ELSEVIER

Discrete Mathematics 255 (2002) 161–179

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Co-Minkowski spaces, their reflection structure and K-loops ☆

L. Giuzzi[a,*], H. Karzel[b]

[a] Dipartimento di Matematica e Fisica, Università Cattolica del Sacro Cuore, Via Musei 41, 25121 Brescia, Italy

[b] Zentrum Mathematik, Technische Universität München, D-80290 München, Germany

Received 5 April 1999; received in revised form 9 August 2000; accepted 21 August 2000

Abstract

In this work an infinite family of K-loops is constructed from the reflection structure of co-Minkowski planes and their properties are analysed.

Keywords: K-loops; Reflection structure; Quadratic spaces; Co-Minkowski planes

1. Introduction

In the first part of this work, following [5,6], co-Minkowski planes over a field $\mathbb{K}$ in the sense of [3] are introduced and the idea of quadratic co-Minkowski cone is presented.

In Section 2 it is shown that it is possible, under the assumptions that the field $\mathbb{K}$ has exactly two square classes with -1 non-square, to impose a reflection structure on the (quadratic) cone of a co-Minkowski plane; this structure is proved to be that of a (discrete) symmetric space in the sense of [4] and, according to [2], gives rise to a K-loop, which is proper if $|\mathbb{K}|\geqslant 7$.

In Section 3 the structure of the K-loop thus obtained is studied with the extra provision that 2 is a square in $\mathbb{K}$. This loop is always fibred in subgroups and it is

☆ Research carried out inside the project "Geometries and related algebraic structures" with support from Vigoni programme 1997/98; L. Giuzzi is funded by an I.N.D.A.M scholarship.

* Corresponding author.

E-mail addresses: giuzzi@dmf.bs.unicatt.it, l.giuzzi@sussex.ac.uk (L. Giuzzi), karzel@mathematik.tu-muenchen.de (H. Karzel).

PII: S0012-365X(01)00396-X

shown that it is possible to describe its centraliser structure in a geometric way. The last part of the work is focused on analysing the action of the structure group of the loop on the lines of the cone.

2. Construction of co-Minkowski planes

In this work, [4] has been used as a reference for the theory of quadratic vector spaces.

The following assumptions will be made:

1. $\mathbb{K}$ is a field of odd or zero characteristic;
2. the pair (V, f) is a 3-dimensional quadratic vector space on $\mathbb{K}$;
3. the symbol σ denotes the orthogonality relation induced by f on the subspaces of V, that is, for any $W \leqslant V$

$$W^\sigma := \{x \in V : f(x, y) = 0 \ \forall y \in W\}.$$

2.1. Definitions

According to [5,6], a co-Minkowski plane can be defined as follows.

Definition 1. The symmetric relation $\wr$ is defined on the subspaces of V as: $\forall V_1, V_2 \leqslant V$,

$$V_1 \wr V_2 \ \Leftrightarrow \ \{(0,0,0)\} \notin \{V_1 \cap V_2^\sigma, V_1^\sigma \cap V_2\}.$$

Definition 2. A 5-*tuple* (P, L, I, α, β) is the datum of 5 sets with the following properties:

1. L is a subset of 2^P;
2. I is a symmetric relation in $(P \times L) \cup (L \times P)$;
3. α is a symmetric relation in $L \times L$;
4. β is a symmetric relation in $P \times P$.

Definition 3. Assume now f to be non-trivial. An (i, j)-*metric-projective derivation* of (V, f) is the 5-tuple $(\mathscr{P}\mathscr{L}, I, \perp, \top)$ defined as follows:

- $\mathscr{P}$ is the set of all the i-dimensional subspaces of V;
- $\mathscr{L}$ is the set of all the j-dimensional subspaces of V with $j \neq i$;
- I is the natural incidence relation between elements of $\mathscr{P}$ and $\mathscr{L}$;
- $\perp$ is the $\wr$ relation restricted to $\mathscr{L} \times \mathscr{L}$;
- $\top$ is the $\wr$ relation restricted to $\mathscr{P} \times \mathscr{P}$.

Definition 4. A 5-tuple $\mathfrak{V} = (\mathscr{P}, \mathscr{L}, I, \perp, \top)$ is a *metric-projective coordinate plane* (*mpc plane*) if there exist integers $i, j \in \{1, 2\}$ and a quadratic space (V, f), such that $\mathfrak{V}$ is the (i, j)-metric-projective derivation of (V, f).

The radical and the Witt index of the quadratic space (V, f) will be denoted, respectively, by $\mathrm{Rad}(V)$ and $\mathrm{Ind}_W(V)$.

Definition 5. Let $\mathfrak{V}$ be the mpc plane derived from the quadratic space (V, f) and let $\alpha = \dim \mathrm{Rad}(V)$ and $\beta = \mathrm{Ind}_W(V)$ We will call $\mathfrak{V}$ according to the following table:

(α, β)	(i, j)	
	(1,2)	(2,1)
(0,0)	Elliptic	Elliptic
(0,1)	Hyperbolic	Hyperbolic
(1,0)	co-Euclidean	Euclidean
(1,1)	co-Minkowski	Minkowski
(2,0)	Galilean	Galilean.

Definition 6. A point p of an mpc plane $\mathfrak{V}$ is *isotropic* if $p \top p$.

The name derives from the fact that the isotropic points of $\mathfrak{V}$ are exactly the points arising from the subspaces of V isotropic with respect to the form f.

Definition 7. Let $\mathfrak{V} = (\mathbb{P}, \mathscr{L}, I, \perp, \top)$ be an mpc plane, and let $U \subseteq \mathbb{P}$. The *trace structure of* $\mathfrak{V}$ *along* U is the structure: $(U, \mathscr{L}', I', \perp', \top')$ where

1. $\mathscr{L}' := \{ l \cap U \colon\ l \in \mathscr{L}\ \&\ |l \cap U| \geqslant 2 \}$;
2. I' is the restriction of I to $(U \times \mathscr{L}') \cup (\mathscr{L}' \times U)$;
3. $\perp'$ is defined in $\mathscr{L}' \times \mathscr{L}'$ as, $l' \perp' m'$ if and only if:

$$\exists l, m \in \mathscr{L} \colon\ l \perp m \text{ and } l' = l \cap U,\ m' = m \cap U;$$

4. $\top'$ is the restriction of $\top$ to U.

Definition 8. A *co-Minkowski plane* is the trace structure of a co-Minkowski mpc plane along the set of its non-isotropic points.

2.2. A model

Following [1], it is possible to provide a model of a co-Minkowski plane as follows. The same assumptions as before are taken.

Let $\mathscr{N} := (n_0, n_1, n_2)$ be a fixed ordered basis of V, and consider the quadratic form associated to the matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

with respect to $\mathcal{N}$. The kernel of this quadratic form is the union of the two planes $M_0 := (\mathbb{K}n_2 + \mathbb{K}n_0)$ and $M_1 := (\mathbb{K}n_2 + \mathbb{K}n_1)$, that is

$$f(x,x)=0 \Leftrightarrow x \in M_0 \cup M_1.$$

Hence, it is possible to associate to every point v of $V \setminus (M_0 \cup M_1)$ the reflection $\tilde{v}$ of axis $\mathbb{K}v$. Namely, for any v with $f(v,v) \neq 0, \tilde{v}$ is defined to be the mapping

$$\tilde{v}: \begin{cases} V \to V, \\ x \to -x + 2\frac{f(x,v)}{f(v,v)}v. \end{cases}$$

The following lemma is a standard result in the theory of quadratic forms.

Lemma 1. *For all $v \in V$ such that $f(v,v) \neq 0$ and for all $i \in \mathbb{K}$,*

1. Fix $\tilde{v} = \mathbb{K}v$;
2. Fix $(-\tilde{v}) = \{v\}^{\sigma}$;
3. $\tilde{v}^2 = id$;
4. $\widetilde{\lambda v} = \tilde{v}$ if $\lambda \neq 0$.
5. $\tilde{v}(M_1) = M_0$;
6. $\tilde{v} \in \mathrm{O}(V,q)$;
7. $\forall \sigma \in \mathrm{O}(V,q)$ *we have* $\sigma \tilde{v} \sigma^{-1} = \widetilde{\sigma(v)}$;
8. $x \in V^{(i)} \leftrightarrow \tilde{v}(x) \in V^{(i)}$.

For any $i \in \mathbb{K} \setminus \{0\}$, define $\mathbb{K}^{(i)}$ to be the set of all the elements of $\mathbb{K}$ in the same square class of i, that is

$$\mathbb{K}^{(i)} := \{t \in \mathbb{K}\colon\ \exists x \in \mathbb{K} \text{ such that } t = ix^2\}$$

and let, for any vector space V over $\mathbb{K}$

$$V^{(i)} := \{x \in V\colon\ f(x,x) \in \mathbb{K}^{(i)}\}.$$

The set $\mathbb{K}^{(0)}$ is defined accordingly to be $\{0\}$ and, likewise, $V^{(0)} := \{x \in V\colon f(x,x) = 0\}$.

Let $(\mathbb{P}, \mathcal{R})$ be the projective derivation of V, that is the linear space having as point set

$$\mathbb{P} := \frac{V^{\star}}{\mathbb{K}^{\star}}$$

and as set of lines

$$\mathcal{R} := \{\pi(W^{\star})\colon\ W \leqslant V; \dim W = 2\}.$$

Let also $\pi: V^{\star} \to \mathbb{P};\ x \to \mathbb{K}^{\star}x$ be the usual projection map.

All the $V^{(i)}$'s are homogeneous sets and, if $i \neq 0$, they do not contain $(0,0,0)$. Hence, the structure of the quadratic classes can be carried onto the projective plane.

Definition 9. Let V be any vector space over $\mathbb{K}$ and let $i \in \mathbb{K}$. Then,
- for $i \neq 0$

$$\mathbb{P}^{(i)} := \pi(V^{(i)});$$

- otherwise

$$\mathbb{P}^{(0)} := \pi(V^{(0)} \setminus \{(0,0,0)\}).$$

By Lemma 1 we have:

Lemma 2. *The reflection mapping* $\tilde{}$ *is compatible with the projection* π, *in the sense that*

$$\hat{}: \begin{cases} \mathbb{P}\setminus\mathbb{P}^{(0)} \to \mathrm{Aut}(\mathbb{P},\mathscr{R}) \\ \pi(v) \to \widehat{\pi(v)} : \begin{cases} \mathbb{P} \to \mathbb{P}, \\ \pi(x) \to \pi(\tilde{v}(x)). \end{cases} \end{cases}$$

is well defined.

The following notation will be used:

$$N := \pi(M_0 \cap M_1 \setminus \{(0,0,0)\}),$$

$$\mathbb{P}^M := \bigcup_{i \in \mathbb{K}^\star} \mathbb{P}^{(i)}.$$

We will also write $\mathscr{R}^M, \mathscr{R}^{(i)}$ and $\mathscr{R}^0$ for the sets of lines obtained as trace structures of the projective plane $(\mathbb{P},\mathscr{R})$ along, respectively, the sets $\mathbb{P}^M, \mathbb{P}^{(i)}$ and $\mathbb{P}^0$.

The triple $(\mathbb{P}^M, \mathscr{R}^M, \hat{}|_{\mathbb{P}^M})$ presents the same incidence structure as the co-Minkowski plane induced by f and $\hat{}|_{\mathbb{P}^M}$ is 'compatible' with the metric structure of the latter in the following sense:

- $\forall x, y, t \in \mathbb{P}^M:\ x \top y \leftrightarrow \hat{t}(x) \top \hat{t}(y)$;
- $\forall t \in \mathbb{P}^M:\ \mathrm{Fix}\, \hat{t} = \{p : t \top p\} \cup \{t\}$.

In the language of [6] any line L of $\mathscr{R}^M$ is called *radical* if and only if

$$\forall S \in \mathscr{R}^M:\ S \perp L.$$

The previous statement amounts to ask that the image of the radical of the vector space (V, f) belongs to a radical line; thus, it follows that the set of all radical lines of $\mathfrak{M}$ is exactly

$$\{L \in \mathscr{R}^M:\ L \cup \{N\} \in \mathscr{R}\}.$$

This implies that, given any point $p \in \mathbb{P}^M$, there exists exactly one radical line in $(\mathbb{P}^M, \mathscr{R}^M, \hat{})$ passing through it; such a line will be denoted by the symbol $\overline{p, N}$.

2.3. Co-Minkowski cones

Since by Lemma 1, point (8), for any $p \in \mathbb{P}^M$ and for any $i \in \mathbb{K}^\star$ the restriction of $\hat{p}$ to $\mathbb{P}^{(i)}$ is a permutation of $\mathbb{P}^{(i)}$, it is possible to state the definition that follows:

Definition 10.

- a *co-Minkowski cone* is any triple $(\mathbb{P}^{(i)}, \mathscr{R}^{(i)}, \hat{}|_{\mathbb{P}^{(i)}})$ with $i \in \mathbb{K}^\star$;
- the triple $(\mathbb{P}^{(1)}, \mathscr{R}^{(1)}, \hat{}|_{\mathbb{P}^{(1)}}) =: (\mathbb{P}^+, \mathscr{R}^+, \hat{}|_{\mathbb{P}^+}$ is called *quadratic co-Minkowski cone*.

Definition 11. The trace of a radical line of $(\mathbb{P}^M, \mathscr{R}^M)$ along the set $\mathbb{P}^{(i)}$ is a *long* line of the cone $(\mathbb{P}^{(i)}, \mathscr{R}^{(i)}, \hat{}|_{\mathbb{P}^{(i)}})$; the trace of a non-radical line is called a *short* line.

From now on, the following extra assumptions will be made on $\mathbb{K}$:

1. there are only two square classes in $\mathbb{K}$;
2. -1 is a non-square in $\mathbb{K}$,

that is

$$\mathbb{K} := \mathbb{K}^{(1)} \dot{\cup} \{0\} \dot{\cup} \mathbb{K}^{(-1)}.$$

Remark. If $\mathbb{K}$ is finite the existence of two square classes is immediate and the condition that -1 is a non-square is equivalent to ask $|\mathbb{K}| \not\equiv 1 (\mathrm{mod}\, 4)$.

Our main concern will be with what happens in the quadratic co-Minkowski cone; however, all the geometric constructions can be applied also to $(\mathbb{P}^{(-1)}, \mathscr{R}^{(-1)}, \hat{}|_{\mathbb{P}^{(-1)}})$.

In order to simplify the notation, where no confusion is expected to arise, the restriction $\hat{}|_{\mathbb{P}^+}$ will be written simply as $\hat{}$.

3. The reflection structure

If $t \in \mathbb{K}^{(1)}$, then there exists exactly two square roots $r_1, r_2 \in \mathbb{K}$ of t with $r_1 = -r_2$. By the assumptions that -1 is a non-square in $\mathbb{K}$ and that there are no more than two square classes, one of the r_i's is always a square.

The symbol $\sqrt{t}$ will be used for denoting the solution of the equation $x^2 - t = 0$ that is a square.

3.1. Canonical representations

It is possible to provide a canonical representation of the points of the cone $\mathbb{P}^+$. This, done in the following lemma, is aimed at simplifying successive computations.

Lemma 3. *Let* $p = \mathbb{K}^\star(a, b, c)$ *be a point of* $\mathbb{P}^+$, *and suppose* 2 *to be a square in* $\mathbb{K}$. *Then there exists a unique* $(\alpha, \beta) \in \mathbb{K}^{(1)} \times \mathbb{K}$ such that

$$(\alpha, \alpha^{-1}, \beta) \in \mathbb{K}^\star(a, b, c).$$

On the other hand, if $p = K^\star(a, a^{-1}, c)$, *for any* $a, c \in \mathbb{K}$, *then* $p \in \mathbb{P}^+$.

Proof. By hypothesis, $\mathbb{K}^{(1)} = \mathbb{K}^{(2)}$. Since $p \in \mathbb{P}^+$, then $q(p) := f(p,p) = 2ab \in \mathbb{K}^{(2)}$ and, from the latter, $ab \in \mathbb{K}^{(2)}$. If $a \in \mathbb{K}^{(1)}$, let $p' := (1/\sqrt{ab})(a,b,c)$; otherwise define $p' = -(1/\sqrt{ab})(a,b,c)$. Then $\mathbb{K}^\star p' = \mathbb{K}^\star(a,b,c)$, and p' satisfies the required properties. The inverse is an immediate consequence of the fact that $aa^{-1} = 1 \in \mathbb{K}^{(1)}$. $\square$

For the rest of this work, 2 will be assumed to be a square in $\mathbb{K}$; the points of $\mathbb{P}^+$ will also be always denoted by their canonical representatives.

The reflection $\hat{p}(x)$ can be described in the following way, using the canonical representation:

$$\begin{aligned}
\hat{p}(x) &= \widehat{(p_0, p_0^{-1}, p_2)}(x_0, x_0^{-1}, x_2) \\
&= -(x_0, x_0^{-1}, x_2) + (p_0 x_0^{-1} + p_0^{-1} x_0)(p_0, p_0^{-1} p_2) \\
&= (-x_0 + p_0^2 | x_0^{-1} + x_0, -x_0^{-1} + x_0^{-1} + p_0^{-2} x_0, p_2 p_0 x_0^{-1} + p_2 p_0^{-1} x_0 - x_2) \\
&= \left(\frac{p_0^2}{x_0}, \frac{x_0}{p_0^2}, -x_2 + p_2 \frac{p_0^2 + x_0^2}{p_0 x_0} \right).
\end{aligned}$$

3.2. Operation construction

Let o be the point $(1,1,0)$ of $\mathbb{P}^+$.

Lemma 4. *For all $x = (x_0, x_0^{-1}, x_2) \in \mathbb{P}^+$ there exists one and only one $p \in \mathbb{P}^+$ such that $\hat{p}(x) = o$.*

Proof. By construction x_0 can be taken as a square.

From the description of $\hat{p}$, the following relation has to be satisfied:

$$\left(\frac{p_0^2}{x_0}, \frac{x_0}{p_0^2}, -x_2 + p_2 \frac{p_0^2 + x_0^2}{p_0 x_0} \right) = (1,1,0),$$

whence, since $x_0 \neq 0$

$$\frac{p_0^2}{x_0} = 1 \leftrightarrow p_0 = \sqrt{x_0},$$

$$p_2 = x_2 \frac{x_0 \sqrt{x_0}}{x_0 + x_0^2} = x_2 \frac{\sqrt{x_0}}{1 + x_0}.$$

This proves the lemma. $\square$

Since $\hat{v}$ can be seen as a reflection of centre v in $\mathbb{P}^+$, the previous lemma is actually a definition of *the* 'mid point' between any point $p \in \mathbb{P}^+$ and the fixed point o.

Definition 12. Let $o := (1,1,0) \in \mathbb{P}^+$. For all $p \in \mathbb{P}^+$, let $p' \in \mathbb{P}^+$ be the unique point such that $\hat{p}'(o) = p$. The mapping $p_+ : \mathbb{P}^+ \to \mathbb{P}^+$ is defined as the one that for any $x \in \mathbb{P}^+$ acts as

$$p_+(x) := \hat{p}'\hat{o}(x).$$

For any $a, b \in \mathbb{P}^+$, we also define their 'sum' as

$$a + b := a_+(b).$$

Observe that in general $a + b \neq b + a$.

Lemma 5. *For all $a \in \mathbb{P}^+$, it is true that $a + o = o + a = a$.*

Proof. On the left-hand side the computation of $o + a$ yields

$$o + a = o_+(a) = \hat{o}\hat{o}(a) = \mathrm{id}(a) = a$$

on the other side, $a + o$ is

$$a + o = \hat{a}'\hat{o}(o) = \hat{a}'(o) = a.$$

The result follows. $\square$

The following theorem provides an explicit formula for computing the operation $+$ between two points given in canonical form.

Theorem 6. *Let a, b be two points of $\mathbb{P}^+$. Then the point $a + b$ has as representative*

$$a + b = \left(a_0 b_0, \frac{1}{b_0 a_0}, b_2 + a_2 \frac{a_0 b_0 + 1/b_0}{1 + a_0} \right).$$

Proof. We know by Lemma 4 that

$$a' = \left(\sqrt{a_0}, \frac{1}{\sqrt{a_0}}, a_2 \frac{\sqrt{a_0}}{1 + a_0} \right)$$

and that

$$\hat{o}(b) = \left(\frac{1}{b_0}, b_0, -b_2 \right).$$

Hence,

$$a + b := \hat{a}'\hat{o}(b) = \left(a_0 b_0, \frac{1}{b_0 a_0}, b_2 + a_2 \frac{\sqrt{a_0}}{1 + a_0} \left(a_0 + \frac{1}{b_0^2} \right) \frac{b_0}{\sqrt{a_0}} \right)$$

$$= \left(a_0 b_0, \frac{1}{a_0 b_0}, b_2 + a_2 \frac{a_0 b_0 + 1/b_0}{1 + a_0} \right). \qquad \square$$

By using this formula it is possible to consider when the operation is associative. Indeed,

$$a+(b+c)=\left(a_0b_0c_0,\frac{1}{a_0b_0c_0},c_2+b_2\frac{b_0c_0+1/c_0}{1+b_0}+a_2\frac{a_0b_0c_0+1/b_0c_0}{1+a_0}\right),$$

while

$$(a+b)+c=\left(a_0b_0c_0,\frac{1}{a_0b_0c_0},c_2+\left(b_2+a_2\frac{a_0b_0+1/b_0}{1+a_0}\right)\frac{a_0b_0c_0+1/c_0}{1+a_0b_0}\right),$$

whence it follows

$$\begin{aligned}
&((a+b)+c)-(a+(b+c))\\
&=\left(0,0,b_2\frac{b_0c_0+1/c_0}{1+b_0}+a_2\frac{a_0b_0c_0+1/b_0c_0}{1+a_0}\right.\\
&\quad\left.-\left(b_2+a_2\frac{a_0b_0+1/b_0}{1+a_0}\right)\frac{a_0b_0c_0+1/c_0}{1+a_0b_0}\right)\\
&=\left(0,0,b_2\left(\frac{b_0c_0+1/c_0}{1+b_0}-\frac{a_0b_0c_0+1/c_0}{1+a_0b_0}\right)\right.\\
&\quad\left.+a_2\frac{(a_0b_0c_0+1/b_0c_0)(1+a_0b_0)-(a_0b_0+1/b_0)(a_0b_0c_0+1/c_0)}{(1+a_0)(1+a_0b_0)}\right)\\
&=\left(0,0,b_2\frac{b_0c_0(1-a_0)+b_0((a_0-1)/c_0)}{(1+b_0)(1+a_0b_0)}\right.\\
&\quad\left.+a_2\frac{a_0b_0c_0-a_0c_0+a_0((1-b_0)/c_0)}{(1+a_0)(1+a_0b_0)}\right)\\
&=\left(0,0,b_0b_2(1-a_0)\frac{c_0-1/c_0}{(1+b_0)(1+a_0b_0)}\right.\\
&\quad\left.-a_0a_2(1-b_0)\frac{c_0-1/c_0}{(1+a_0)(1+a_0b_0)}\right)\\
&=\left(0,0,\frac{(b_0b_2(1-a_0)(1+a_0)-a_0a_2(1-b_0)(1+b_0))(c_0-1/c_0)}{(1+a_0)(1+b_0)(1+a_0b_0)}-\right)\\
&=\left(0,0,\frac{c_0-1/c_0}{(1+a_0)(1+b_0)(1+a_0b_0)}(b_0b_2(1-a_0^2)-a_0a_2(1-b_0^2))\right).
\end{aligned}$$

If an ordered triple $(a,b,c)\in\mathbb{P}^{+3}$ is said to *associate* whenever $a+(b+c)=(a+b)+c$, it is possible to synthesize the previous computation in the following lemma.

Lemma 7. *A triple* $(a,b,c)\in\mathbb{P}^{+3}$ *associates if and only if either one of the following two conditions is satisfied*:

1. $c_0=\frac{1}{c_0}$ *that is* $c_0=1$;
2. $b_0b_2(1-a_0^2)=a_0a_2(1-b_0^2)$.

An immediate consequence of Lemma 7 is that in general '$+$' is non-associative; hence, $(\mathbb{P}^+,+)$ is not a group.

Lemma 8. *For any* $c\in\mathbb{P}^+$, *there exists one and only one* $b\in\mathbb{P}^+$ *such that*:

$$c+b=b+c=o.$$

Such an element b *will be written as* $-c$.

Proof. In order for b to be a right inverse of a, it has to satisfy

1. $a_0b_0=1\leftrightarrow a_0=b_0^{-1}$,

2r. $b_2+a_2\frac{a_0b_0+1/b_0}{1+a_0}=0\leftrightarrow b_2=-a_2\frac{1+a_0}{1+a_0}\leftrightarrow b_2=-a_2$.

If it is a left inverse, on the other hand, it has to be such that

1. $a_0b_0=1\leftrightarrow a_0=b_0^{-1}$,

2l. $a_2+b_2\frac{a_0b_0+1/a_0}{1+b_0}=0\leftrightarrow a_2=-b_2\frac{1+b_0}{1+b_0}\leftrightarrow a_2=-b_2$.

The lemma follows by comparing the conditions 21 and 2r. □

3.3. Loops

Definition 13. An algebraic structure $(L,+)$ is called a *loop* if the following conditions hold true:

1. $\exists o\in L$: $\forall a\in L$: $a+o=o+a=a$;
2. $\forall a,b\in L$: $\exists!(x,y)\in L^2$ such that: $\begin{cases} a+x=b,\\ y+a=b.\end{cases}$

A loop is *proper* if it is not a group.

If a loop is proper, we shall write $-a$ for the only solution of the equation $x+a=o$, while a^- will indicate the solution of $a+x=o$.

Definition 14. Let $(L,+)$ be a loop; for any $a\in L$ consider the mapping

$$a^+:\begin{cases} L\to L,\\ x\to a+x.\end{cases}$$

Define now $\delta_{a,b}$ to be, for any two elements $a,b\in L$,

$$\delta_{a,b}:=\begin{cases} L\to L,\\ x\to\delta_{a,b}(x):=(((a+b)^+)^{-1}a^+b^+)(x).\end{cases}$$

The $\delta_{a,b}$'s measure how much a loop is not a group.

Definition 15. The structure group $\varDelta$ of a loop $(L,+)$ is the group generated by all the $\delta_{a,b}$'s as $a,b\in L$.

Definition 16. A loop $(L,+)$ is a *K-loop* if the following are satisfied:

1. $\forall a,b\in L$: $\delta_{a,b}\in \mathrm{Aut}(L,+)$,
2. $(-a)+(-b)=-(a+b)$ (automorphic inverse property),
3. $\delta_{a,b}=\delta_{a,b+a}$.

Observe that if a K-loop is a group, then, by (2), it is commutative.

From the Lemma 1, points (5) and (6) and the Lemma 2 it is possible to deduce the following result.

Lemma 9. *For all $a,b\in\mathbb{P}^+$,*

$$\widehat{a(b)}=\hat{a}\hat{b}\hat{a}.$$

With this remark it is possible to prove the main theorem of this section.

Theorem 10. *The algebraic structure $(\mathbb{P}^+,+)$ is a proper K-loop.*

Proof. From Lemmas 5 and 8 it follows that $(\mathbb{P}^+,+)$ is at least a loop.

By [2], the condition in Lemma 9 is enough to prove that a loop is indeed a K -loop, whence the result. □

The smallest example under our assumptions, is provided when starting from the field $\mathbb{K}=\mathrm{GF}(7)$; this produces a proper K-loop of 21 elements.

It is however worthwhile to remark that so far no finiteness hypothesis has been necessary. In fact, if $\mathbb{K}$ is finite the only conditions that have been used are:

1. -1 non-square, [1]
2. 2 square.

Thus we have actually provided an example of an infinite family of finite K-loops.

Remark. For any triple p,q,x the δ's can be written explicitly as

$$\delta_{p,q}(x) := \left(x_0,\frac{1}{x_0},x_2+q_2\frac{q_0x_0+1/x_0}{1+q_0}+p_2\frac{p_0q_0x_0+1/q_0x_0}{1+p_0}\right.$$
$$\left.+\left(x_0+\frac{1}{p_0q_0x_0}\right)\frac{-q_2-p_2(p_0q_0+(1/q_0)/(1+p_0))}{1+1/q_0p_0}\right).$$

[1] This yields that the characteristic has to be odd, since it implies $\mathbf{1}\neq-\mathbf{1}$.

It follows that every $\delta_{p,q}$ acts as the identity on the first two components of any point p. Since the quadratic form q depends only on these components, it follows that all the δ's preserve orthogonality as well.

4. The line structure

In this section, $(\mathbb{P}^+,+)$ will be assumed to be a K-loop, constructed from a co-Minkowski cone as presented before.

Aim of this section is to show the interplay between the algebraic properties of the loop and the geometry of the structure $(\mathbb{P}^+,\mathscr{R}^+,\hat{\ })$.

For every $b=(b_0,1/b_0,b_2)\in\mathbb{P}^+$ define the *centraliser* of b to be the set

$$Z(b):=\{x\in\mathbb{P}^+:\ x+b=b+x\}.$$

Let also

$$Z(b):=\{x\in\mathbb{P}^+:\ x+b=b+x\}.$$

Let also

$$Z_1(b):=\{(1/b_0,b_0,t):\ t\in\mathbb{K}\}$$

and

1. for $b_0\neq 1$,

$$Z_2(b):=\left\{L(b,t):\ t\in\mathbb{K}^2,\ \text{where } L(b,t):=\left(t,1/t,\frac{(t^2-1)}{t}g(b)\right),\right.$$
$$\left. g(b):=\frac{b_2b_0}{(b_0^2-1)}\right\};$$

2. for $b_0=1$,

$$Z_2(b)=\{-b\}.$$

Theorem 11. *For any* $b\in\mathbb{P}^+$:

$$Z(b)=Z_1(b)\cup Z_2(b)$$

and

$$Z_1(b)\cap Z_2(b)=\{(-b)\}.$$

Now let b be a point with $b_0\neq 1$, and consider the equation of the line between a point of the form $b_{(t)}=L(b,t)$, for some $t\in\mathbb{K}^{(2)}$, and o. Let p be a generic point on $\overline{o,b_{(t)}}\setminus\{o\}$. After a normalisation, such a point can be written in the form

$$p=R(b,t,\mu):=\left[\sqrt{\frac{(\mu+t)t}{\mu t+1}},\sqrt{\frac{\mu t+1}{(\mu+t)t}},\frac{(t^2-1)b_2b_0}{\sqrt{\mu+t}\sqrt{\mu t+1}\sqrt{t}(b_0^2-1)}\right],$$

where μ is a parameter that varies in the set

$$D(t):=\left\{\mu\in\mathbb{K}:\ \frac{\mu+t}{\mu t+1}\in\mathbb{K}^{(2)}\right\}.$$

We claim that as μ varies in $D(t)$, the first component of $R(b,t,\mu)$ assumes all possible values for a point of $\mathbb{P}^{+}$. In fact, the relation

$$\frac{(\mu+\alpha)\alpha}{\mu\alpha+1}=\beta$$

makes sense only when $\mu\neq -1/\alpha$. Indeed, when $\mu=-1/\alpha$, the second coordinate of the point $p=R(b,t,\mu)$ would be zero, against the assumption $p\in\mathbb{P}^{+}$. Moreover, since

$$(\mu+\alpha)\alpha=\beta(\mu\alpha+1)\leftrightarrow\mu\alpha(1-\beta)=\beta-\alpha^2\leftrightarrow\mu=\frac{\beta-\alpha^2}{\alpha(1-\beta)},$$

the before mentioned relation can be solved for all $\alpha\in\mathbb{K}^{(2)},\beta\in\mathbb{K}$, with $\beta\neq 1$.

On the other hand, $\beta=1$ corresponds to the only point on the line that has the first two components equal to 1, that is o, against the hypothesis.

The symbol $R(b,t,\mu)_0$ will be used in order to denote the first component of the vector $R(b,t,\mu)$. Consider now the point $L(b,R(b,t,\mu)_0)$.

After a formal substitution, the formula becomes

$$L(b,R(b,t,\mu)_0)=\left(\sqrt{\frac{\mu+t}{\mu+1/t}},\left(\sqrt{\frac{\mu+t}{\mu+1/t}}\right)^{-1},\right.$$
$$\left.\frac{((\mu+t)/(\mu+1/t)-1)b_2b_0}{\sqrt{(\mu+t)/(\mu+1/t)}(b_0-1)(1+b_0)}\right).$$

The first two components are by construction the same as those of the point $R(b,t,\mu)$; we claim that also $R(b,t,\mu)_2=L(b,R(b,t,\mu)_0)_2$. In fact, this is the same as to verify the relation

$$\frac{((\mu+t)/(\mu+1/t)-1)b_2b_0}{\sqrt{(\mu+t)/(\mu+1/t)}(b_0-1)(1+b_0)}-\frac{(t^2-1)b_2b_0}{\sqrt{(\mu+t)(\mu+1/t)t}(b_0-1)(b_0+1)}=0$$

to be identically satisfied.

Given that

$$\frac{(t^2-1)b_2b_0}{\sqrt{(\mu+t)(\mu+1/t)t}(b_0-1)(b_0+1)}$$
$$=\frac{(t-1/t)b_2b_0}{\sqrt{(\mu+t)/(\mu+1/t)}(b_0-1)(b_0+1)(\mu+1/t)},$$

the previous equation simplifies to

$$\left(\frac{(\mu+t)}{(\mu+1/t)}-1\right)=\frac{(t-1/t)}{\mu+1/t}$$

and the latter is true for all allowed values of μ, t, b_0 and b_2.

Finally, since for any given t', as μ varies in $D(t'), R(b,t,\mu)_0$ assumes all the possible values among the squares of $\mathbb{K}$,

$$Z_2(b)=\{R(b,t',\mu):\ \mu\in D(t')\}\cup\{o\}=\overline{b,o}\cap\mathbb{P}^+.$$

On the other hand, the set $Z_1(b)$ is a line of $\mathbb{P}^+$ passing through $-b$, and, by considering that the radical N of the quadratic form f is the class $[(0,0,1)]$, it follows that $Z_1(b)$ is, in fact, the line $\overline{-b,N}$ of the co-Minkowski cone.

Theorem 12. *For any $b\in\mathbb{P}^+$ with $b_0\neq 1$, the set $Z_2(b)$ is an Abelian group isomorphic to the multiplicative group of the squares of $\mathbb{K}$; if $b_0=1$, then $Z_1(b)$ is also an Abelian group, isomorphic to the additive group of $\mathbb{K}$.*

Proof. If $m,n\in Z_2(b)$, then there exist $t_1,t_2\in\mathbb{K}^{(2)}$ such that

$$m=(t_1,1/t_1,L(b,t_1)),\quad n=(t_2,1/t_2,L(b,t_2)).$$

If $o\in\{m,n\}$, then $m+n\in\{m,n\}\subseteq Z_2(b)$.

Suppose $o\notin\{m,n\}$. Since $Z_2(b)$ is the line $\overline{o,b}$,

$$\{m,n\}\subseteq Z_2(b)=\overline{o,b}\leftrightarrow Z_2(m)=\overline{o,m}=\overline{o,b}=\overline{o,n}=Z_2(n).$$

It follows:

$$m+n=n+m.$$

Moreover,

$$L(b,t_1t_2)=L(b,t_2)+L(b,t_1)\frac{t_1t_2+1/t_2}{1+t_1}$$

implies

$$\begin{aligned}m+n&=\left(t_1t_2,\frac{1}{t_1t_2},L(b,t_2)+L(b,t_1)\frac{t_1t_2+1/t_2}{1+t_1}\right)\\&=(t_1t_2,L(b,t_1t_2))\in Z_2(b).\end{aligned}$$

On the other hand, $Z_2(b)$ is closed under composition and contains o; hence, it must be an *Abelian* sub-K-loop of $(\mathbb{P}^+,+)$, whence we deduce that it is a group.

The first part of the theorem now follows from the fact that the projection

$$\psi_b:\begin{cases}Z_2(b)\to\mathbb{K}^{(2)},\\ (x_0,\frac{1}{x_0},x_2)\to x_0\end{cases}$$

is a group isomorphism.

If $b_0=1$, then $Z_1(b)=\{(1,1,t):\ t\in\mathbb{K}\}$, that immediately implies that $Z_1(b)\simeq(\mathbb{K},+)$, whence the second part of the thesis. □

Definition 17. A loop $(L,+)$ is *fibred in sub-groups* if and only if there exists a set $\mathscr{F}$ such that:

1. $\forall X\in\mathscr{F}:\ X\subseteq L$ is a non-trivial group;
2. $L\notin\mathscr{F}$;
3. $\forall t\in L\setminus\{o\}, \exists! X\in\mathscr{F}:\ t\in X$.

The elements of $\mathscr{F}$ will be called *fibres* of the loop.
Theorem 12 can be restated as follows.

Theorem 13. *The loop* $(\mathbb{P}^+,+)$ *is fibred in subgroups, the fibres being the lines* $\overline{o,p}$, *for* $p\in\mathbb{P}^+\setminus\{o\}$.

Assume now $\mathbb{K}$ to be a finite field GF(q) with q odd. Half of its non-zero elements are squares; hence, for any $b\in\mathbb{P}^+$ different form o the following cardinalities can be computed:

$$|\overline{o,N}|=|\overline{-b,N}|=q,$$

$$|\overline{b,o}|=\frac{q-1}{2}.$$

Lemma 14. *Given any point* $p\in\mathbb{P}^+$, *there are exactly* $q+1$ *lines of* $(\mathbb{P}^+,\mathscr{R}^+)$ *it belongs to.*

Proof. The order of p in $\mathbb{P}$ is $q+1$; and this provides an upper bound for its order in the trace structure $\mathbb{P}^+$.
Suppose first $p_0\neq 1$, and consider the line

$$\overline{o,N}:=\{(1,1,t):\ t\in\mathbb{K}\}.$$

By construction, $p\notin\overline{o,N}$ and $|\overline{o,N}|=q$. On the other hand, since $(\mathbb{P}^+,\mathscr{R}^+)$ is a linear space, that there are exactly q lines through a intersecting $\overline{o,N}$.
Let U,W be the two lines in $\mathscr{R}$ such that $\overline{p,N}\subseteq U$ and $\overline{o,N}\subseteq W$. Then $U\cap W=\{N\}\notin\mathbb{P}^+$, and the line $\overline{p,N}$ of $\mathbb{P}^+$ is not one of those counted before. The consequence of this argument is that there are at least $q+1$ lines of $\mathbb{P}^+$ passing through p, and the theorem follows.
Exactly, the same technique can be used in the case $p_1=1$, by just replacing $\overline{o,N}$ with $\overline{q,N}$, with $q\notin\overline{o,N}$. □

Corollary 15. *Let* $p\in\mathbb{P}^+$, *and suppose* R *to be a line of* $\mathbb{P}^+$ *such that* $p\in R$ *and* $R\neq\overline{p,N}$. *Then for all* $r\in\mathbb{P}^+$:

$$\overline{r,N}\cap R\neq\emptyset.$$

Proof. If $p\in\overline{r,N}$, the corollary is trivial. If $p\notin\overline{r,N}$, then there are exactly q distinct lines through p incident with $\overline{r,N}$. It follows that there is only one more line through p, and that has to be $\overline{p,N}$, not incident with $\overline{r,N}$ in $\mathbb{P}^+$. By hypothesis, $R\neq\overline{p,N}$; hence, R has to belong to the set of the lines incident with $\overline{r,N}$. □

The following lemma is of more interest.

Lemma 16. *For any point $a\in\mathbb{P}^+$, the only line of $\mathscr{R}^+$ through it with q points is the radical one, that is $\overline{a,N}$, all the others having cardinality $(q-1)/2$.*

Proof. Let R be a line through a different from $\overline{a,N}$. By the previous corollary, R intersects all the lines of the form $\overline{p,N}$ for any $p\in\mathbb{P}^+$. Since each of those lines has cardinality q,

$$|R|q=|\mathbb{P}^+|.$$

On the other hand,

$$|\mathbb{P}^+|=q\frac{q-1}{2},$$

whence the thesis. □

Define, for any $a\in\mathbb{P}^+$

$$\Delta_a:=\{\delta_{a,b}:\ b\in\overline{o,N}\}.$$

Lemma 17. *For any $a\in\mathbb{P}^+$: Δ_a is a group, isomorphic to $\overline{o,N}$, that is $(\mathbb{K},+)$.*

Proof. Let $b,c\in\overline{o,N}$. By direct computation,

$$\begin{aligned}\delta_{a,b}\delta_{a,c}(x)=\Bigg(&x_0,1/x_0,x_2+\frac{x_0+1/x_0}{2}(b_2+c_2)+a_2\frac{a_0x_0+1/x_0}{1+a_0}\\&-(b_2+c_2+a_2)\frac{x_0+1/a_0x_0}{1+1/a_0}\Bigg)\\&=\delta_{a,(1,1,b_2+c_2)}(x)=\delta_{a,b+c}(x),\end{aligned}$$

that proves the thesis. □

Lemma 18. *Given $a,c\in\mathbb{P}^+\backslash\overline{o,N}$, there exists exactly one $b\in\overline{o,N}$ such that*

$$\overline{o,c}=\delta_{a,b}(\overline{o,a}).$$

Proof. Let $\mathfrak{O}'$ be the set of all the lines through o different from $\overline{o,N}$.

Since the point b can, by hypothesis, be represented as $(1,1,b_2)$, it is possible to write $\delta_{a,b}$ as

$$\delta_{a,(1,1,b_2)}(a)=\left[\left(a_0,\frac{1}{a_0},-\frac{1}{2}\frac{b_2a_0^2-2b_2a_0-2a_2a_0+b_2}{a_0}\right)\right].$$

The $\delta_{a,b}$'s are all collineations of $\mathbb{P}^+$. Since the element o is the identity of the loop $(\mathbb{P}^+,\cdot)$, it is fixed by any of the δ's; moreover, the formula for $\delta_{a,b}$ implies that $a\notin\overline{o,N}$ causes $\delta_{a,b}(a)\notin\overline{o,N}$. Hence, given $\eta\in\Delta_a$ and $L\in\mathfrak{O}'$, then $\eta(L)\in\mathfrak{O}'$. The latter can be expressed by saying that Δ_a is a group that acts in a natural way on the set $\mathfrak{O}'$.

In order to prove the lemma it is now enough to verify the regularity of the group Δ_a on $\mathfrak{O}'$. This property is equivalent to prove that, for any element $\overline{o,a}=:L\in\mathfrak{O}'$, the application

$$\sigma_L:\begin{cases}\Delta_a\to\mathfrak{O}',\\ \delta_{a,b}\to\delta_{a,b}L\end{cases}$$

is bijective.

The injectivity is a consequence of the fact that from

$$b_2a_0^2-2b_2a_0-2a_2a_0+b_2=b_2'a_0^2-2b_2'a_0-2a_2a_0+b_2'$$
$$\Leftrightarrow(b_2-b_2')(a_0^2-2a_0+1)=0,$$

it follows $b_2=b_2'$ or $(a_0-1)^2=0$, that is $a_0=1$ or $b'=b$, and the case $a_0=1$ implies $a\in\overline{o,N}$, against the hypothesis.

Surjectivity can be seen by just looking at the third component of b, given that there are no restrictions on b_2. □

In the previous proof the following result has been obtained as well.

Corollary 19. *For all $a\in\mathbb{P}^+$, $b\in\overline{o,N}$*

$$\delta_{a,b}(a)\in\overline{a,N}.$$

Lemma 20. *For any line $L=\overline{a,N}$, different from $\overline{o,N}$*

$$\Delta_L:=\{\delta_{a,b}:\ a\in L,b\in\overline{o,N}\}$$

is an Abelian group isomorphic to $\overline{o,N}$, acting regularly on the set $\mathfrak{O}'$. Moreover, $\Delta_L=\Delta_a$ for any $a\in L$.

Proof. Let $\mathfrak{O}'$ be as in Lemma 18.

For any $a,c\in\mathbb{P}^+,b\in\overline{o,N}$,

$$\delta_{a,b}(c)=\left(c_0,\frac{1}{c_0},-\frac{1}{2}\frac{-2c_2c_0-2c_2c_0a_0-b_2c_0^2+b_2a_0c_0^2+b_2-b_2a_0}{c_0(1+a_0)}\right)$$

and similarly,

$$\delta_{c,b}(c) = \left(c_0, \frac{1}{c_0}, -\frac{1}{2}\frac{b_2c_0^2 - 2b_2c_0 - 2c_2c_0 + b_2}{c_0} \right).$$

The two images coincide if and only if the third components are the same, that is

$$b_2(c_0 - 1)(a_0 - c_0) = 0.$$

This yields three possibilities: $b_2 = 0$, $c_0 = 1$ or $a_0 = c_0$.

The case $b_2 = 0$ is "trivial" since it corresponds to the situation in which $\delta_{a,b} = \delta_{c,b} = \mathrm{id}$.

The case $c_0 = 1$ is equivalent to $c \in \overline{o,N}$, and the same computation shows that $\overline{o,N}$ is fixed point-wise by the $\delta_{a,b}$'s.

Let us suppose then $c_0 \neq 1$; then

$$\delta_{c,b}(\overline{o,c}) = \delta_{a,b}(\overline{o,c}) \Leftrightarrow c \in \overline{a,N}.$$

Since both a and c are arbitrary it follows that the action of any $\delta_{t,b} \in \Delta_t$ on a line of $\mathfrak{O}'$ does not depend upon the choice of the point t on the line $\overline{t,N}$.

On the other hand, since

1. all the lines of the form $\overline{k,N}$ are fixed set-wise;
2. the δ's are all collineations;
3. any point $q \in \mathbb{P}^+$ can be determined as intersection of $\overline{o,q} \in \mathfrak{O}'$ and $\overline{q,N}$;

the action of a δ on the lines of $\mathfrak{O}'$ is enough in order to determine its action on the whole cone $\mathbb{P}^+$.

It follows that the permutation group Δ_a does not depend on the choice of a on $L = \overline{a,N}$, that is the thesis. □

Note that the following has also been verified while proving the result.

Corollary 21. *Given $a \in \mathbb{P}^+ \setminus \overline{o,N}$ and let $b \in \overline{o,N} \setminus \{o\}$,*

$$\operatorname{Fix} \delta_{a,b} = \overline{o,N}.$$

Theorem 22. *For any $p \notin \overline{o,N}$,*

$$\Delta_{\overline{p,N}} = \Delta.$$

Proof. Under the assumption $|\mathbb{K}| \geqslant 7$, there exist at least 3 long lines in $(\mathbb{P}^+, +)$. Let

$$O := \overline{o,N},$$

$$L := \overline{p,N},$$

$$S := \overline{q,N},$$

with $S \notin O, L$. In order to prove the thesis, it is sufficient to show that Δ acts in a regular way on the points of the line $\overline{p,N}$. Since $\Delta_{\overline{p,N}} \leqslant \Delta$, the transitivity is immediate.

Suppose now that there exists some $x \in \overline{p,N}$ fixed by $\delta \in \Delta$. Because $(\mathbb{P}^+,+)$ is a fibred K-loop, the elements of Δ are all collineations. Let $y \in S$; since δ fixes x and the point $t := \overline{x,y} \cap O$, it has to fix all the line $\overline{x,y}$; thus y is fixed. This means that the line S is fixed point-wise, that is that all the short lines have to be fixed set-wise. On the other hand the long lines are always fixed set-wise, whence we deduce that δ has to be the identity. □

If $2 < |\mathbb{K}| < 7$, then the K-loop $(\mathbb{P}^+,+)$ constructed in the same geometric way is a group; hence, both Δ and $\Delta_{\overline{p,N}}$ are trivial. In this case the previous result is trivially true.

References

[1] E. Gabrieli, H. Karzel, The reflection structure of generalised co-Minkowski spaces leading to K-loops. Resultate Math. 32 (1997) 73–79.

[2] H. Karzel, Recent developments on absolute geometries and algebraization by K-loops. Discrete Math. 208/209 (1999) 387–409.

[3] O. Loos, Symmetric spaces, Benjamin, New York, 1969.

[4] O.T. O'Meara, Introduction to Quadratic Forms, Springer, Berlin, 1963.

[5] H. Struve, R. Struve, Endliche Cayley–Kleinsche Geometrien., Arch. Math. 48 (1987) 178–184.

[6] H. Struve, R. Struve, Zum Begriff der projektiv-metrischen Ebene, Z. Math. Logik Grundlag. Math. 34 (1988) 79–88.