\underline{Q}}_{\mathrm{fin}}(X,Y) \neq \varnothing\,. \tag{13.1}$$

(Antisymmetry follows from the fact that basic Q-sets are irreducible.)

Definition 13.1. The partially ordered set $(B, \sqsubseteq)$ of (13.1) is called the *Burnside order* of the left quasigroup Q.

Example 13.2. Let Q be a group. By Proposition 12.3, the left quasigroup actions of Q coincide with the (right) group actions of Q. The set B of basic types $[P\backslash Q]$ may be identified as the set of conjugacy classes P^Q of subgroups P of Q. Then the Burnside order of Q is given by

$$P_1^Q \sqsubseteq P_2^Q \quad \Leftrightarrow \quad \exists\, q \in Q\,.\, P_1^q \subseteq P_2\,,$$

i.e., by containment of subgroups within the conjugacy classes. The partial order $\sqsubseteq$ is written as $\subseteq_Q$ in the notation of [2].

The Burnside order provides a framework for certain aspects of Sylow theory. Let Q be a finite left quasigroup. Since Q-set isomorphisms are set isomorphisms, the function

$$h\colon B \to \mathbb{N}; [X] \mapsto |X|$$

is well-defined. Note that the regular type is the only basic type b with $b^h = |Q|$. Consider the function

$$k\colon B \to 2^{\mathbb{N}}; b \mapsto \left\{ |P| \;\middle|\; b = [P\backslash Q] \text{ for a subquasigroup } P \text{ of } Q \right\}.$$

Definition 13.3. Let Q be a finite left quasigroup. Then the structure $(B, \sqsubseteq, h, k)$ is known as the *labeled Burnside order* of Q.

Definition 13.4. Let Q be a finite left quasigroup, and let p be a prime number. A basic type s of Q is said to be a *Sylow p-type* of Q if

(a) s^h is coprime to p, and
(b) $\exists\, r \in \mathbb{N}\,.\; p^r \in s^k$ and $|Q| = s^h \cdot p^r$.

Isomorphism types of homogeneous spaces of Sylow p-subquasigroups are certainly Sylow p-types:

Proposition 13.5. *Let P be a Sylow p-subquasigroup of a finite left quasigroup Q for a prime number p. Then the basic type $[P\backslash Q]$ is a Sylow p-type of Q.*

Proof. Suppose that $|P| = p^r$. Then $[P\backslash Q]^h = |P\backslash Q|$ is coprime to p, and $p^r \in [P\backslash Q]^k$ with $|Q| = [P\backslash Q]^h \cdot p^r$. □

Corollary 13.6. *Let Q be a finite, non-empty set, considered as a projection left quasigroup. Let p be a prime that does not divide $|Q|$. Then the regular type is a Sylow p-type.*

Proof. Let S be a singleton subset of Q. Since $\mathrm{LMlt}_Q S$ is trivial, the basic type $[S\backslash Q]$ is regular. As in Example 10.3(d), S is a Sylow p-subquasigroup of Q. Proposition 13.5 then shows that $[S\backslash Q]$ is a Sylow p-type. □

For non-empty subquasigroups of finite quasigroups, the converse of Proposition 13.5 holds.

Proposition 13.7. *Let P be a non-empty subquasigroup of a finite quasigroup Q. If the basic type $[P\backslash Q]$ is a Sylow p-type of Q for a prime number p, then P is a Sylow p-subquasigroup Q.*

Proof. Condition (a) of Definition 10.1 is immediate. The coprimality of $|P\backslash Q| = [P\backslash Q]^h$ to p yields condition (c). By Definition 13.4(b), there is a subquasigroup P' of Q, of p-power order p^r, with $[P'\backslash Q] = [P\backslash Q]$ and $|Q| = |P\backslash Q| \cdot p^r$. In particular, Proposition 10.4 shows that P' is right Lagrangean in Q. Since $[P'\backslash Q] = [P\backslash Q]$ and P is non-empty, it follows that P is also right Lagrangean in Q. Thus $|P| = |Q|/|P\backslash Q| = p^r$, yielding the remaining conditions (b) and (d) of Definition 10.1. □

For non-empty subquasigroups of finite left quasigroups, the converse of Proposition 13.5 may fail.

Example 13.8. Let Q be a 2-element set, with a singleton subset S. Consider Q as a projection left quasigroup. Let $p = 3$ and $P = Q$. The triviality of the group $\mathrm{LMlt}\, Q$ implies that $\varnothing\backslash Q = P\backslash Q$. By Corollary 13.6, $P\backslash Q$ is a Sylow 3-type of Q. However, as noted in Example 10.3(c), P is not a Sylow 3-subquasigroup of Q.

The following two definitions are designed to capture the respective conjugacy and maximality of Sylow subgroups of finite groups within the left quasigroup context.

Definition 13.9. Let Q be a finite left quasigroup. A prime number p is said to be:

(a) *Sylowian* for Q if Q has a unique Sylow p-type;
(b) *strongly Sylowian* for Q if it is Sylowian, say with unique Sylow p-type s, and if for each basic type b with $s^h | b^h$, one has $b \sqsubseteq s$.

By Sylow's Theorem [22, Th. 10.56], each prime is strongly Sylowian for each finite group (compare Example 13.2).

Example 13.10. The prime number 3 is strongly Sylowian for the Paige loop $\mathsf{PSL}_{1,3}(2)$ of order 120.

Proposition 13.11. *Let Q be a finite set, considered as a projection left quasigroup. Let p be a prime that does not divide $|Q|$. Then p is strongly Sylowian for Q.*

Proof. By Corollary 13.6, the regular type is a Sylow p-type. Now if s is a Sylow p-type, Definition 13.4(b) shows that $s = [S\backslash Q]$ with $|S| = 1$, and since $\mathrm{LMlt}_Q S$ is trivial, it follows that s is the regular type. Thus p is Sylowian. Finally, if b is a basic type with $s^h | b^h$, then $|Q| = s^h \leq b^h \leq |Q|$ implies $b^h = |Q|$, so $b = s$. Thus p is strongly Sylowian. □

Acknowledgement

I am grateful to K.W. Johnson for information concerning the history of Sylow's Theorem, and to anonymous referees for helpful comments on an earlier version of this paper.

References

[1] M.F. Barnsley, *Fractals Everywhere*, Academic Press, San Diego, CA, 1988.
[2] S. Bouc, "Burnside rings," pp. 739–804 in M. Hazewinkel (ed.), *Handbook of Algebra, vol. 2*, North-Holland, Amsterdam, 2000.

[3] R.H. Bruck. *A Survey of Binary Systems*, Springer, Berlin, 1958.
[4] S.M. Gagola III, "The existence of Sylow 2-subloops in finite Moufang loops," *J. Algebra* **322** (2009), 1029–1037.
[5] S.M. Gagola III, "The development of Sylow p-subloops in finite Moufang loops," *J. Algebra* **322** (2009), 1565–1574.
[6] S.M. Gagola III, "Conjugacy of Sylow 2-subloops of the Chein loops $M_{2n}(G, 2)$," *Comm. Algebra* **37** (2009), 2804–2810.
[7] S.M. Gagola III, "The number of Sylow p-subloops in finite Moufang loops," *Comm. Algebra* **38** (2010), 1436–1448.
[8] S.M. Gagola III, "The conjugacy of triality subgroups of Sylow subloops of Moufang loops," *J. Group Theory* **13** (2010), 821–840.
[9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008. `http://www.gap-system.org`
[10] A. Grishkov and A. Zavaritsine, "Sylow's theorem for Moufang loops," *J. Algebra* **321** (2009), 1813–1825.
[11] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
[12] J.E. Hutchinson, "Fractals and self similarity," *Indiana Univ. Math. J.* **30** (1981), 713–747
[13] J. Ježek, "Normal subsets of quasigroups," *Comment. Math. Univ. Carol.* **16** (1975), 77–85.
[14] K.W. Johnson and J.D.H. Smith, "On the smallest simple, unipotent Bol loop," *J. Combin. Theory Ser. A* **117** (2010), 790–798.
[15] K.W. Johnson and J.D.H. Smith, "Matched pairs, permutation representations, and the Bol property," *Comm. Alg.* **38** (2010), 2903–2914.
[16] G.A. Miller, "Extensions of two theorems due to Cauchy," *Bull. Amer. Math. Soc.* **16** (1910), 510–513.
[17] G.A. Miller, "A new proof of Sylow's theorem," *Ann. of Math.* **16** (1915), 169–171.
[18] L.J. Paige, "A class of simple Moufang loops," *Proc. Amer. Math. Soc.* **7** (1956), 471–482.
[19] A.B. Romanowska and J.D.H. Smith, *Modes*, World Scientific, Singapore, 2002.
[20] J.D.H. Smith, "Permutation representations of left quasigroups," *Alg. Univ.* **55** (2006), 387–406.
[21] J.D.H. Smith, *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.
[22] J.D.H. Smith, *Introduction to Abstract Algebra*, Chapman and Hall/CRC, Boca Raton, FL, 2009.
[23] J.D.H. Smith and A.B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.
[24] P. Vojtěchovský, *Finite simple Moufang loops*, Ph.D. thesis, Iowa State University, 2001. Available online at
`http://www.math.du.edu/~petr/data/papers/finite_simple_Moufang_loops.pdf`
[25] H. Wielandt, "Ein Beweis für die Existenz von Sylowgruppen," *Arch. Math.* **10** (1959), 401–402.

Department of Mathematics, Iowa State University, Ames, Iowa 50011, U.S.A.

Email address: jdhsmith@iastate.edu

URL: http://www.math.iastate.edu/jdhsmith/