Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 308 (2008) 415–421
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Binary operations derived from symmetric permutation sets and applications to absolute geometry

Helmut Karzel[a], Silvia Pianta[b, 1]

[a] *Zentrum Mathematik, T.U. München, D-80290 München, Germany*
[b] *Dipartimento di Matematica e Fisica, Università Cattolica, Via Trieste, 17, I-25121 Brescia, Italy*

Received 21 October 2004; received in revised form 30 November 2005; accepted 27 November 2006
Available online 2 June 2007

Abstract

A permutation set (P, A) is said symmetric if for any two elements $a, b \in P$ there is exactly one permutation in A switching a and b. We show two distinct techniques to derive an algebraic structure from a given symmetric permutation set and in each case we determine the conditions to be fulfilled by the permutation set in order to get a left loop, or even a loop (commutative in one case). We also discover some nice links between the two operations and finally consider some applications of these constructions within absolute geometry, where the role of the symmetric permutation set is played by the regular involution set of point reflections.

Keywords: Non-associative algebraic structure; Loop; Symmetric permutation set; Involution set; Absolute geometry

0. Introduction

Let $(P, \mathscr{L}, \equiv, \alpha)$ be an absolute plane geometry (we use the notations of [2,5]) and, for $a, b, c, \ldots \in P, a \neq b$, denote by: $\overline{a, b}$ the (uniquely determined) line joining a and b, $S(a; b, c) := \{x \in P \mid (x, a) \equiv (b, c)\}$ the circle with centre a and radius given by the congruence class of (b, c), $m_{a,b}$ the midpoint of a and b, $\tilde{a} : P \to P; x \mapsto x'$, where $x' = (\overline{a, x} \cap S(a; a, x))\backslash\{x\}$ if $x \neq a$ and $x' = a$ if $x = a$, the reflection in the point a.

An n-tuple $(a_1, a_2, \ldots, a_n)$ of n distinct points is called *convex* if $\forall i \in \mathbb{Z}_n$ and $\forall j \in \mathbb{Z}_n\backslash\{i, i+1, i+2\}$: $(\overline{a_i, a_{i+1}} \mid a_{i+2}, a_j) = 1$, i.e. a_j lies on the same halfplane with origin the line $\overline{a_i, a_{i+1}}$ containing a_{i+2}.

Now fix a point $o \in P$ and consider the following constructions:

First method: Given $a, b \in P$, let $a \oplus b \in S(a; o, b) \cap S(b; o, a)$ such that $(a, o, b, a \oplus b)$ is convex. The same result is achieved by setting $a \oplus b := \widetilde{m_{a,b}}(o)$.

Second method: Given $a, b \in P$ let $a^+ := \widetilde{m_{o,a}} \circ \tilde{o}$ and let $a + b := a^+(b)$ be the image of b under the motion a^+.

In Euclidean geometry both methods lead to the same result : $a \oplus b = a + b$ and $(a, o, b, a + b)$ is a parallelogram. Moreover $(P, +)$ is a commutative group and a^+ a translation.

In non-Euclidean geometry the binary operations "$\oplus$" and "$+$" are different and $(P, \oplus)$ and $(P, +)$ are not groups any more.

[1] Research partially supported by the Research Project of M.I.U.R. (Italian Ministry of Education, University and Research) "Strutture geometriche, combinatoria e loro applicazioni" and by the Research group G.N.S.A.G.A. of INDAM.
E-mail address: pianta@dmf.unicatt.it (S. Pianta).

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2006.11.058

For hyperbolic geometry Capodaglio in [1] studies the structure of $(P, \oplus)$ and shows that it is a commutative loop. $(P, +)$ too is a loop, not commutative but satisfying the conditions characterizing Bruck-loops or, what is the same, K-loops.

These two operations can be obtained from more general structures, the so-called symmetric permutation sets, introduced in Section 2.

A set P together with a subset $A \subseteq \text{Sym}\, P$ is called *symmetric permutation set* (P, A) if for each $a, b \in P$ there exists a unique permutation $\widetilde{ab} \in A$ such that $\widetilde{ab}(a) = b$ and $\widetilde{ab}(b) = a$. If $o \in P$ is fixed, define $a + b := \widetilde{oa} \circ \widetilde{oo}(b)$ and $a \oplus b := \widetilde{ab}(o)$ and call $(P, +)$ the *K-derivation* and $(P, \oplus)$ the *C-derivation* of (P, A) in o.

Then $(P, +_o)$ is a left loop if and only if $\widetilde{oo}$ is an involution and a loop if moreover the subset $\widetilde{oP} := \{\widetilde{ox} \mid x \in P\}$ of A acts regularly on P (cf.(3.1)), while $(P, \oplus)$ is a commutative loop if and only if o is a regular point of the permutation set $(P, \widetilde{aP})$ for all $a \in P$ (cf. (2.2)).

In Sections 2 and 3 we discuss the conditions that are needed to derive from each of the algebraic structures $(P, +)$ and $(P, \oplus)$ again a symmetric permutation set and determine in which cases this structure coincides with the original (P, A). Moreover we establish some relations between properties of (P, A) and, respectively, of $(P, +)$ and $(P, \oplus)$.

Section 4 is devoted to the special case of regular involution sets. The point set P of an ordinary absolute geometry (in the sense of [2]), together with the set $A = \widetilde{P}$ of all point reflections, make up an example of a regular invariant involution set. Here (P, A) has the additional property that for all $\alpha \in A$, $|\text{Fix}\,\alpha| = 1$, and furthermore the relation $\rho := \{(a, b, c) \in P^3 \mid \tilde{a} \circ \tilde{b} \circ \tilde{c} \in \widetilde{P}\}$ is a ternary equivalence relation which coincides with the collinearity relation.

In this case, the *K*-derivation in any point $(P, +)$ turns out to be a Bruck-loop (i.e. a K-loop) with the additional property that for all $a, b, c \in P \backslash \{o\}$, if $a^+ \circ c^+, b^+ \circ c^+ \in P^+$, then $a^+ \circ b^+ \in P^+$.

More generally, this property of the K-loop derivation characterizes those regular invariant involution sets (P, A) with $|\text{Fix}\,\alpha| = 1$ for all $\alpha \in A$, such that the relation ρ is a ternary equivalence relation (cf. (4.5)).

1. Notations and basic notions

In this paper we will use the following notations:

P will denote a non empty set, Sym P the group of all permutations of P, and $J := \{\sigma \in \text{Sym}\, P \mid \sigma^2 = \text{id}\}$.

If $A \subseteq \text{Sym}\, P$ then (P, A) is called *permutation set* and a point $p \in P$ will be called *transitive* if $A(p) = P$, *semiregular* if, for all $x \in P$, there exists at most one $\alpha \in A$ with $\alpha(p) = x$. Let $(P, A)_t$ denote the set of all transitive points and $(P, A)_s$ the set of semiregular points and let $(P, A)_r := (P, A)_t \cap (P, A)_s$ be the set of all *regular* points of (P, A).

The permutation set (P, A) will be called *transitive*, *semiregular*, *regular*, *invariant*, and *involution set* if, respectively, $P = (P, A)_t$, $P = (P, A)_s$, $P = (P, A)_r$, $\alpha \circ A \circ \alpha^{-1} = A$ for all $\alpha \in A$, and $A \subseteq J$.

If P is provided with a binary operation $+ : P \times P \to P; (a, b) \mapsto a + b$ then for $a \in P$ denote by $a^+ : P \to P; x \mapsto a + x$, the left addition by a, and let $P^+ := \{a^+ \mid a \in P\}$.

An element $o \in P$ is called a *left neutral element* if $o^+ = \text{id}$, a *right neutral element* if $x + o = x$ for all $x \in P$, and a *neutral element* if it is both a left and a right neutral element.

The pair $(P, +)$ is called a *left loop* if $P^+ \subseteq \text{Sym}\, P$ and there is a neutral element o, and a *loop* if $(P, +)$ is a left loop such that (P, P^+) is regular (these definitions are equivalent to the usual well-known definitions of left loop and loop, that can be found e.g. in [6]).

In a left loop $(P, +)$ we can define the following maps:

$\widehat{ab} : P \to P; x \mapsto (x^+)^{-1}(a + b)$, in particular $\hat{a} := \widehat{aa}$,

$\delta_{a,b} := ((a + b)^+)^{-1} \circ a^+ \circ b^+$,

$\nu := \hat{o} : P \to P; x \mapsto -x := (x^+)^{-1}(o)$,

$a^\circ := a^+ \circ \nu$,

and then the following *application sets*:

$\wedge(P, +) := \widehat{P} := \{\widehat{ab} \mid a, b \in P\}$,

$\circ(P, +) := P^\circ := \{a^\circ \mid a \in P\}$.

From these definitions it follows directly:

Proposition 1.1. *Let* $(P, +)$ *be a left loop then*:

(1) $\widehat{P} \subseteq \text{Sym}\, P \Leftrightarrow$ $(P, +)$ *is a loop*,

(2) $\widehat{P} \subseteq J \Leftrightarrow (P, +)$ *is a commutative loop*,
(3) $P^\circ \subseteq \mathrm{Sym}\, P \Leftrightarrow v \in \mathrm{Sym}\, P$,
(4) $P^\circ \subseteq J \Leftrightarrow (\star)\ \forall a, b \in P : a - (a - b) = b$ (cf. [2]).

Moreover for a left loop $(P, +)$ we can formulate the following conditions which are suitable to characterize some particular classes of loops:

(Bol) $\forall a, b \in P : a^+ \circ b^+ \circ a^+ \in P^+$.
(AIP) $v \in \mathrm{Aut}(P, +)$.
(K1) $\forall a, b \in P : \delta_{a,b} \in \mathrm{Aut}(P, +)$.
(K2) $\forall a, b \in P : \delta_{a,b} = \delta_{a,b+a}$.

A left loop which satisfies (Bol) is already a loop and it is called *Bol loop*. A Bol loop satisfying (AIP) is a *Bruck loop* and a loop where (AIP), (K1) and (K2) are valid is a *K-loop*. According to Kreuzer [7], Bruck loops and K-loops are the same (cf. also [6]).

2. Symmetric permutation sets

In this section let (P, A) be a *symmetric permutation set*, that is a permutation set such that the following condition holds:

(S) $\forall x, y \in P\ \exists_1\ \alpha \in A$ such that $\alpha(x) = y$ and $\alpha(y) = x$;

set $\widetilde{xy} := \alpha$, $\tilde{x} := \widetilde{xx}$ and $\widetilde{P} := \{\widetilde{xy} \mid x, y \in P\} \subseteq A$.
It is straightforward to verify:

Proposition 2.1. *In a symmetric permutation set* (P, A), *define* $\sim: P \times P \to \widetilde{P}; (a, b) \mapsto \widetilde{ab}$. *Then* $\sim$ *is a map and, given* $a, b, c, \ldots \in P$ *and* $\alpha \in A$:

(1) $\widetilde{ab} = \widetilde{ba}$.
(2) *If* $a \in \mathrm{Fix}\, \alpha^2$ *and* $b := \alpha(a)$, *then* $\alpha = \widetilde{ab}$.
(3) *If* $a \in \mathrm{Fix}\, \alpha$, *then* $\alpha = \tilde{a}$.
(4) $\widetilde{P} = \{\alpha \in A \mid \mathrm{Fix}\, \alpha^2 \neq \emptyset\}$ *and* $(P, \widetilde{P})$ *is also a symmetric permutation set*.
(5) *If* $\widetilde{P} \subseteq J$ *then* $(P, \widetilde{P})$*is even a regular involution set*.
(6) $\forall \alpha \in A : \mathrm{Fix}\, \alpha \neq \emptyset \Leftrightarrow A = \widetilde{P} = \{\tilde{a} \mid a \in P\}$.
(7) $\forall \alpha \in A : |\mathrm{Fix}\, \alpha| \leqslant 1 \Leftrightarrow \forall\ a \in P : \mathrm{Fix}\, \tilde{a} = \{a\}$.
(8) $\forall \alpha \in A : |\mathrm{Fix}\, \alpha| = 1 \Leftrightarrow \forall a, b \in P,\ \exists_1 m_{a,b} \in P : \widetilde{m_{a,b}} = \widetilde{ab}$.

Now, for any choice of a fixed point $o \in P$ the following binary operations can be derived from the symmetric permutation set (P, A)

$$\oplus : P \times P \to P; (a, b) \mapsto a \oplus b := \widetilde{ab}(o),$$
$$+ : P \times P \to P; (a, b) \mapsto a + b := \widetilde{ao} \circ \tilde{o}(b).$$

We call $\oplus = C_o(P, A)$ the *C-derivation* and $+ = K_o(P, A)$ the *K-derivation* of (P, A) in o.
From (2.1) it follows directly:

Proposition 2.2. *The operation* "$\oplus$" *is commutative with* o *as neutral element and* $(P, \oplus)$ *is a loop if and only if* (P, A) *satisfies the condition*:

(A_o) $\forall a, b \in P\ \exists_1 c \in P : \widetilde{ac}(o) = b$, *i.e.* $\forall a \in P$, o *is a regular point of the permutation set* $(P, \widetilde{aP} := \{\widetilde{ax} | x \in P\})$.

On the other hand, we have by (1.1.2):

Proposition 2.3. *Let* $(P, \boxplus)$ *be a commutative loop and let* $\widehat{P} := \wedge(P, \boxplus)$, *then* $(P, \widehat{P})$ *is a regular involution set*.

Proposition 2.4. *For the following statements*:

(1) $A \subseteq J$, *i.e.* (P, A) *is a regular involution set*,

(2) $\forall a, b, c \in P$, *if* $d := \widetilde{ab}(c)$ *then* $\widetilde{ab} = \widetilde{cd}$,

(3) $\forall o \in P$, $(P, \oplus)$, *with* $\oplus := C_o(P, A)$, *is a commutative loop*,

(4) $\forall a \in P$, $(P, \widetilde{aP} := \{\widetilde{ax} | x \in P\})$ *is a regular set of permutations*,

we have: (1) $\Leftrightarrow$ (2) $\Rightarrow$ (3) $\Leftrightarrow$ (4).

Proof. (1) $\Rightarrow$ (2): For $a, b \in P$, $\widetilde{ab} \in J$ implies $\widetilde{ab}(d) = c$ and so by (S), $\widetilde{ab} = \widetilde{cd}$.

(2) $\Rightarrow$ (1): Let $a, b, x \in P$ and $y := \widetilde{ab}(x)$ then by (2), $\widetilde{ab}(y) = \widetilde{xy}(y) = x$, i.e. $\widetilde{ab} \in J$.

(2) $\Rightarrow$ (3): Let $a, b \in P$, $c := \widetilde{ob}(a)$, then by (2) $\widetilde{ob} = \widetilde{ac}$, hence $\widetilde{ac}(o) = \widetilde{ob}(o) = b$. Assume $\widetilde{ad}(o) = b$, thus $\widetilde{ad} = \widetilde{ob}$ then $d = \widetilde{ad}(a) = \widetilde{ob}(a) = c$. Therefore by (2.2), $(P, \oplus)$ is a commutative loop.

(3) $\Leftrightarrow$ (4): By (2.2) we have (3) $\Leftrightarrow$ (A_o) holds for all $o \in P$, i.e. $\forall a \in P : P \subseteq (P, \widetilde{aP})_r \Leftrightarrow$ (4). $\square$

Proposition 2.5. *Assume that a symmetric permutation set* (P, A) *satisfies condition* (A_o) *of* (2.2) *with respect to a point* $o \in P$, *let* $\oplus := C_o(P, A)$, *hence* $(P, \oplus)$ *is a commutative loop and let* $\widehat{P} := \wedge(P, \oplus)$ *be the corresponding regular involution set according to* (2.3). *Then* $\widehat{P} = \widetilde{P} \Leftrightarrow \widetilde{P} \subseteq J$.

Proof. By (2.3) we have only to show "$\Leftarrow$". Since $\widetilde{P} \subseteq J$ the permutation set $(P, \widetilde{P})$ is regular by (2.4.1). Therefore, given $a, b, x \in P$ and set $x' := \widehat{ab}(x)$, the definitions entail $\widetilde{ab}(o) = a \oplus b = x \oplus x' = \widetilde{xx'}(o)$, thus $\widetilde{ab} = \widetilde{xx'}$, i.e. $\widetilde{ab}(x) = x' = \widehat{ab}(x)$. Consequently $\widetilde{ab} = \widehat{ab}$. $\square$

3. The K-derivation of a symmetric permutation set

In this section let $+ := K_o(P, A)$ be the K-derivation of a symmetric permutation set (P, A) in a point $o \in P$. Then for each $a \in P$, $a^+ = \widetilde{oa} \circ \tilde{o} \in \operatorname{Sym} P$ hence $(a^+)^{-1} = \tilde{o}^{-1} \circ \widetilde{oa}^{-1}$ and if we set $-a := (a^+)^{-1}(o) = \tilde{o}^{-1}(a)$ we obtain:

$$a + o = \widetilde{oa} \circ \tilde{o}(o) = \widetilde{oa}(o) = a; \quad o + a = \tilde{o} \circ \tilde{o}(a),$$

$$a + (-a) = o; \quad -a + a = (-a)^+(a) = \widetilde{o(-a)} \circ \tilde{o}(a),$$

$$a - (a - b) = \widetilde{oa} \circ \tilde{o} \circ \tilde{o}^{-1}(a - b) = \widetilde{oa} \circ \widetilde{oa}(b).$$

The equation $a + x = b$ has the unique solution $x := \tilde{o}^{-1} \circ \widetilde{oa}^{-1}(b)$ and if y is a solution of $y + a = b$ then $\widetilde{oy} \circ \tilde{o}(a) = b$. In particular, since $\widetilde{ox}(x) = o$ implies $\widetilde{ox}^{-1}(o) = x$, we see that $y + a = \widetilde{oy} \circ \tilde{o}(a) = o$ has the uniquely determined solution $y := \tilde{o}(a)$. This shows:

Proposition 3.1. *The operation* "+" *has the properties*:

(L1) $\forall x \in P : x + o = x$.

(L2) $\forall x \in P, \exists_1 \sim x \in P : \sim x + x = o$.

(L3) $\forall a, b \in P, \exists_1 x \in P : a + x = b$.

Moreover:

(1) $(P, +)$ *is a left loop if and only if* $\tilde{o} \in J$.

(2) $(P, +)$ *satisfies the condition* $(\star)$ *of* (1.1.4) *if and only if* $\widetilde{oP} \subseteq J$ (*then* $(P, +)$ *is a left loop*).

(3) $(P, +)$ *is a loop if and only if* $(P, \widetilde{oP})$ *is regular and* $\tilde{o} \in J$.

Remark 1. Note that $-x = \tilde{o}^{-1}(x)$ is the right inverse for all $x \in P$, whereas $\sim x = \tilde{o}(x)$ is the left inverse (well defined by (L2)).

Remark 2. For the K-derivation $+ := K_o(P, A)$ of a symmetric permutation set (P, A) in a point $o \in P$ we need only the subset $\widetilde{oP} := \{\widetilde{oa} | a \in P\} \subseteq \widetilde{P} \subset A$. Since $a^+ = \widetilde{oa} \circ \tilde{o}$ and $\tilde{o}^{-1} = \nu$ we obtain $\widetilde{oa} = a^+ \circ \tilde{o}^{-1} = a^+ \circ \nu = a^\circ$, i.e. $\widetilde{oP} = P^\circ$. If $\widetilde{oP} = P^\circ \subseteq J$, then $(P, \widetilde{oP}; o)$ is a reflection structure in the sense of [2] and $(P, +)$ is a left loop satisfying $(\star)$.

If $A \subseteq J$, i.e. (P, A) is a regular involution set, then $\widetilde{P} = \widetilde{oP} = P^\circ = A$ and $(P, +)$ is a loop satisfying the condition $(\star)$ of (1.1.4) (see [2]).

From this remark and (2.5) we obtain:

Proposition 3.2. *Let (P, A) be a symmetric permutation set, let $o \in P$ be fixed and let "$+ = K_o(P, A)$" and "$\oplus = C_o(P, A)$" be the K-derivation and the C-derivation in o, respectively, and let $P^\circ := \circ(P, +)$, $\widehat{P} := \wedge(P, \oplus)$. Then the following statements are equivalent*:

(1) $A \subseteq J$ *hence* $\widetilde{P} = P^\circ = A$.
(2) $(P, +)$ *is a loop satisfying* $(\star)$ *of* (1.1.4).
(3) $(P, \oplus)$ *is a commutative loop and* $\widehat{P} = A$.
(4) (P, A) *is a regular involution set*.

Now let $(P, +)$ be a set with a binary operation "$+$" satisfying (L1), (L2) and (L3) of (3.1). Then by (L1) there is a right neutral element o, by (L3) we have $P^+ \subseteq \mathrm{Sym}\, P$ and so $(P, +)$ is a left loop if $o^+ = \mathrm{id}$. Moreover for any $x \in P$ there is exactly one element $-x \in P$ determined by $x + (-x) = o$. Therefore the *negative map* $v : P \to P; x \mapsto -x$ is defined and it is a permutation of P by (L2).

Consequently, for all $a \in P$, $a^\circ = a^+ \circ v$ is a permutation, hence $P^\circ \subseteq \mathrm{Sym}\, P$. Moreover a° interchanges a and o since $a^\circ(o) = a^+ \circ v(o) = a^+(o) = a$ and $a^\circ(a) = a^+(-a) = o$.

(P, P°) is even a symmetric permutation set if $\forall a, b \in P$ there is exactly one $x^\circ \in P^\circ$ with $x^\circ(a) = x - a = b$ and $x^\circ(b) = x - b = a$.

If $(P, +)$ is even a loop then for any $a, b \in P$ there is exactly one $c \in P$ with $b = c - a = c^\circ(a)$ and so the set P° acts regularly on P. Therefore (P, P°) satisfies (S) if and only if $P^\circ \subseteq J$, which is equivalent to the condition $(\star)$ of (1.1.4). We may resume all these considerations in the following:

Proposition 3.3. *If $(P, +)$ satisfies* (L1),(L2) *and* (L3), *then*:

(1) $P^\circ \subseteq \mathrm{Sym}\, P$ *and* $\forall a \in P : a^\circ(o) = a$ *and* $a^\circ(a) = o$.
(2) (P, P°) *is a symmetric permutation set* $\Leftrightarrow$
(S′) $\forall\, a, b \in P \exists_1\, x \in P : x - a = b$ *and* $x - b = a$.
(3) (P, P°) *is a regular permutation set* $\Leftrightarrow$ $(P, +)$ *is a loop*.
(4) $P^\circ \subseteq J \Leftrightarrow (P, +)$ *satisfies* $(\star)$ *of* (1.1.4).
(5) (P, P°) *is a regular involution set* $\Leftrightarrow$ $(P, +)$ *satisfies* (S′) *and* $(\star) \Leftrightarrow (P, +)$ *is a loop satisfying* $(\star)$.

To conclude this section, we show some connections between the two operations that can be derived, via the K- or the C-derivation, by a symmetric permutation set:

Proposition 3.4. *Let $a, b \in P$ then*:

(1) $a + b = b + a \Leftrightarrow o \in \mathrm{Fix}\, (\widetilde{oa} \circ \tilde{o} \circ \widetilde{ob})^2$.
(2) $a \oplus b = a + b \Leftrightarrow o \in \mathrm{Fix}\, (\widetilde{ab} \circ \widetilde{oa} \circ \tilde{o} \circ \widetilde{ob})$.
(3) $a \oplus b = a + b = b + a \Leftrightarrow o \in \mathrm{Fix}\, (\widetilde{ab} \circ \widetilde{oa} \circ \tilde{o} \circ \widetilde{ob}) \cap \mathrm{Fix}\, (\widetilde{ab} \circ \widetilde{ob} \circ \tilde{o} \circ \widetilde{oa})$.
(4) *If* $\widetilde{oa} \circ \tilde{o} \circ \widetilde{oa} \in A$ *then* $\tilde{a} = \widetilde{oa} \circ \tilde{o} \circ \widetilde{oa}$ *and* $a \oplus a = a + a$.

4. The C- and K-derivation of regular involution sets

In this section let (P, A) be a regular involution set.

Proposition 4.1. *Let $o \in P$ be fixed, let $+ := K_o(P, A)$ and $\oplus := C_o(P, A)$ then*:

(1) $P^\circ := \circ(P, +) = \widehat{P} := \wedge(P, \oplus) = A$ (*by* (3.2)).
(2) $\forall a, b \in P : (a \oplus b) - a = b$ (*i.e.* $a \oplus b$ *is the solution of the equation* $x - a = b$) *and* $\ominus a = -a$.
(3) $\forall a, b \in P : a + b = ((\ominus b)^\oplus)^{-1}(a)$.

Proof. (2) By (1) there is exactly one $c^\circ \in P^\circ$ such that $b = c^\circ(a)$ hence $\widetilde{ab} = c^\circ$ and so $a \oplus b = \widetilde{ab}(o) = c^\circ(o) = c$, implying $a \oplus b - a = \widetilde{a, b} \circ \tilde{o} \circ \tilde{o}^{-1}(a) = b$.

(3) Since $P^\circ = A = \widehat{P}$ by (1) and $\tilde{o}(b) = -b = \ominus b$ by (2), we get $a + b = \widetilde{oa} \circ \tilde{o}(b) = \widehat{oa}(\ominus b) = ((\ominus b)^{\oplus})^{-1}(o \oplus a) = ((\ominus b)^{\oplus})^{-1}(a)$. □

Proposition 4.2. *Let $a, b \in P$ then*:

(1) $\widetilde{oa} \circ \tilde{o} \circ \widetilde{ob} \in J \Leftrightarrow a^+ \circ b^+ = b^+ \circ a^+ \Rightarrow a + b = b + a$.
(2) $\widetilde{oa} \circ \tilde{o} \circ \widetilde{ob} \in A \Leftrightarrow a^+ \circ b^+ \in P^+ \Rightarrow a^+ \circ b^+ = b^+ \circ a^+$ *and* $a + b = a \oplus b$.
(3) *If* $a^+ \circ b^+ = b^+ \circ a^+$ *then*: $a + b = a \oplus b \Leftrightarrow a^+ \circ b^+ \in P^+$.

Proof. (1) $\widetilde{oa} \circ \tilde{o} \circ \widetilde{ob} \in J \Leftrightarrow a^+ \circ b^+ = \widetilde{oa} \circ \tilde{o} \circ \widetilde{ob} \circ \tilde{o} = \widetilde{ob} \circ \tilde{o} \circ \widetilde{oa} \circ \tilde{o} = b^+ \circ a^+ \Rightarrow a + b = a^+ \circ b^+(o) = b^+ \circ a^+(o) = b + a$.

(2) If $c = \widetilde{oa} \circ \tilde{o} \circ \widetilde{ob}(o)$ then: $\widetilde{oa} \circ \tilde{o} \circ \widetilde{ob} \in A \Leftrightarrow \widetilde{oa} \circ \tilde{o} \circ \widetilde{ob} = \widetilde{oc} \Leftrightarrow a^+ \circ b^+ = \widetilde{oa} \circ \tilde{o} \circ \widetilde{ob} \circ \tilde{o} = \widetilde{oc} \circ \tilde{o} = c^+ \Rightarrow a^+ \circ b^+ = b^+ \circ a^+$ by (1) and since $\widetilde{oa} \circ \tilde{o} \circ \widetilde{ob}(b) = a$ we have $\widetilde{oa} \circ \tilde{o} \circ \widetilde{ob} = \widetilde{ab}$ and so $a \oplus b = \widetilde{ab}(o) = \widetilde{oa} \circ \tilde{o} \circ \widetilde{ob}(o) = a^+(b) = a + b$. □

Proposition 4.3. *Let $\sigma \in \operatorname{Sym} P$, let $o \in P$ and $o' = \sigma(o)$ and let $+ := K_o(P, A)$, $+' := K_{o'}(P, A)$, $\oplus := C_o(P, A)$ and $\oplus' := C_{o'}(P, A)$ then the following statements are equivalent*:

(1) σ *is an* automorphism of (P, A), *i.e.* $\sigma \circ A \circ \sigma^{-1} = A$.
(2) $\forall a, b \in P : \widetilde{\sigma(a)\sigma(b)} = \sigma \circ \widetilde{ab} \circ \sigma^{-1}$.
(3) σ *is an isomorphism between* $(P, +)$ *and* $(P, +')$.
(4) σ *is an isomorphism between* $(P, \oplus)$ *and* $(P, \oplus')$.

Proof. The equivalence of (1)–(3) is proved in [3] and [4]. Since $\sigma(a \oplus b) = \sigma \circ \widetilde{ab}(o) = \sigma \circ \widetilde{ab} \circ \sigma^{-1} \circ \sigma(o)$ and $\sigma(a) \oplus' \sigma(b) = \widetilde{\sigma(a)\sigma(b)}(o') = \widetilde{\sigma(a)\sigma(b)}(\sigma(o))$, σ is an isomorphism between $(P, \oplus)$ and $(P, \oplus')$ if and only if $\sigma \circ \widetilde{ab} \circ \sigma^{-1}(\sigma(o)) = \widetilde{\sigma(a)\sigma(b)}(\sigma(o))$ and this is equivalent with (2) by the regularity of (P, A). □

Remark 3. If we denote by $N(A) := \{\sigma \in \operatorname{Sym} P \mid \sigma \circ A \circ \sigma^{-1} = A\}$ the normalizer of the set A of involutions in $\operatorname{Sym} P$, then by definition of automorphisms of (P, A), $N(A) = \operatorname{Aut}(P, A)$. If A is invariant then $A \subseteq \operatorname{Aut}(P, A)$.

From (4.3) it follows:

Proposition 4.4. *Let (P, A) be a regular invariant involution set, let $o, o' \in P$ be two fixed points, and denote the corresponding K- and C-derivations by $+ := K_o(P, A)$, $+' := K_{o'}(P, A)$, $\oplus := C_o(P, A)$, $\oplus' := C_{o'}(P, A)$, respectively. Then the loops $(P, +)$ and $(P, +')$ and also $(P, \oplus)$ and $(P, \oplus')$, respectively, are isomorphic.*

Proposition (4.1) describes the connections between the loops $(P, +)$ and $(P, \oplus)$ obtained from the regular involution set (P, A) via the derivations in a fixed point $o \in P$ and shows that $(P, \oplus)$ can be obtained from $(P, +)$ and vice versa.

Now we make the further assumption that the regular involution set (P, A) is invariant, then by [2], $(P, +)$ is a K-loop and $\circ(P, +) = P^\circ = A$. Moreover if $o' \in P$ is an other fixed point and $+' := K_{o'}(P, A)$ then $\widetilde{oo'}$ is an isomorphism between $(P, +)$ and $(P, +')$, according to Proposition (4.4).

Conditions which characterize the loops $(P, \oplus)$ derived from an invariant regular involution set have not such a nice form. Clearly if $\oplus' := C_{o'}(P, A)$ then again $\widetilde{oo'}$ is an isomorphism between the commutative loops $(P, \oplus)$ and $(P, \oplus')$ (according to (4.4)).

From the point of view of geometry, the subclass of the invariant regular involution sets (P, A) characterized by the following property is of particular interest: $\forall \alpha \in A : |\operatorname{Fix} \alpha| = 1$.

Then the map
$P \times P \to P; (a, b) \mapsto \operatorname{Fix} \widetilde{ab}$ is surjective
and the map
$P \to A; x \mapsto \tilde{x}$ is a bijection.
If $c := \operatorname{Fix} \widetilde{ab}$ then $\widetilde{ab} = \tilde{c}$ and so we will call the point c the *midpoint* of a and b.

Under this assumption we introduce two ternary relations on the set P:

$$\rho' := \{(a,b,c) \in P^3 \mid \tilde{a} \circ \tilde{b} \circ \tilde{c} \in J\}$$

and

$$\rho := \{(a,b,c) \in P^3 \mid \tilde{a} \circ \tilde{b} \circ \tilde{c} \in \widetilde{P}\}.$$

Both ternary relations are reflexive and symmetric and we have $\rho \subseteq \rho'$.

If we consider the assumption that they are also *transitive*, i.e.

$$\forall\, a,b,c,d \in P,\ \text{if } a \neq b \text{ and } (a,b,c),(a,b,d) \in \rho \text{ then } (b,c,d) \in \rho,$$

and in this case we speak of a *ternary equivalence relation*, then we can distinguish the three following subclasses:

(I) For (P, A) the relation ρ' is an equivalence relation.
(II) For (P, A) the relation ρ is an equivalence relation.
(III) For (P, A) the relations ρ' and ρ are equal and ρ is an equivalence relation.

These classes have their counterparts in the K-loop $(P,+)$ derived in any point o from the regular and invariant involution set (P, A).

If $(P,+)$ is a K-loop we define for any $a \in P^* := P\backslash\{o\}$ the sets $[a]' := \{x \in P \mid a^+ \circ x^+ = x^+ \circ a^+\}$ and $[a] := \{x \in P \mid a^+ \circ x^+ \in P^+\}$. Then, by (4.2.2), $[a] \subseteq [a]'$ and we can state:

Proposition 4.5. *If (P, A) is a regular and invariant involution set, the relation ρ' and ρ, respectively, is a ternary equivalence relation on the set P if and only if the corresponding K-loop $(P,+)$ derived in any point $o \in P$ satisfies the following* exchange condition:

(E′) $\forall a, b \in P^* : b \in [a]' \Rightarrow [a]' = [b]'$,
(E) $\forall a, b \in P^* : b \in [a] \Rightarrow [a] = [b]$, *respectively*.

In particular, it is easy to check that the exchange condition (E) for the K-loop $(P,+)$ is equivalent to the property that for all $a, b, c \in P\backslash\{o\}$, if $a^+ \circ c^+, b^+ \circ c^+ \in P^+$, then $a^+ \circ b^+ \in P^+$.

We close with the remark that in an ordinary absolute geometry the point set P together with the set $\widetilde{P}$ of all point reflections is an invariant regular involution set of the class (III) and that the relation ρ is exactly the collinearity relation of the absolute geometry.

References

[1] R. Capodaglio, Two loops in the absolute plane, Mitt. Math. Ges. Hamburg 23 (1) (2004) 95–104.
[2] H. Karzel, Recent developments on absolute geometries and algebraization by K-loops, Discrete Math. 208, 209 (1999) 387–409.
[3] H. Karzel, S. Pianta, E. Zizioli, Loops, reflection structures and graphs with parallelism, Result. Math. 42 (2002) 74–80.
[4] H. Karzel, S. Pianta, E. Zizioli, From involution sets, graphs and loops to loop-nearrings, in: Proceedings of 2003 Conference on Nearrings and Nearfields, Hamburg, Springer, Berlin, July 27–August 3, 2005, pp. 235–252.
[5] H. Karzel, K. Sörensen, D. Windelberg, Einführung in die Geometrie, Uni-Taschenbücher 184, Göttingen, 1973, ISBN 3-525-03406-7.
[6] H. Kiechle, Theory of K-loops, Lecture Notes in Mathematics, vol. 1778, Springer, Berlin, 2002.
[7] A. Kreuzer, Inner mappings of Bol loops, Math. Proc. Cambridge Philos. Soc. 123 (1998) 53–57.