SYMMETRIC SETS WITH MIDPOINTS AND ALGEBRAICALLY EQUIVALENT THEORIES

JIMMIE LAWSON AND YONGDO LIM

Abstract. In this paper we consider an algebraic generalization of symmetric spaces of noncompact type to a more general class of symmetric structures equipped with midpoints. These symmetric structures are shown to have close relationships to and even categorical equivalences with a variety of other algebraic structures: transversal twisted subgroups of involutive groups, a special class of loops called B-loops, and gyrocommutative gyrogroups.

1. Introduction

The story of this paper began with the authors' investigation of the geometric mean of two positive definite matrices [13] and, more generally, of two members of the symmetric cone of a Euclidean Jordan algebra [15, 16]. These investigations motivated us to search for a general, yet elementary, axiomatic framework in which to develop the theory of a geometrical mean. Since all our examples consisted of symmetric spaces, we decided to develop the theory in the context of symmetric spaces.

The basic notion of a symmetric space is that of a space equipped with a "canonical reflection" S_x through each point x, called a symmetry. The symmetry S_x should be involutive, the point x should be an "isolated" fixed point, and the symmetries should preserve appropriate geometrical structure. In particular, in the presence of the existence of "midpoints," the symmetry that carries x to y should be the symmetry S_m through the midpoint m of x and y. This provides our general framework for the notion of a midpoint of points x and y in the context of symmetry: it is the point through which one reflects x to obtain y and vice-versa. The classical symmetric spaces of noncompact type admit such a theory of midpoints and illustrate our study.

Date: October 1, 2003.

We have adopted a modified version of the axiomatic approach of Loos [17, Chapter II] to symmetric spaces in which the axioms are given in terms of a binary operation $(x, y) \to x \bullet y$ on a set X. Closely related algebraic structures, called symmetric sets, were also studied by Nobusawa and his collaborators; see [20] and its references. We have replaced the fourth axiom of Loos, which asserts that fixed points of symmetries are topologically isolated, by an axiom that ensures the existence of a unique midpoint or mean between any two points. With this axiom one no longer needs the presence of a topology and thus the theory becomes purely algebraic, although our original motivation was heavily topological and geometric.

We were surprised to discover that extremely close ties, even categorical equivalences, existed between our structures and a variety of other algebraic structures: twisted subgroups (a generalization of subgroups), involutive groups, a special class of loops called B-loops, and gyrocommutative gyrogroups. The connection of symmetric spaces with involutive groups is well-established; indeed Helgason [6] develops the theory of Riemannian symmetric spaces in the context of Lie groups with involution. More recent work has made connections between twisted subgroups, involutive groups, and certain classes of loops; see for example, [10], [1], [3], [11]. In this paper we tie all of these together by making precise these connections for the specific class of symmetric sets that we have in mind. There appear to be some advantages of our approach to these various more-or-less equivalent structures: it provides a simpler axiom system and a more geometric viewpoint than the other frameworks.

In the second section we give the basic axioms and elementary properties of the algebraic systems we study: symmetric sets with midpoints, which we call dyadic symmetric sets or dyadic symsets for short. The most useful category of dyadic symsets for the purposes of this paper is the one with pointed objects and point-preserving homomorphisms.

The next section gives a basic geometric example, ruled symmetric spaces. In the fourth section we give a class of examples of fundamental importance for the theory: dyadic symsets that arise from twisted subgroups of groups.

In the fifth section we introduce the displacement or transvection group of a dyadic symmetric set. We define a quadratic representation of a dyadic symset into its displacement group that is reminiscent of the quadratic representation in the theory of

Jordan algebras. The image of the quadratic representation turns out to be a twisted subgroup with unique square roots, and thus this embedding machinery allows us to represent an abstract dyadic symset as one arising in a canonical fashion from a twisted subgroup of a group.

The assignment of the displacement group to a dyadic symset is not functorial: it does not extend to the morphism level. To enhance the possibility of converting questions and problems about symsets to the group setting and thus to gain access to the powerful methods of group theory, we take some effort in the sixth and seventh section to develop a functorial representation of the category of pointed dyadic symsets in the category of involutive groups, particularly those admitting a polar decomposition. To this end we develop the concept of the universal twisted representation.

In the eighth section we introduce a special type of loop (a non-associative group) called a B-loop and establish an equivalence of categories between the category of pointed dyadic symsets and point-preserving homomorphisms and the category of B-loops and homomorphisms. At the level of the grounding functor to sets, this equivalence is the identity. These results can be reformulated for uniquely 2-divisible gyrocommutative gyrogroups, a class of loops that has recently been shown to be equivalent to K-loops. Gyrogroups were introduced as appropriate objects for the study of Einstein velocity addition in special relativity ([22] and [23]).

2. Symmetric sets with midpoints

We consider binary systems $(X, \bullet)$ for which $S_x : X \to X$ defined by $S_x(y) = x \bullet y$ may be viewed as a symmetry or reflection through x. We write $S_x y$ for $S_x(y)$. Note that S_x is left translation by x with respect to the binary operation; it would thus make sense to denote it by L_x or λ_x, but we adopt the notation S_x as connotative of a symmetry.

More formally, we begin with a *binary system* $(X, \bullet)$, a set endowed with a binary operation $(x, y) \mapsto x \bullet y : X \times X \to X$ (these are sometimes called groupoids or magmas). For each x, we have the *symmetry* S_x defined by $S_x y = x \bullet y$. We list our fundamental axioms with equivalent alternative formulations in terms of the symmetries S_x in parentheses.

Definition 2.1. A *symmetric set*, or *symset* for short, consists of a binary system $(X, \bullet)$ satisfying for all $a, b, c \in X$ the first three of the following list of axioms:

(1) $a \bullet a = a$ ($S_a a = a$);
(2) $a \bullet (a \bullet b) = b$ ($S_a S_a = \mathrm{id}_X$);
(3) $a \bullet (b \bullet c) = (a \bullet b) \bullet (a \bullet c)$ ($S_a S_b = S_{S_a b} S_a$);
(4*) the equation $x \bullet a = b$ ($S_x a = b$) has a solution $x \in X$.
(4) the equation $x \bullet a = b$ ($S_x a = b$) has a unique solution $x \in X$, called the *midpoint* or *mean* of a and b, and denoted $a\#b$.

If the binary system $(X, \bullet)$ satisfies the first three axioms and Axiom (4*), then X is called a *homogeneous symset*, and if it satisfies the first three axioms together with Axiom (4), then it is called a *dyadic symset*.

Property (1) is sometimes referred to as the idempotent property, property (2) as the left key property and property (3) as the left distributive property. Note that property (4*) resp. (4) is equivalent to the requirement that right translations are surjective resp. bijective.

Remark 2.2. The adjective "dyadic" refers to the ability to find midpoints and their iterates. The dyadic nature of such structures will become clear as the paper unfolds.

Symmetric sets (satisfying the first three axioms) and homogeneous symsets were introduced in the work of Nobusawa and his collaborators; see [19], [9], and [20] and their references. These works primarily consider finite symsets, in which case Axioms (4*) and (4) coincide. Since the pioneering work of Joyce [7] binary systems $(X, \bullet)$ satisfying the first three axioms of Definition 2.1 have become quite prevalent in knot theory, where they are referred to as *involutory quandles*. (For *quandles* in general, Axiom (2) is weakened to require only that S_a be bijective; such structures are called *pseudo-symmetric sets* by Nobusawa.) We are unaware of any focused study of our Axiom (4).

Recall that a function $f : X \to Y$ between magmas is a *homomorphism* if $f(u \bullet v) = f(u) \bullet f(v)$ for all $u, v \in X$. Note that Axiom (2) is equivalent to the assertion that each S_a is involutive (hence bijective). Furthermore Axiom (3) is equivalent to the assertion that each S_a is a self-homomorphism; this becomes apparent when Axiom

(3) is written in the "mixed" form:

$$S_a(b \bullet c) = (S_a b) \bullet (S_a c).$$

Hence Axioms (2) and (3) together are equivalent to the assertion that each symmetry S_a is an involutive automorphism.

A *quasigroup* $(G, \bullet)$ consists of a binary system for which the equations $x \bullet a = b$ and $a \bullet y = b$ have unique solutions x and y in G. The next lemma establishes that dyadic symsets are quasigroups and gives an alternative characterization of dyadic symsets as a special class of quasigroups.

Lemma 2.3. *A set G endowed with a binary operation is a dyadic symset if and only if it is an idempotent quasigroup for which each left translation S_x is an involutive automorphism.*

Proof. Assume that $(X, \bullet)$ is a dyadic symset. Axiom (1) asserts idempotency, Axioms (2) and (3) are equivalent to the assertion that all S_x are involutive automorphisms, and Axiom (4) asserts the unique solution of $x \bullet a = b$. Since S_a is an automorphism, the equation $a \bullet y = S_a y = b$ has a unique solution. The converse follows even more directly. □

In verifying that specific examples satisfy the axioms, it is often helpful to have the axioms given in a weakened form. We are indebted to Karl-Hermann Neeb for suggesting a much more direct proof of the next observation.

Lemma 2.4. *Let $(X, \bullet)$ be a symset having a distinguished point ε satisfying for all $a, b, c \in X$:*

- (4^*_ε) *the equation $x \bullet \varepsilon = b$ has a solution $x \in X$; or*
- (4_ε) *the equation $x \bullet \varepsilon = b$ has a unique solution $x \in X$.*

Then $(X, \bullet)$ is a homogeneous resp. dyadic symset.

Proof. Let $a, b \in X$. By (4^*_ε) pick u such that $S_u \varepsilon = u \bullet \varepsilon = a$. By Axiom (2), S_u is involutive, and hence $\varepsilon = S_u a$. Pick x such that $x \bullet \varepsilon = S_u b$. Applying S_u to both sides, we have via Axiom (3) $S_u x \bullet S_u \varepsilon = S_u x \bullet a = b$. Thus $S_u x$ is a solution of $(\,) \bullet a = b$. If $y \bullet a = b$ were another, then applying S_u to both sides yields $S_u y \bullet \varepsilon = S_u b$, hence $S_u y = x$ if $(\ ) \bullet \varepsilon = S_u b$ has a unique solution, and therefore $y = S_u x$, which establishes uniqueness in general. □

Remark 2.5. Not only does the preceding lemma provide a weaker condition to verify, but it also suggests a concept that will be crucial for our further developments, that of a pointed symmetric set. The category of pointed symsets and point-preserving homomorphisms is both vital and suggestive for our later developments.

Definition 2.6. The category SYM of pointed symsets has pointed symsets as objects and homomorphisms preserving the distinguished points as morphisms. The categories HSYM of homogeneous symsets and DSYM of dyadic symsets are the obvious full subcategories. Products and subobjects are defined in the standard way.

The operation $(x, y) \to x\#y$ of taking the mean or midpoint in a dyadic symset is also a binary operation. There is a very close connection between the mean and the symmetric reflection given by

$$x \bullet y = z \quad \Leftrightarrow \quad x = y\#z.$$

This often allows one to use one or the other, whichever is more convenient.

Lemma 2.7. *A function is a homomorphism of dyadic symsets if and only if it is a #-homomorphism. Thus, in the presence of Axiom (4), Axiom (3) is equivalent to* $S_x(y\#z) = S_x y \# S_x z$ *for all* $x, y, z \in X$*, i.e., the symmetries preserve the midpoints.*

Proof. Using $x \bullet y = z$ if and only if $x = y\#z$, we have for $x = y\#z$, $f(x) \bullet f(y) = f(x \bullet y) = f(z)$, and thus $f(x) = f(y)\#f(z)$. Conversely if f is a #-homomorphism, then for $z = x \bullet y$, we have $x = y\#z$, and hence $f(x) = f(y)\#f(z)$. It follows that $f(x) \bullet f(y) = f(z)$.

The last assertion follows from what we have just done, since Axiom (3) is equivalent to S_x being a symset homomorphism, which we have just seen is equivalent to being a #-homomophism, and the proof depended only on Axiom 4. □

3. Symmetric topological spaces with midpoints

The class of symmetric spaces of noncompact type forms a key topological example of a class of dyadic symmetric sets. We present a more general topological class. Let

X be a Hausdorff space. We assume that X comes equipped with a *linear geodesic family* Γ, a family of homeomorphisms γ from the real line $\mathbb{R}$ onto a closed subset of X such that for each pair of distinct points $x, y \in X$, there exists $\gamma \in \Gamma$, unique up to linear parameterization, such that $x, y \in \gamma(\mathbb{R})$. (The uniqueness condition means that if $x, y \in \gamma_1(\mathbb{R}) \cap \gamma_2(\mathbb{R})$, then there exists $a, b \in \mathbb{R}$, $a \neq 0$, such that for all $t \in \mathbb{R}$, $\gamma_1(t) = \gamma_2(at + b)$.)

We define the *midpoint* or *mean* of x and y to be $\gamma((s+t)/2)$ if $\gamma \in \Gamma$ and $\gamma(s) = x$, $\gamma(t) = y$. This is well-defined by the uniqueness up to linear parameterization condition. For $m \in X$ we define the *point reflection* S_m by $S_m x = y$ if m is the midpoint of x and y. The point reflection S_m is called a *symmetry* if $S_x\gamma \in \Gamma$ for all $\gamma \in \Gamma$.

Lemma 3.1. *Let X be a Hausdorff family endowed with a geodesic family Γ. If each point reflection S_u, $u \in X$, is a symmetry, then X is a dyadic symmetric set.*

Proof. It is immediate that Axioms (1), (2), and (4) are valid. Suppose that m is the midpoint of x and y. Then there exists a geodesic $\gamma : \mathbb{R} \to X$ such that $\gamma(s) = x$, $\gamma(t) = y$, and $\gamma((s+t)/2) = m$. By hypothesis for $u \in X$, $\gamma_1 := S_u\gamma$ is a geodesic with $\gamma_1(s) = S_u x$, $\gamma_1(t) = S_u y$, and $\gamma_1((s+t)/2) = S_u m$. Hence $S_u m$ is the midpoint of x and y, i.e., S_u preserves midpoints. By Lemma 2.7 X is a dyadic symset. $\square$

Example 3.2. Let X be a differentiable manifold modeled on a Banach space, and equipped with a covariant derivative D arising from a spray. A D-*symmetry* is a diffeomorphism $S_x : X \to X$ that is a D-isomorphism, that leaves x fixed, and that has derivative $-\mathrm{id}$ on $T_x X$. The manifold X is called D-*symmetric* if it has a D-symmetry at every point, and if $\exp_x : T_x \to X$ is surjective for all $x \in X$ (see [12, Chapter XIII,5]). A D-symmetric manifold is geodesically complete and each D-symmetry preserves geodesics.

Let X be a D-symmetric manifold, let Γ be the family of geodesics, and let us assume additionally that $\exp_x : T_x X \to X$ is a diffeomorphism for each $x \in X$. Then the family Γ is a geodesic family in our earlier sense. Hence all the conditions of Lemma 3.1 are satisfied, and X is a dyadic symset.

The finite-dimensional Riemannian symmetric spaces of noncompact type are a special case of such D-symmetric manifolds.

4. Twisted subgroups

There are close connections between symsets and groups. In this section we begin this development and simultaneously construct important examples of symsets, particularly dyadic symsets.

The notion of a twisted subgroup appears explicitly in [1], although it is implicit at places in the work of Nobusawa and his group. The notion of a twisted subgroup also arises in several contexts in the theory of loops.

Definition 4.1. A *twisted subgroup* of a group G is a subset P of G containing the identity e such that (i) if $x, y \in P$, then $xyx \in P$, and (ii) if $x \in P$, then $x^{-1} \in P$. Alternatively one can replace (i) and (ii) with the equivalent condition that $xy^{-1}x \in P$ whenever $x, y \in P$.

For $x, y \in P$, a twisted subgroup, we define $x \bullet y := xy^{-1}x$. Then it is straightforward to verify that the binary system $(P, \bullet)$ satisfies the three axioms for a symset. For example, for Axiom (3):

$$x \bullet (y \bullet z) = x \bullet (yz^{-1}y) = xy^{-1}zy^{-1}x,$$

while

$$(x \bullet y) \bullet (x \bullet z) = (xy^{-1}x) \bullet (xz^{-1}x) = (xy^{-1}x)(x^{-1}zx^{-1})(xy^{-1}x) = xy^{-1}zy^{-1}x,$$

so that the two are equal.

Proposition 4.2. *Let P be a subset of a group G containing the identity e, and define $x\bullet y = xy^{-1}x$. Then $(P, \bullet)$ is a symset resp. homogeneous symset resp. dyadic symset if and only if P is a twisted subgroup resp. 2-divisible twisted subgroup resp. uniquely 2-divisible twisted subgroup. If $h : G_1 \to G_2$ is a group homomorphism carrying a twisted subgroup P_1 into a twisted subgroup P_2, then the restriction $h : (P_1, \bullet) \to (P_2, \bullet)$ is a homomorphism of symsets.*

Proof. We have already seen that if P is a twisted subgroup, then the three axioms of a symset are satisfied. Conversely assume that $(P, \bullet)$ is a symset. Then $x, y \in P$ implies $x \bullet y = xy^{-1}x \in P$. That P is a twisted subgroup follows from the alternative definition of a twisted subgroup.

Assume that P is a twisted subgroup. Then for $x, y \in P$, $x = y^2$ if and only if $y \bullet e = ye^{-1}y = y^2 = x$. Thus for $\varepsilon = e$, the identity of G, condition (4^*_ε) resp. condition (4_ε) of Lemma 2.4 is satisfied if and only if P is 2-divisible resp. uniquely 2-divisible. Hence the proposition follows from Lemma 2.4.

The last assertion of the proposition is immediate from the group homomorphism property and the definition of the symset operation. □

Example 4.3. Consider the additive dyadic group $(\mathbb{D}, +)$ of all fractions of the form $m/2^n$ for $m, n \in \mathbb{Z}$. Then each element $t \in \mathbb{D}$ has a unique square, namely $t/2$, and thus $\mathbb{D}$ itself is a uniquely 2-divisible twisted subgroup of itself. Hence by Proposition 4.2 $(\mathbb{D}, \bullet)$ is a dyadic symset with $t \bullet s = t - s + t = 2t - s$. The symmetries are given by $S_t s = 2t - s$. Also $t\#s = (1/2)t + (1/2)s$, since $(t\#s) \bullet t = s$. We call the dyadic symset $\mathbb{D}$ the *dyadic line.*

Lemma 4.4. *Let P be a twisted subgroup of a group G. If $x \in P$, then the cyclic subgroup generated by x is a subset of P. If P is additionally uniquely 2-divisible, then for each $x \in P$, there is a unique group homomorphism σ from the additive group $(\mathbb{D}, +)$ of dyadic rationals into G such that the image is contained in P and $\sigma(1) = x$.*

Proof. The first assertion is well-known (see, for example, [1]). However, for our purposes, it is instructive to give a proof from the symset point of view. For $x \in P$, we define $x^0 = e$, $x^1 = x$, inductively $x^{n+1} = x^n \bullet x^{n-1}$ for higher positive n, and $x^{-n} = e \bullet x^n$. These are all in the symset $(P, \bullet)$ and one easily sees that they agree with the usual powers in the group G.

In the case that P is uniquely 2-divisible, we define $x^{1/2} = e\#x$, which is the unique square root of x in P, and then recursively obtain $x^{1/2^n}$. We can then define a group homomophism σ from $\mathbb{D}$ into G by $\sigma(m/2^n) = (x^{1/2^n})^m = x^{m/2^n}$; elementary group theoretic arguments yield that it is a group homomorphism, and hence also a symset homomorphism (Proposition 4.2) □

Definition 4.5. The preceding proof suggests how powers should be defined in pointed symsets, namely $x^0 = \varepsilon$, $x^1 = x$, inductively $x^{n+1} = x^n \bullet x^{n-1}$ for positive integers n, and $x^{-n} = \varepsilon \bullet x^n$. If additionally the symset is dyadic, we define $x^{1/2} = \varepsilon\#x$, inductively $x^{1/2^{n+1}} = \varepsilon\#x^{1/2^n}$, and $x^{m/2^n} = (x^{1/2^n})^m$ for all dyadic rationals.

There are close connections between involutive groups and twisted subgroups.

Corollary 4.6. *Let G be a group equipped with an involutive antiautomorphism $x \mapsto x^*$. Then the set $P_G := \{xx^* : x \in G\}$ is a twisted subgroup, and hence is a homogeneous resp. dyadic symset under $x \bullet y = xy^{-1}x$ if and only if P is 2-divisible resp. uniquely 2-divisible.*

Proof. We observe that $e = ee^*$, $(xx^*)^{-1} = (x^{-1})^*(x^{-1})^{**}$, and $aba = xx^*y(xx^*y)^* \in P$ for $a = xx^*$, $b = yy^*$. Thus P is a twisted subgroup, and the remaining assertions follow directly from Proposition 4.2. □

Example 4.7. Let A be a C^*-algebra (see, for example [24, II.15] for basic definitions and properties). We consider the subset of strictly positive self-adjoint members of A, which is the set $P = \{x \in A : x = aa^* \text{ for some invertible } a \in A\}$. By the preceding corollary P is a twisted subgroup of the group of all invertible elements of A, and hence a symmetric set with respect to $x \bullet y = xy^{-1}x$. Also it is standard that members of P have unique strictly positive self-adjoint roots of all orders, so that $(P, \bullet)$ is a dyadic symset. These observations apply, in particular, to the C^*-algebra of bounded linear operators on a Hilbert space, in particular, to the matrix algebra over $\mathbb{R}^n$.

5. The displacement group and the quadratic representation

A basic tool in the study of symmetric sets and spaces is the quadratic representation into the group of displacements; see [17], [19], or [9].

Definition 5.1. Let (X, ε) be a pointed symset. Each composition S_xS_y is called a *displacement* or *transvection* and the group $G(X)$ generated by all S_xS_y, $x, y \in X$, is called the *group of displacements* or *transvection group*. The isotropy group at ε is denoted $K(X)$. The *quadratic representation* of X is the map $Q : X \to G(X)$ defined by $Q(x) = S_xS_\varepsilon$.

Remark 5.2. Since $Q(x)Q(y)^{-1} = (S_xS_\varepsilon)(S_\varepsilon S_y) = S_xS_y$ (since $(S_y)^{-1} = S_y$ by Axiom (2)), we have that $G(X)$ is alternatively the group generated by $Q(X)$.

The next lemma gives fundamental properties of the quadratic representation.

Lemma 5.3. *For a, b in a pointed symset (X, ε), we have*

(i) $Q(Q(a)b) = Q(a)Q(b)Q(a)$;

(ii) $Q(\varepsilon) = id_X$ *and* $Q(a)^{-1} = Q(a^{-1})$, *where* $a^{-1} := S_\varepsilon a$;

(iii) $Q(a \bullet b) = Q(a)Q(b)^{-1}Q(a)$.

Proof. For items (i) and (iii), see [17, Lemma 1.1, Chapter II] or [19]. For (ii), we observe $Q(\varepsilon) = (S_\varepsilon)^2 = \mathrm{id}_X$ and

$$Q(a)^{-1} = (S_a S_\varepsilon)^{-1} = S_\varepsilon S_a = S_{S_\varepsilon a} S_\varepsilon = Q(a^{-1}).$$

□

Item (i) of the previous lemma is sometimes called the *fundamental property* of the quadratic representation.

Theorem 5.4. *Let (X, ε) be a a pointed symset. Then $Q(X) \subseteq G(X)$ is a twisted subgroup and hence a symset with respect to $x \bullet y = xy^{-1}x$. Furthermore, members of $Q(X)$ are inverted by the involutory automorphism $g \mapsto S_\varepsilon g S_\varepsilon : G(X) \to G(X)$. If X is homogeneous, then $Q(X)$ is 2-divisible, and if X is dyadic, then $Q(X)$ is uniquely 2-divisible. The map $x \mapsto Q(x) : (X, \bullet) \to (Q(X), \bullet)$ is a homomorphism of pointed symsets and is an isomorphism in the case that X is dyadic.*

Proof. For $x, y \in Q(X)$, $Q(x)Q(y)^{-1}Q(x) = Q(Q(x)y^{-1}) \in Q(X)$ by Lemma 5.3(i), and thus $Q(X)$ is a twisted subgroup of $G(X)$. If the twisted subgroup is given the structure of a symset, then Lemma 5.3(iii) establishes that the map $x \to Q(x)$ is a homomorphism of symsets from X onto $Q(X)$.

For $x \in X$, we have

$$S_\varepsilon Q(x) S_\varepsilon = S_\varepsilon S_x S_\varepsilon S_\varepsilon = S_{S_\varepsilon x} S_\varepsilon = Q(S_\varepsilon x) = Q(x^{-1}).$$

Thus conjugation by S_ε carries $Q(X)$ into itself and hence the subgroup $G(X)$ that it generates into itself. Since $(S_\varepsilon)^2 = \mathrm{id}_X$, it follows that $g \mapsto S_\varepsilon g S_\varepsilon : G(X) \to G(X)$ is an involutory automorphism. By Lemma 5.3(ii), $Q(x^{-1}) = Q(x)^{-1}$, so members of $Q(X)$ are inverted under conjugation by S_ε.

Suppose that X is homogeneous. Since the surjective homomorphic image of a homogeneous symset remains homogeneous, it follows from Proposition 4.2 that $Q(X)$ is 2-divisible.

Suppose that X is dyadic. If $a = Q(x)\varepsilon = Q(y)\varepsilon$, then by Axiom (4) $x = \varepsilon\#a = y$. Thus the quadratic representation $Q : X \to Q(X)$ is an isomorphism of symsets, and hence $Q(X)$ is a dyadic symset. By Proposition 4.2 $Q(X)$ is uniquely 2-divisible. $\square$

Example 5.5. Consider a finite dimensional Jordan algebra A over the field of real numbers. Then the set M of invertible elements is open in A and becomes a symmetric space with the product

$$x \bullet y = P(x)y^{-1},$$

where $P(x)$ is the *Jordan algebra quadratic representation* defined by $P(x)(y) = 2x(xy) - x^2y$ ([17, Chapter II, Theorem 1.2]). In particular, the binary operation $x \bullet y$ on M satisfies the three axioms of a symset (and, in addition, the symmetries are homeomorphisms with isolated fixed points).

If one restricts attention to Euclidean Jordan algebras and the corresponding symmetric cones X, the images of the exponential mapping, then the symmetric cone is closed under the bullet operation and additionally satisfies the fourth axiom concerning the existence of means or midpoints. Indeed specific formulas exist for calculating the geometric mean, which is the midpoint (see [15]). Let ε denote the identity of the Jordan algebra A. We calculate in the symmetric cone X:

$$S_xS_\varepsilon(y) = x \bullet (\varepsilon \bullet y) = x \bullet y^{-1} = P(x)(y).$$

Since $S_xS_\varepsilon = Q(x)$ in the dyadic symset $(X, \bullet)$, we see that $Q(x)$ in $(X, \bullet)$ and $P(x)$ in the Jordan algebra sense agree on X. A number of the formulas and calculations of this section are highly reminiscent of calculations with the quadratic representation in the theory of Jordan algebras, and we see that indeed these calculations in sysmsets generalize those on the symmetric cones of Euclidean Jordan algebras.

Corollary 5.6. *Let $(X, \bullet)$ be a dyadic symset and let $x, y \in X$. Then there exists a unique homomorphism g of dyadic symsets from the dyadic line $(\mathbb{D}, \bullet)$ to X such that $g(0) = x$ and $g(1) = y$.*

Proof. We set $\varepsilon = x$, the distinguished point of X. The map $x \mapsto Q(x) : X \to Q(X) \subseteq G(X)$ is an isomorphism of pointed symsets and $Q(X)$ is a uniquely 2-divisible twisted subgroup by Theorem 5.4. By Lemma 4.4 there exists a unique group homomorphism σ from $(\mathbb{D}, +)$ into $Q(X)$ such that $\sigma(1) = Q(y)$ and by Proposition

4.2 it is also a symset homomorphism. The composition $Q^{-1}\sigma$ is then the desired symset homomorphism. If there were another, then the composition with Q would give one into $Q(X)$, which would also be a group homomorphism (since powers in the symset and group sense agree), but the latter is unique. □

6. Universal twisted representations

The quadratic representation gives a useful connection between symsets and twisted subgroups of groups, but it suffers the disadvantage that it is not functorial. In this section we give an alternative representation that is functorial. We consider the categories SYM of pointed symsets and symset homomorphisms and the category $\mathcal{G}^\circ$ of involutive groups. The second category has for objects pairs (G,τ), where τ is an involutive automorphism of G, and for morphisms (G_1,τ_1) to (G_2,τ_2) homomorphisms $h : G_1 \to G_2$ such that $h \circ \tau_1 = \tau_2 \circ h$. For (G,τ) an involutive group and $g \in G$, we set $g^* := (\tau(g))^{-1}$. We note that $g \mapsto g^* : G \to G$ is an antiautomorphism.

Definition 6.1. Let $(S,\bullet,\varepsilon)$ be a pointed symset and (G,τ) an involutive group. A *twisted representation* of S in G is a function $h : S \to G$ such that

(i) for all $s,t \in S$, $h(s \bullet t) = h(s)h(t)^{-1}h(s)$,
(ii) $h(S) \subseteq \{g \in G : g = g^*\}$,
(iii) $h(\varepsilon) = e$, the identity of G.

If, additionally, for any twisted representation $h_1 : S \to G_1$ there exists a unique homomorphism of involutive groups $f : G \to G_1$ such that $h_1 = fh$, then the twisted representation h is called a *universal twisted representation.*

We show that for every symset S, there is a universal twisted representation for S. We first recall a construction from [1].

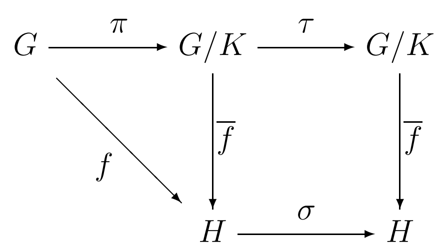
Lemma 6.2. *(Aschbacher) Let the group G be generated by a subset X. Then*

(i) *there exists a smallest normal subgroup K of G such that the quotient group G/K admits an involution that inverts the elements of the image of X;*
(ii) *any homomorphism $f : G \to H$ into an involutive group H that carries X into the elements inverted by the involution of H has kernel containing K;*
(iii) *the induced homomorphism $\overline{f} : G/K \to H$ is a homomorphism of involutive groups.*

The normal subgroup K is generated by

$$\{x_1^{-1}\cdots x_n^{-1} : x_1\cdots x_n = e,\ x_1,\ldots,x_n \in X\},$$

where $e = e^2 \in G$. The involution τ on G/K is given by $\tau(x_1\cdots x_n K) = x_1^{-1}\cdots x_n^{-1}K$.



Proposition 6.3. *Every symset S has a universal twisted representation that is unique up to an isomorphism commuting with the twisted homomorphisms.*

Proof. We first form the free group $F(S)$ over the set S of generators. We then consider the smallest normal subgroup N of $F(S)$ containing $\{(s\bullet t)^{-1}st^{-1}s) : s,t \in S\}$. Then the function $\beta : S \to F(S)/N$ defined by $\beta(s) = sN$ satisfies $\beta(s\bullet t) = \beta(s)\beta(t)^{-1}\beta(s)$ and thus is a twisted homomorphism.

Note that $\beta(S)$ generates $F(S)/N$ and hence by the preceding lemma there exists a smallest group congruence on $F(S)/N$, namely the coset congruence associated with K, such that the quotient group $F^\bullet(S)$ is involutive and the image of $\beta(S)$ is inverted by the involution. Let $j_S : S \to F^\bullet(S)$ be the composition of β and the quotient map from $F(S)/N$ onto $F^\bullet(S)$. We claim that this is the universal twisted representation (note that it is a twisted representation).

Let $k : S \to H$ be a twisted representation into the involutive group H. Then k factors through the free group $F(S)$ and hence through $F(S)/N$ since $k(s\bullet t) = k(s)k(t)^{-1}k(s)$. It then follows from Lemma 6.2 that k factors through $F^\bullet(S)$, i.e., there exists a homomorphism of involutive groups $\ell : F^\bullet(S) \to H$ such that $\ell\circ j_S = k$. Note that ℓ is unique since $j_S(S)$ generates $F^\bullet(S)$.

The argument for the uniqueness of the universal twisted representation up to isomorphism is the standard one for universal objects. $\square$

We typically denote the universal twisted represention for a pointed symset S by $j_S : S \to F^\bullet(S)$.

Corollary 6.4. *Given a pointed symset S, there exist a unique homomorphism of involutive groups $\gamma : F^\bullet(S) \to G(S)$ such that $\gamma j_S = Q$, where $G(S)$ is the displacement group and Q is the quadratic representation.*

Proof. This follows from the preceding proposition and Theorem 5.4. □

Corollary 6.5. *For S a dyadic symset, the universal twisted representation is injective.*

Proof. This follows from the preceding corollary and the fact that the quadratic representation is injective (Theorem 5.4). □

Given a homomorphism $f : S \to T$ of point symsets, we obtain $F^\bullet(f) : F^\bullet(S) \to F^\bullet(T)$, where $F^\bullet(f)$ is the unique homomorphism of involutive groups induced by the twisted homomorphism $j_T f : S \to T \to F^\bullet(T)$. The following proposition is then straightforward to verify.

Proposition 6.6. *The correspondences $S \to F^\bullet(S)$ and $(f : S \to T) \to F^\bullet(f) : F^\bullet(S) \to F^\bullet(T)$ define a functor from the category SYM of pointed symsets to the category $\mathcal{G}^\circ$ of involutive groups.*

7. Dyadic symsets and groups with polar decomposition

We pursue the lines of investigation of the preceding section for the special case of dyadic symsets and obtain considerable more structure in this setting. As mentioned in the introduction, connections between symmetric spaces and involutive groups have long been known and play an important role in the theory of Riemannian symmetric spaces.

We work in this section in the setting of an involutive group G, a group equipped with an involutive automorphism σ. We set $g^* = \sigma(g^{-1}) = (\sigma(g))^{-1}$ and note that $g \mapsto g^* : G \to G$ is an involutive antiautomorphism. Let

$$K = G^\sigma := \{x \in G : \sigma(x) = x\}, \qquad P_G := \{xx^* : x \in G\} \subseteq G_\sigma := \{g \in G : g = g^*\}.$$

(That $(xx^*)^* = x^{**}x^* = xx^*$ shows $P_G \subseteq G_\sigma$.)

We recall some basic terminology. Let G be group with subgroup H. A subset L of G is called a *transversal of G/H* or *transversal to H* if the identity $e \in L$ and L

intersects each coset gH of H in precisely one point. Thus the map $g \mapsto gH : G \to G/H$ has a cross-section, namely the map that picks the member of L out of each coset. One sees readily that a subset L containing e is a transversal of G/H if and only if the map $(x, h) \mapsto xh : L \times H \to G$ is a bijection. In the case of an involutive group (G, σ), if $L \subseteq \{g \in G : g = g^*\}$, then the map $(x, k) \mapsto xk : L \times G^\sigma \to G$ is called a *polar map*. Hence L containing e is transversal to G^σ if and only if the polar map is a bijection. If it is a bijection, then the pair (L, G^σ) is called a *polar decomposition* for (G, σ).

Lemma 7.1. *The sets P_G and G_σ are twisted subgroups, and hence the operation $x \bullet y := xy^{-1}x$ on P_G and G_σ satisfies the three axioms for a symset.*

Proof. By Corollary 4.6 P_G is a twisted subgroup. For $x, y \in G_\sigma$, the equality

$$(x \bullet y)^* = (xy^{-1}x)^* = x^*(y^{-1})^*x^* = xy^{-1}x = x \bullet y$$

shows that G_σ is also a twisted subgroup. We have already noted (Proposition 4.2) that the first three axioms are satisfied for twisted subgroups. □

The next lemma presents a type of converse to the preceding lemma.

Lemma 7.2. *Let (G, σ) be an involutive group and let Q be a twisted subgroup contained in G_σ. Then the subgroup H generated by Q is an involutive subgroup with respect to the restriction of σ, and $P_H \subseteq Q$. If Q is 2-divisible, then $P_H = Q$.*

Proof. Since Q is closed under inversion and contained in G_σ, it is invariant under σ, and thus the group H it generates is invariant under σ. Any $h \in H$ can be written as a product of members of Q, $h = q_1 \cdots q_n$. Then $hh^* = q_1 \cdots q_n q_n \cdots q_1$, which is in Q (inductively consider $q_i \cdots q_n q_n \cdots q_i$ as i moves from n to 1). Thus $P_H \subseteq Q$. If Q is 2-divisible, then $x \in Q$ has a square root $y \in Q$, and $x = y^2 = yy^* \in P_H$. □

We note in passing the standard observation that one can alternatively work with the coset decomposition $M := G/K$ instead of P_G. The next remark is standard and can be directly verified [12, Chapter XIII,5].

Remark 7.3. Consider the binary operation on $M = G/K$ defined by

$$xK \bullet yK = xx^*\sigma(y)K.$$

The mapping $xx^* \mapsto xK : P_G \to G/K$ is a well-defined $\bullet$-isomorphism.

Most, if not all, of the equivalence of (2), (3) and (4) below may be found in the literature and is more or less familiar to researchers in loop theory; see, for example, [1], [3], and [10]. For completeness, we include a quick, direct proof.

Theorem 7.4. *Let (G, τ) be an involutive group, $K = G^\tau$ the fixed point subgroup, and $P = \{xx^* : x \in G\}$. The following are equivalent:*

(1) *P is a dyadic symset under the standard operation $x \bullet y := xy^{-1}x$;*
(2) *P is a uniquely 2-divisible twisted subgroup;*
(3) *the polar map $(x, k) \mapsto xk : P \times K \to G$ is bijective;*
(4) *P is transversal to K.*

Proof. The equivalence of (1) and (2) follows from Proposition 4.2, in light of Lemma 7.1 and the equivalence of (3) and (4) is immediate, as remarked in the beginning of this section.

We turn to the equivalence of (2) and (3). If (2) and $g = x_1k_1 = x_2k_2$, then $gg^* = (x_1)^2 = (x_2)^2$. Hence $x_1 = x_2$, and then $k_1 = k_2$.

Conversely, for $gg^* \in P$, let $g = xk$. Then $gg^* = xk(xk)^* = x^2$, so $x \in P$ is a square root of gg^*. If $y \in P$ were another, then one verifies that $y(y^{-1}g)$ would give another decomposition of g, since

$$y^{-1}g = y^{-1}gg^*(g^*)^{-1} = y^{-1}y^2\sigma(g) = y\sigma(g) = \sigma(y^{-1}g).$$

□

We consider the full subcategory DSYM of SYM consisting of pointed dyadic symsets and the full subcategory $P\mathcal{G}^\circ$ of $\mathcal{G}^\circ$ consisting of *involutive groups with polar decomposition* satisfying property (3) (or any of the equivalent properties) of the preceding theorem. We define a functor $\mathcal{P} : P\mathcal{G}^\circ \to$ DSYM that sends an involutive group with polar decomposition (G, σ) to the pointed dyadic symset $(P_G, \bullet)$ given in the previous theorem. One verifies directly that if $f : G \to H$ is a homomorphism of involutive groups, then $f(P_G) \subseteq P_H$, so the restriction $f : P_G \to P_H$ is a homomorphism of pointed dyadic symsets.

There are various equivalent ways of defining adjoint functors. We adopt the following (see [8, Appendix 3]). Functors $F : \mathcal{A} \to \mathcal{B}$ and $P : \mathcal{B} \to \mathcal{A}$ are *adjoint* if for every object $A \in \mathcal{A}$, there is a morphism $\eta_A : A \to PF(A)$ such that for all morphisms $f : A \to PB$ in $\mathcal{A}$, there is a unique morphism $f' : FA \to B$ in $\mathcal{B}$ such that $f = (Pf') \circ \eta_A$. Additionally η should be a natural transformation from the identity functor $1_{\mathcal{A}}$ to PF and F should be given by $F(f) = (\eta_{A_2} f)'$ for $f : A_1 \to A_2$ in $\mathcal{A}$.

Proposition 7.5. *The functors $F^\bullet : DSYM \to P\mathcal{G}^\circ$ and $\mathcal{P} : P\mathcal{G}^\circ \to DSYM$ are adjoint functors, the functor $F^\bullet$ being the left adjoint. Furthermore, we have $\eta : 1_{DSYM} \to \mathcal{P}F^\bullet$ is a natural equivalence of functors.*

Proof. For every pointed dyadic symset X, we define $\eta_X : X \to \mathcal{P}F^\bullet(X)$ to be the corestriction of $j_X : X \to F^\bullet(X)$ to codomain $P_{F^\bullet(X)} = \mathcal{P}(F^\bullet(X))$. It follows from Corollary 6.5 that $j_X : X \to F^\bullet(X)$ is injective, by Lemma 7.2 that $P_{F^\bullet(X)} = j_X(X)$, and hence that $\eta_X : X \to \mathcal{P}F^\bullet(X)$ is an isomorphism of pointed symsets. The naturality of η is straightforward, and the characterization of $F(f)$ in the definition of adjoint functors is simply a reformulation of our definition of $F^\bullet$ at the morphism level.

Let X be a pointed dyadic symset and G an involutive group with polar decomposition. Suppose that $f : X \to P_G$ is a homomorphism of symsets. Then $f : X \to P_G \hookrightarrow G$ is a twisted representation of X, so by Proposition 6.3 extends uniquely to a homomorphism of involutive groups $f' : F^\bullet(X) \to G$ in such a way that $f' j_X(x) = f(x)$ for all $x \in X$. It then follows from the definitions of η_X and $\mathcal{P}$ that $f = (\mathcal{P}f')\eta_X$.

□

Let G be a Banach-Lie group and let $\mathfrak{g}$ be its Banach-Lie algebra. Let σ be a differentiable involutive automorphism of G, and let $\mathfrak{p} = \{X \in \mathfrak{g} : \mathrm{d}\sigma(1)(X) = -X\}$. The coset space $M = G/K$ becomes a geodesically complete Finsler manifold with a canonical spray [18]. If $X \in \mathfrak{p}$, then $\sigma(\exp X) = \exp(\mathrm{d}\sigma(1)(X)) = \exp(-X)$ and

$$(\exp X) = (\exp X/2)(\exp X/2) = (\exp X/2)\sigma(\exp X/2)^{-1} \in P = \{x\sigma(x^{-1}) : x \in G\}$$

and hence $\exp \mathfrak{p} \subset P$. Suppose that the polar map

$$\exp \mathfrak{p} \times K \to G, \quad (\exp X, k) \mapsto (\exp X)k$$

is bijective. Let $x \in G$. Then $x = (\exp X)k$ for some $X \in \mathfrak{p}$ and $k \in K$. Since $x\sigma(x^{-1}) = (\exp X)k\sigma((\exp X)k)^{-1} = (\exp X)kk^{-1}\sigma(\exp X) = (\exp X)^2 = \exp 2X$, we have $P \subset \exp \mathfrak{p}$. We have proved the following.

Corollary 7.6. *If the polar map*

$$\exp \mathfrak{p} \times K \to G, \quad (\exp X, k) \mapsto (\exp X)k$$

is bijective, then the manifold $M = G/K$ *(and also* $\exp \mathfrak{p}$*) is a dyadic symset.*

The previous theory finds a classic illustration in the well-known Cartan decomposition of semisimple Lie groups.

Example 7.7. Let G be a connected semisimple Lie group over the reals with finite dimensional Lie algebra $\mathfrak{g}$. Let τ be a Cartan involution on $\mathfrak{g}$, $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ the corresponding Cartan decomposition and let K be a Lie subgroup with Lie algebra $\mathfrak{k}$, the subalgebra fixed by τ. Then we have

(i) K is closed, connected, and equal to the fixed point set of a unique involutive automorphism of G extending τ;
(ii) The center of G is contained in K; K is compact if and only if G has finite center;
(iii) K is its own normalizer. The centralizer of K in G is the center of K.
(iv) The map $(X, k) \mapsto (\exp X)k$ is a diffeomorphism of $\mathfrak{p} \times K$ onto G. The involution on G sends $g = \exp(X)k$ to $\exp(-X)k$.

The preceding items are all standard, see, for example Theorem 2.3 of Chapter IV of [17]. We remark further that the twisted subgroup $P = \exp \mathfrak{p}$ has unique square roots, indeed unique roots of all orders, since the exponential function restricted to $\mathfrak{p}$ is a bijection onto P.

8. Dyadic symmetric sets and B-loops

Suppose that G is a group, H is a subgroup, and L is a transversal of G/H. Then the map $(x, h) \mapsto xh : L \times H \to G$ is bijective. This allows one to define a multiplication on L as follows: for $a, b \in L$, we write $ab = xh \in LH$ for unique $x \in L$, $h \in H$ and define $a * b := x$. Then as an algebraic structure $(L, *)$ is a left loop, that is, it has an identity, namely the identity e of the group, and there is a unique solution of the equation $a * x = b$ for all $a, b \in L$ (see, for example, [11, Theorem 2.7]). The various types of left loops and loops that arise as one imposes various additional properties on the transversal L have been quite intensively studied.

Things become quite nice in the case that we considered in the previous section. Let (G, τ) be an involutive group, $K = G^\tau$ the fixed point subgroup, and $P = \{xx^* : x \in G\}$ satisfy any of the four equivalent conditions of Theorem 7.4.

Lemma 8.1. *The left loop multiplication in P is given by*

$$a * b := (ab^2a)^{1/2}.$$

Proof. Let $a, b \in P$. Define $k = (a * b)^{-1}ab$, where $a * b = (ab^2a)^{1/2}$. Then

$$\begin{aligned} k \in K &\Leftrightarrow (a * b)^{-1}ab \in K \\ &\Leftrightarrow \sigma((a * b)^{-1}ab) = (a * b)^{-1}ab \\ &\Leftrightarrow \sigma(a * b)^{-1}\sigma(a)\sigma(b) = (a * b)^{-1}ab \\ &\Leftrightarrow (a * b)a^{-1}b^{-1} = (a * b)^{-1}ab \\ &\Leftrightarrow (a * b)^2 = ab^2a \\ &\Leftrightarrow ab^2a = ab^2a. \end{aligned}$$

We thus conclude that $k \in K$. Since by definition $a * b \in P$, we conclude that $(a * b)k$ is the polar decomposition of ab, and hence that $a * b = (ab^2a)^{1/2}$ gives the left loop multiplication. □

Remark 8.2. It is frequently convenient to work with an alternative multiplication on P given by $a \circ b = a^{1/2}ba^{1/2}$. This is no loss in generality, since the left loops $(P, *)$ and $(P, \circ)$ are isomorphic, the isomorphism being given by $D : (P, *) \to (P, \circ)$, $D(x) = x^2$:

$$D(a * b) = D((ab^2a)^{1/2}) = ab^2a = a^2 \circ b^2 = D(a) \circ D(b).$$

The bijectiveness follows from the unique 2-divisibility of the twisted subgroup P. Note that both the multiplications of $(P, *)$ and $(P, \circ)$ agree on any cyclic subgroup of G with that computed in the group G.

We give the basic definitions and elementary properties from loop theory that we employ in the remainder of this section. A *loop* is a left loop $(L, \circ)$ that is also a right loop, that is, equations of the form $y \circ a = b$ also have unique solutions for all a, b in the left loop. A *left Bol loop* is a loop satisfying the Bol-identity (I), and a *Bruck loop* or *K-loop* is a left Bol loop satisfying item (II).

(I) (Bol-identity) $x \circ (y \circ (x \circ z)) = (x \circ (y \circ x)) \circ z$,

(II) (Automorphic inverse property) $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$.

An equivalent definition of a K-loop is to replace item (II) by the following [11, Theorem 6.8]

(II') $(a \circ b) \circ (a \circ b) = a \circ ((b \circ b) \circ a)$.

It is a standard result that a K-loop (indeed a left Bol loop) is power associative and every element has a unique inverse, which together imply that every element is contained in a cyclic subgroup. Furthermore, $x^m \circ (x^n \circ y) = x^{m+n} \circ y$ for all integers m, n. The K-loop is *uniquely* 2*-divisible* if every element has a unique square root. Such loops are sometimes referred to as *B-loops*, although originally only finite B-loops were considered. The term B-loop arose in the work of Glaubermann ([4] and [5]). He studied K-loops that were finite of odd order. Since each cyclic subgroup $\langle x \rangle$ partitions the K-loop in cosets $\langle x \rangle \circ y$ of equal cardinality, one has a Lagrange theorem for cyclic subgroups. Therefore each cyclic subgroup has odd order and hence is uniquely 2-divisible.

Definition 8.3. A *B-loop* is a uniquely 2-divisible K-loop.

We give an alternative characterization of B-loops.

Lemma 8.4. *A K-loop is a B-loop if and only if it is* 2*-divisible and has no elements of order* 2*.*

Proof. A B-loop cannot have elements of order 2, for otherwise the identity e would not have a unique square root. Conversely suppose that a K-loop is 2-divisible and $x^2 = y^2$. Then by (II$'$) in the definition of a K-loop, we have

$$(x^{-1} \circ y)^2 = x^{-1} \circ (y^2 \circ x^{-1}) = x^{-1} \circ (x^2 \circ x^{-1}) = \varepsilon.$$

Since there are no elements of order 2, it follows that $x^{-1} \circ y = \varepsilon$, and left multiplying by x that $x = y$. ∎

Proposition 8.5. *Let L be a uniquely 2-divisible twisted subgroup of a group G. Then L with the operation $a \circ b = a^{1/2}ba^{1/2}$ is a B-loop.*

Proof. See 3.9 of [10] or [11, Theorem 6.14]. □

We need one more basic result about B-loops.

Proposition 8.6. *Let $(L, \circ)$ be a B-loop. Then L is isomorphic to a uniquely 2-divisible twisted subgroup of some group with operation $a \circ b = a^{1/2}ba^{1/2}$.*

Proof. See [11, Theorem 6.15]. □

We come now to a major result of the paper.

Theorem 8.7. *A pointed dyadic symset $(X, \bullet, \varepsilon)$ is a B-loop with respect to the operation $x \circ y = Q(x^{1/2})y = (\varepsilon \# x) \bullet y$. Conversely a B-loop is a dyadic symset with respect to the operation $x \bullet y = x^2 \circ y^{-1}$. The two constructions are inverse constructions. The squaring map, the square root map, and the inversion maps all agree for the two structures $(X, \bullet, \varepsilon)$ and $(X, \circ)$. Furthermore, a function between two pointed dyadic symsets preserving the point ε is a homomorphism if and only if it is a homomorphism between the corresponding B-loops. Hence the functor from the category DSYM of pointed dyadic symsets to the category of B-loops and loop homomorphisms that assigns to a pointed dyadic symset the same set with the corresponding B-loop structure and to a homomorphism of pointed dyadic symsets the same function, now a loop homomorphism, between the corresponding B-loop structures is an isomorphism of categories.*

Proof. By Theorem 5.4 the dyadic symset X is, up to an isomorphic copy, a uniquely 2-divisible twisted subgroup of a group G endowed with the operation $x \bullet y = xy^{-1}x$. Then

$$Q(x^{1/2})y = S_{x^{1/2}}S_\varepsilon y = S_{x^{1/2}}y^{-1} = x^{1/2}yx^{1/2}.$$

The first assertion of the theorem now follows from Proposition 8.5.

Conversely by Proposition 8.6 a B-loop arises, again up to loop isomorphism, from a uniquely 2-divisible twisted subgroup with the operation $a \circ b = a^{1/2}ba^{1/2}$. Then $x \bullet y = x^2 \circ y^{-1} = xy^{-1}x$ yields a dyadic symset operation.

For the assertions about the squaring map, square root map, and inversion map, we again work in an isomorphic copy that is a twisted subgroup, and note that there these operations for both the dyadic symset and the B-loop agree with those in the group and hence with each other.

It follows readily from the preceding computations that the two constructions are inverse constructions, that is, if on a pointed dyadic symset the B-loop operation $\circ$ is defined from $\bullet$ and $\bullet_1$ is defined from $\circ$, then $\bullet_1$ and $\bullet$ are the same operations and vice-versa.

(Note that we can pass directly from any pointed dyadic symset to its B-loop structure and back to the dyadic symset by the formulas given in the theorem. Working in the isomorphic copy of a twisted subgroup was done to facilitate deriving the assertions and make possible the application of known results.)

Since homomorphisms of either type of algebraic structure preserve powers and dyadic roots as well as the given operation, it follows immediately from the formulas for the alternative operation that this operation is also preserve, i.e. the function remains a homomorphism for the new operation defined from the old.

The final categorical assertion follows from the preceding results. □

We mention in closing a final equivalence with the theory of gyrogroups that now immediately results. The notion of a gyrogroup has been introduced by A. Ungar, primarily as an appropriate structure for the study of Einstein velocity addition in special relativity and related topics (see, for example, [23]). Ungar's axioms take the following form.

Let P be equipped with a binary operation $\odot$, an unary operation $x \mapsto x^{-1}$, and an identity e. For $x, y \in P$, define $\mathrm{gyr}[x; y] : P \to P$ by

$$\mathrm{gyr}[x; y]z = (x \odot y)^{-1} \odot (x \odot (y \odot z)).$$

Then P is a *gyrogroup* if it satisfies the following laws (1)-(5) and is a *gyrocommutative* gyrogroup if it additionally satisfies law (6):

(1) $x \odot (y \odot z) = (x \odot y) \odot \mathrm{gyr}[x; y]z$,	(gyroassociative law)
(2) $e \odot x = x \odot e = x$,	(existence of an identity)
(3) $x \odot x^{-1} = x^{-1} \odot x = e$,	(existence of inverses)
(4) $\mathrm{gyr}[e; y] = \mathrm{id}$,	
(5) $\mathrm{gyr}[x \odot y; y] = \mathrm{gyr}[x; y]$,	(loop property)
(6) $x \odot y = \mathrm{gyr}[x; y](y \odot x)$.	(gyrocommutative law)

Sabinin, Sabinina, and Sbitneva [21] have shown that $(P, \odot)$ is a gyrocommutative gyrogroup if and only if it is a K-loop. It then follows immediately that $(P, \odot)$ is a uniquely 2-divisible gyrocommutative gyrogroup if and only if it is a B-loop. By Lemma 8.4 the fact that $(P, \odot)$ is uniquely 2-divisible is equivalent to its being 2-divisible and having no elements of order 2. Thus there is an alternative version of Theorem 8.7 that substitutes gyrocommutative gyrogroups for B-loops, but otherwise leaves the theorem intact.

Theorem 8.8. *A pointed dyadic symset $(X, \bullet, \varepsilon)$ is a uniquely 2-divisible gyrocommutative gyrogroup with respect to the operation $x \circ y = Q(x^{1/2})y$. Conversely a 2-divisible gyrocommutative gyrogroup with no elements of order 2 is a dyadic symset with respect to the operation $x \bullet y = x^2 \circ y^{-1}$. The two constructions are inverse constructions. The squaring map, the square root map, and the inverse maps all agree for the two structures $(X, \bullet, \varepsilon)$ and $(X, \circ)$. Furthermore, a function between two pointed dyadic symsets preserving the point ε is a homomorphism if and only if it is a homomorphism between the corresponding gyrogroups.*

9. Future directions

In this paper we have primarily established relationships and equivalences between the category of pointed dyadic symsets and other algebraic categories. In future papers we plan to focus on the theory of the (geometric) mean in the context of dyadic symsets [14]. We also want to develop these ideas in a topological context, where the dyadic line is replaced by the usual real line.

References

[1] M. Aschbacher, Near subgroups of finite groups, *J. Group Theory* 1 (1998), 113–129.

[2] J. Faraut and A. Korányi, *Analysis on Symmetric Cones*, Clarendon Press, Oxford, 1994.

[3] T. Foguel, Polar decomposition of locally finite groups, *Results Math.* 42 (2002), 69–73.

[4] G. Glauberman, On loops of odd order I, *J. Algebra* 1 (1964), 374-396.

[5] —, On loops of odd order II, *J. Algebra* 8 (1968), 393-414.

[6] S. Helgason, *Differential Geometry, Lie Groups, and Symmetric Spaces*, Academic Press, Orlando, 1978.

[7] D. Joyce, A classifying invariant of knots, the knot quandle, *J. Pure Appl. Alg.* 23 (1982), 37-66.

[8] K. Hofmann and S. Morris, *The Structure of Compact Groups*, de Gruyter, Berlin, 1998.

[9] M. Kano, H. Nagao, and N. Nobusawa, On finite homogeneous symmetric sets, *Osaka J. Math.* 13 (1976), 399–406.

[10] H. Karzel and H. Wefelscheid, Groups with an involutory antiautomorphism and K-loops; application to space-time-world and hyperbolic geometry. *Results Math.* 23 (1993), 338–354.

[11] H. Kiechle, *Theory of K-Loops*, Lecture Notes in Mathematics 1778, Springer, Berlin, 2002.

[12] S. Lang, *Fundamentals of Differential Geometry*, Graduate Texts in Math., Springer, Heidelberg, 1999.

[13] J. D. Lawson and Y. Lim, The geometric mean, matrices, metrics, and more, *Amer. Math. Monthly* 108 (2001), 797-812.

[14] —, Means on dyadic symmetric sets and polar decompositions, preprint.

[15] —, Geometric means on symmetric cones, *Arch. der Math.* 75 (2000), 39-45.

[16] —, Metric and spectral geometric means on symmetric cones, submitted.

[17] O. Loos, *Symmetric spaces, I: General Theory*, Benjamin, New York, Amsterdam, 1969.

[18] K.-H.Neeb, A Cartan-Hadamard theorem for Banach-Finsler manifolds, Proceedings of the Conference on Geometric and Combinatorial Group Theory, Part II (Haifa, 2000), *Geom. Dedicata* 95 (2002), 115-156.

[19] N. Nobusawa, On symmetric structure of a finite set, *Osaka J. Math.* 11 (1974), 569–575.

[20] N. Nobusaws, Orthogonal groups and symmetric sets, *Osaka J. Math.* 20 (1983), 5-8.

[21] L. V. Sabinin, L. L. Sabinina, and L. V. Sbitneva, On the notion of a gyrogroup, *Aeq. Math.* 56 (1998) , 11-17.

[22] A. A. Ungar, Midpoints in gyrogroups. *Found. Phys.* 26 (1996), 1277-1328.

[23] —, Thomas precession: its underlying gyrogroup axioms and their use in hyperbolic geometry and relativistic physics, *Found. Phys.* 27 (1997), 881-951.

[24] H. Upmeier, *Symmetric Banach Manifolds and Jordan C^*-algebras*, North Holland Mathematics Studies, 1985.