ELSEVIER

Journal of Statistical Planning and Inference 72 (1998) 67–77

journal of statistical planning and inference

Automorphisms of finite Einstein geometries

Walter Benz

Mathematisches Seminar der Universität Hamburg, Bundesstraße 55, 20146 Hamburg, Germany

Abstract

Characterizations of automorphisms, or of mappings which are close to automorphisms L of three special finite geometries are presented. These geometries are finite analogues of Lorentz–Minkowski geometry, of de Sitter's world, and of Einstein's cylinder universe. © 1998 Elsevier Science B.V. All rights reserved.

AMS classification: 51 E 25; 51 K 05; 83 C 15; 83 C 40

Keywords: Lorentz transformation; Isometry of a distance space; Group of motions

1. Introduction

Three finite geometries will play a rôle in this paper. The real counterparts of these geometries are n-dimensional

Lorentz–Minkowski geometry LMG,
de Sitter's world DSW,
Einstein's cylinder universe ECU.

The real geometries LMG and DSW are solutions of

$$\mathrm{Ric} = \lambda g, \tag{1}$$

where Ric is the Ricci tensor, g the metric tensor and λ a (constant) scalar. Manifolds of Lorentz–Minkowski signature satisfying Eq. (1) are called Einstein spaces. Geometry ECU is not an Einstein space, but a solution of Einstein's law of gravitation

$$\mathrm{Ric} = \lambda g + \kappa T, \tag{2}$$

where T is the energy-impulse tensor and where κ is a scalar.

The aim of this paper is to present results about the characterization of automorphisms of the three finite geometries in question. Several things are known in this connection. But there are also, of course, open problems, as will be stated explicitely later on.

PII: S0378-3758(98)00022-6

2. The real case LMG

Suppose that $n \geqslant 2$ is an integer. n-dimensional Lorentz–Minkowski geometry is then defined to be the geometry $(\mathbb{R}^n, \mathbb{L}^n)$ consisting of the set $\mathbb{R}^n$ of *points* and the group $\mathbb{L}^n$ of Lorentz transformations of $\mathbb{R}^n$ as group of *motions* of $\mathbb{R}^n$ (see our book RG, i.e. Real Geometries, Benz, 1994). The Lorentz transformations of $\mathbb{R}^n$ are the mappings

$$(x_1 \dots x_n) \to xL + a$$

with real matrices $a = (a_1 \dots a_n)$,

$$L = \begin{pmatrix} l_{11} & \dots & l_{1n} \\ \vdots & & \\ l_{n1} & \dots & l_{nn} \end{pmatrix}$$

such that

$$LML^{\mathrm{T}} = M := \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & -1 \end{pmatrix} \tag{3}$$

holds true. L^{T} denotes the transpose of the matrix L.

A 2-point-invariant of $(\mathbb{R}^n, \mathbb{L}^n)$ is given by

$$d(x, y) = (x_1 - y_1)^2 + \cdots + (x_{n-1} - y_{n-1})^2 - (x_n - y_n)^2$$

for $n \geqslant 2$ and

$$x = (x_1, \dots, x_n) \in \mathbb{R}^n \quad \text{and} \quad y = (y_1, \dots, y_n) \in \mathbb{R}^n.$$

The following results are fundamental.

Theorem 1. *Let $f : \mathbb{R}^n \to \mathbb{R}^n$ $(n \geqslant 3)$ be a bijection satisfying*

$$\forall_{x, y \in \mathbb{R}^n} \; d(x, y) = 0 \;\Leftrightarrow\; d(f(x), f(y)) = 0.$$

Then f has the form $f(x) = k \cdot \lambda(x)$ for a real number $k \neq 0$ and a Lorentz transformation $\lambda \in \mathbb{L}^n$.

This theorem was proved by Alexandrov (1950, 1967, 1975) (see Lester, 1995).

Theorem 2. *Let $k \neq 0$ be a fixed real number and let*

$$f : \mathbb{R}^n \to \mathbb{R}^n \ (n \geqslant 2)$$

be a mapping satisfying

$$\forall_{x,y\in\mathbb{R}^n}\, d(x,y)=k \;\Rightarrow\; d(f(x),f(y))=k.$$

Then $f\in\mathbb{L}^n$.

Theorem 2 was proved in the case $n>2$ and $k>0$ by Lester (1981), and in the cases
1. $n=2$,
2. $n>2$ and $k<0$

by Benz (1992). Proofs for Theorems 1 and 2 are in our book GT, i.e. Geometrische Transformationen (Benz (1992), Sections 6.6 and 6.13–6.15).

3. The finite case of LMG

Let R be a finite and associative ring with identity element 1 such that $1\neq 0$. Define R^n, $n\geqslant 1$ an integer, as the set of all ordered n-tuples $(x_1,\dots,x_n)$ with elements $x_i\in R$. Define, moreover,

$$(x_1,\dots,x_n)+(y_1,\dots,y_n):=(x_1+y_1,\dots,x_n+y_n),$$
$$\lambda\cdot(x_1,\dots,x_n):=(\lambda x_1,\dots,\lambda x_n)$$

for $x_i, y_i, \lambda\in R$. Then $(R^n,+)$ turns out to be an abelian group and the multiplication $\lambda\cdot x$ with $\lambda\in R$ and $x\in R^n$ satisfies usual rules:

$$\lambda\cdot(x+y)=\lambda x+\lambda y,$$
$$(\lambda+\mu)\cdot x=\lambda x+\mu x,$$
$$(\lambda\mu)\cdot x=\lambda\cdot(\mu x),$$
$$1\cdot x=x$$

for all $\lambda,\mu\in R$ and all $x,y\in R^n$.

The structure (R^n,R,d) with

$$d(x,y):=(x_1-y_1)^2+\cdots+(x_{n-1}-y_{n-1})^2-(x_n-y_n)^2 \tag{4}$$

for $x,y\in R^n$ is a *distance space* (see RG 22). In order to define the notion of a distance space, let $M\neq\emptyset$ and W be sets and let, moreover, δ be a mapping from $M\times M$ in W. Then (M,W,δ) is called a *distance space* and $\delta(x,y)$ the *distance* of x,y. We say that $f:M\to M$ is an *isometry* in the case that

$$\delta(x,y)=\delta(f(x),f(y))$$

holds true for all $x,y\in M$. An isometry needs not to be injective. However, the set of all bijective isometries of (M,W,δ) is a group (under the permutation product) which we denote by $I(M,W,\delta)$. For every group G there exists a distance space (M,W,δ) such that

$$G\cong I(M,W,\delta).$$

If we denote the group of the function (4) by $\mathbb{L}_R^n$, we get the geometry $(R^n, \mathbb{L}_R^n)$ (compare Section 1.2, *Geometry of a notion or a function*, of RG, 21 ff). If R is commutative and if $1+1$ is not a zero divisor of R, then $\mathbb{L}_R^n$ $(n \geqslant 2)$ is given by the mappings

$$(x_1, \ldots, x_n) \to xL + a$$

with matrices $a = (a_1 \ldots a_n)$,

$$L = \begin{pmatrix} l_{11} & \ldots & l_{1n} \\ \vdots & & \\ l_{n1} & \ldots & l_{nn} \end{pmatrix}$$

over R such that Eq. (3) holds true (see GT, 55 ff).

Problem 1. *Let R be a ring as described at the beginning of this section and let k be a fixed element of R. Determine then all*

$$f : R^n \to R^n \quad (n \geqslant 2)$$

such that

$$\forall_{x,y \in R^n}\, d(x,y) = k \;\Rightarrow\; d(f(x), f(y)) = k$$

holds true.

A solution of this problem is not known. But there are several partial results in the direction of this problem, and there are even results about generalizations of the problem with respect to the metric (4).

Suppose that R is commutative and that $2 := 1+1$ is a unit element of R. If, furthermore, $n = 2$ and k is a unit element as well, then Problem 1 can be replaced equivalently by

Problem 2. *Determine all $f : R^2 \to R^2$ such that*

$$\forall_{x,y \in R^2}\, D(x,y) = 1 \;\Rightarrow\; D(f(x), f(y)) = 1 \tag{5}$$

holds true where D is defined by

$$D(x,y) := (x_1 - y_1)(x_2 - y_2) \tag{6}$$

for $x, y \in R^2$.

Problem 2 makes sense also in the case that R is a ring as described at the beginning of this section, so especially in the cases that R is not commutative or that 2 is not a unit element of R.

The following theorem holds true.

Theorem 3. *Let R be a Galois field* GF(q) *with $q \neq 5$,*

$$2 \nmid q \quad \text{and} \quad 3 \nmid q.$$

All mappings $f: \mathrm{R}^2 \to \mathrm{R}^2$ satisfying Eq. (5) are then bijective and they are all given by

$$f(x) = \left(a\,\sigma(x_1) + b, \frac{1}{a}\sigma(x_2) + c\right) \text{ for all } x \in R^2 \tag{7}$$

or

$$f(x) = \left(a\,\sigma(x_2) + b, \frac{1}{a}\sigma(x_1) + c\right) \text{ for all } x \in R^2, \tag{8}$$

where a, b, c are elements of R with $a \neq 0$ and where σ is an automorphism of R.

This theorem is part of results of Radó and Benz (see Schaeffer, 1986). Theorem 3 cannot be extended to the case GF(5) as was shown by Samaga (1982). The following mapping:

$$f: [\mathrm{GF}(5)]^2 \to [\mathrm{GF}(5)]^2$$

satisfies Eq. (5), but it has not one of the forms (7) or (8) since it is not bijective.

$$\begin{aligned}
&f(0,0) = f(1,2) = f(2,4) = f(3,1) = f(4,3) := (0,0),\\
&f(0,4) = f(1,1) = f(2,3) = f(3,0) = f(4,2) := (1,1),\\
&f(0,3) = f(1,0) = f(2,2) = f(3,4) = f(4,1) := (2,2),\\
&f(0,2) = f(1,4) = f(2,1) = f(3,3) = f(4,0) := (3,3),\\
&f(0,1) = f(1,3) = f(2,0) = f(3,2) = f(4,4) := (4,4).
\end{aligned}$$

In order to verify that f is a mapping which preserves D-value 1, Samaga took an arrangement of the set of points x of $[\mathrm{GF}(5)]^2$ in rows and columns with

	j	$j+1$
i	x	$x+(1,2)$
$i+1$	$x+(1,1)$	

implying that all points y with $D(x,y) = 1$ for a given x are at the following positions:

	$j-1$	j	$j+1$
$i-1$	y	y	
i		x	
$i+1$		y	y

Replacing (a,b) by ab and looking to the array, as described,

32	44	01	13	20	32	44	$\to$ 44
43	00	12	24	31	43	00	$\to$ 00
04	11	23	30	42	04	11	$\to$ 11
10	22	34	41	03	10	22	$\to$ 22
21	33	40	02	14	21	33	$\to$ 33
32	44	01	13	20	32	44	$\to$ 44
43	00	12	24	31	43	00	$\to$ 00

of the set of points, one realizes immediately that f preserves D-value 1.

There are also counterexamples in the cases $q \in \{2,3,4,8,9,16\}$ (Benz, 1982; Jürgensen, 1982 for $q = 16$).

Concerning these counterexamples we would like to present a generalization to the ring case of an idea which we published in Benz (1982) in connection with the field case. However, we would like to go a step further, even in the field case. We will say that the *points* $x, y \in R^2$ are *equivalent*, $x \sim y$, if, and only if, there exist points

$$P_1, \ldots, P_{m+1} \in R^2$$

with $x = P_1$, $y = P_{m+1}$ and $D(P_i, P_{i+1}) = 1$ for $i = 1, \ldots, m$, where m is a positive integer. This relation is symmetric and transitive, and it is also reflexive in view of the points

$$P_1 = x,\ P_2 = x + (1,1),\ P_3 = x.$$

A. *Suppose that Γ is an equivalence class and that t is a fixed element of R^2. Then*

$$\Gamma_t := \{x + t \mid x \in \Gamma\}$$

is also an equivalence class. Moreover, if Γ and Δ are equivalence classes, then there exists a $t \in R^2$ such that $\Delta = \Gamma_t$ holds true.

Proof. Obviously,

$$\forall_{x,y,t \in R^2}\, x \sim y \Leftrightarrow x + t \sim y + t.$$

This proves the first statement. Suppose now that Γ and Δ are equivalence classes. Take $a \in \Gamma$ and $b \in \Delta$ and put $t := b - a$. Then

$$b \in \Gamma \cap \Delta$$

and hence $\Gamma_t = \Delta$. □

B. A consequence of statement A is *that the equivalence classes of R^2 are all of the same cardinality.*

C. *Suppose that Γ is a fixed equivalence class of R^2 and that φ is a fixed mapping which associates to every equivalence class Δ of R^2 an element $\varphi(\Delta)$ of Δ. Then*

$$\forall_{x \in R^2} f(x) = x + \varphi(\Gamma) - \varphi([x]),$$

where $[x]$ denotes the equivalence class containing x, satisfies Eq. (5). *This mapping f is not bijective in the case that there exist at least two equivalence classes.*

Proof. Suppose that $D(x,y) = 1$ holds true. Hence, $y \in [x]$ and thus

$$\varphi([x]) = \varphi([y]).$$

This implies $f(x) - f(y) = x - y$, i.e. $D(f(x), f(y)) = 1$. If there exists a class $\Delta \neq \Gamma$, then $\Delta \cap \Gamma = \emptyset$, i.e.

$$\varphi(\Delta) \neq \varphi(\Gamma).$$

That f is not bijective is now a consequence of

$$f(\varphi(\Delta)) = \varphi(\Delta) + \varphi(\Gamma) - \varphi(\Delta) = f(\varphi(\Gamma)).$$

Examples. (a) $R = \mathrm{GF}(2)$.
The equivalence classes are

$$\{(0,0),(1,1)\},$$
$$\{(1,0),(0,1)\}.$$

(b) $R = \mathrm{GF}(3)$.
The classes are

$$\{(0,0),(1,1)(-1,-1)\},$$
$$\{(1,0),(-1,1),(0,-1)\},$$
$$\{(0,1),(1,-1),(-1,0)\}.$$

(c) $R = \mathrm{GF}(4)$.
Put $\mathrm{GF}(4) = \{0, 1, \varepsilon, \varepsilon^2\}$ with $\varepsilon^2 + \varepsilon + 1 = 0$. The classes are then

$$\{(0,0),(1,1),(\varepsilon,\varepsilon^2),(\varepsilon^2,\varepsilon)\},$$
$$\{(1,0),(0,1),(\varepsilon^2,\varepsilon^2),(\varepsilon,\varepsilon)\},$$
$$\{(\varepsilon,0),(\varepsilon^2,1),(0,\varepsilon^2),(1,\varepsilon)\},$$
$$\{(0,\varepsilon),(1,\varepsilon^2),(\varepsilon^2,0),(\varepsilon,1)\}.$$

(d) $R = \mathrm{GF}(q)$, $q > 4$. There is exactly one equivalence class (Benz, 1982). Samaga (1984) proves

Theorem 4. *The statement of Theorem* 3 *remains true in the cases* $q \in \{32, 128\}$. *If, in addition,* f *is assumed to be bijective, then the statement remains true also for* $q \in \{64, 81\}$.

It would be nice to prove that Theorem 3 holds true for all Galois fields $\mathrm{GF}(q)$ with $q > 16$.

Let R be a Galois field $\mathrm{GF}(q)$. Dilatations

$$f : R^2 \to R^2$$

of the plane R^2 are mappings such that

$$x - y \quad \text{and} \quad f(x) - f(y)$$

are linearly dependent for all $x, y \in R^2$. This then implies easily that a dilatation f has the form

$$f(x) = \lambda x + a$$

for all $x \in R^2$ with fixed $\lambda \in R$ and $a \in R^2$. The following result is due to Schaeffer (1984).

Theorem 5. *Suppose that* $R = \mathrm{GF}(q)$ *is a Galois field such that* $\mathrm{char}\, R \neq 2, 3, 5$. *If then* $f : R^2 \to R^2$ *is a mapping satisfying*

$$\forall_{x,y \in R^2}\, D(x, y) = 1 \ \Rightarrow\ x - y, f(x) - f(y) \text{ are linearly dependent},$$

then f *is already a dilatation of* R^2.

Also, with respect to Theorem 5 it would be nice to know what happens in the cases $\mathrm{char}\, R \in \{2, 3, 5\}$.

Concerning an analogous characterization of dilatations in normed spaces, see GT, 115 ff and Baker (1994), Laugwitz (1993).

Concerning higher-dimensional cases with respect to problem 1 compare Radó (1986): let V be a metric vector space over $\mathrm{GF}(p^m)$, $p > 2$ a prime and $3 \leqslant n = \dim V < \infty$; every distance 1 preserving mapping must then be semilinear (up to a translation) provided that

$$n \not\equiv 0, -1, -2 \pmod p$$

or that the discriminant of V satisfies a certain condition.

With respect to Problem 2 the case of a ring R which is not a field really occurs in Schaeffer (1984).

The cases $R = F[x]/\langle x^2 \rangle$ or $R = F \times F$ are for instance included in Schaeffer's paper (1984). Skew fields are considered by Samaga (1982).

4. The real case DSW and generalizations

Let R be a ring with identity element 1 which is supposed to be commutative and associative. We shall assume that $1+1$ is not a zero divisor of R. For an integer $n \geqslant 2$ we denote by R^n the R-module already introduced in Section 3. We are then interested in the distance space

$$S_R^n = (M, W, d)$$

with

$$M = \{(x_1, \ldots, x_{n+1}) \in R^{n+1} \mid x_1^2 + \cdots x_n^2 - x_{n+1}^2 = 1\},$$
$$W = R,$$
$$d(x, y) = xy$$

where the scalar product

$$x \cdot y = (x_1, \ldots, x_{n+1}) \cdot (y_1, \ldots, y_{n+1})$$

is defined by

$$xy = x_1 y_1 + \cdots + x_n y_n - x_{n+1} y_{n+1}.$$

We proved (RG 132 f)

Theorem 6. *Every isometry of the distance space S_R^n, $n \geqslant 2$, must be bijective, and moreover of the form*

$$f(x) = xL \tag{9}$$

for all $x \in S_R^n$ with

$$LML^{\mathrm{T}} = M := \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$

for

$$L = \begin{pmatrix} l_{11} & \cdots & l_{1,n+1} \\ \vdots & & \\ l_{n+1,1} & \cdots & l_{n+1,n+1} \end{pmatrix}$$

with $l_{ij} \in R$.

S_R^n together with its group of isometries (also called *motions*) is said to be n-dimensional de Sitter's world over R. In the case $R := \mathbb{R}$ we get DSW.

We now would like to mention a result of Schröder (to appear). Let Q be a regular quadratic form on a vector space V over the Galois field $R = \mathrm{GF}(q)$ such that

$$M := \{x \in V \mid Q(x) = 1\}$$

contains a line and such that

$$4 \leqslant \dim V \leqslant \infty.$$

A 1-isometry of M is a bijection f of M satisfying

$$\forall_{x,y \in M}\ \delta(x, y) = k \Leftrightarrow \delta(f(x), f(y)) = k$$

for a fixed element k of R, where we put

$$\delta(x, y) := Q(x - y).$$

Theorem 7. *Suppose that*

$$[k = 2 \quad \textit{and} \quad |R| = 3 \quad \textit{and} \quad \dim V = 4 \quad \textit{and} \quad |M| = 24]$$

does not hold true. Then f is induced by a semilinear bijection.

Schröder (1986) also offers counterexamples in the exceptional case as well as in the case $\dim V = 3$.

5. Einstein's cylinder universe

Let R be a ring as described at the beginning of Section 4 and let $n \geqslant 2$ be an integer. The distance space

$$C_R^n = (S^n, W, \delta)$$

is defined as follows:

$$S^n = \{(x_1, \ldots, x_{n+1}) \in R^{n+1} \mid x_1^2 + \cdots x_n^2 = 1\},$$

$$W = R \times R,$$

$$\delta(x, y) = (xy, (x_{n+1} - y_{n+1})^2).$$

The scalar product xy of

$$x = (x_1, \ldots, x_{n+1}) \quad \text{and} \quad y = (y_1, \ldots, y_{n+1})$$

is given by

$$xy = x_1 y_1 + \cdots + x_n y_n.$$

The following result holds true (RG 105 ff)

Theorem 8. *Every distance preserving mapping of C_R^n must be bijective and they are all given by the transformations*

$$f(x) = (x_1 \ldots x_{n+1}) \cdot \left(\begin{array}{ccc|c} & A & & 0 \\ & & & \vdots \\ & & & 0 \\ \hline 0 & \ldots & 0 & c \end{array} \right) + (0 \ldots a),$$

where A is an $n \times n$-matrix over R with

$$AA^{\mathrm{T}} = E := \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

and where c and a are elements of R with $c^2 = 1$.

The case $C_{\mathbb{R}}^n$ is exactly the geometry ECU. We would like to pose the following

Problem 3. *Let R be a Galois field and let k be a fixed element of $R \times R$. Determine then all*

$$f : S^2 \to S^2$$

such that

$$\forall_{x,y,\in S^2}\ \delta(x,y)=k \Rightarrow \delta(f(x),f(y))=k$$

holds true.

References

Alexandrov, A.D., 1950. Seminar Report. Uspehi Mat. Nauk. 5 (3) (37), 187.

Alexandrov, A.D., 1967. A contribution to chronogeometry. Canad. J. Math. 19, 1119–1128.

Alexandrov, A.D., 1975. Mappings of spaces with families of cones and space–time transformations. Ann. Math. 103, 229–257.

Baker, J.A., 1994. Some propositions related to a dilatation theorem of W. Benz. Aequat. Math. 47, 79–88.

Benz, W., 1994. Real geometries. BI-Wissenschaftsverlag, Mannheim, Leipzig, Wien, Zürich.

Benz, W., 1992. Geometrische Transformationen. BI-Wissenschaftsverlag, Mannheim, Leipzig, Wien, Zürich.

Benz, W., 1982. On mappings preserving a single Lorentz–Minkowski distance. III. J. Geometry 18, 70–77.

Benz, W., 1982. A Beckman–Quarles-type theorem for finite desarguesian planes. J. Geometry 19, 89–93.

Benz, W., 1992. On structures $T(t,q,r,n)$. Ann. Discrete Math. 52, 25–36.

Benz, W., 1992. Isometries in Galois Spaces. Le Matematiche Vol. XLVII fasc. II, pp. 197–204.

Jürgensen, A., 1982. Untersuchungen einiger Körper der Charakteristik 2 und 3 auf Gültigkeit der Aussage eines Satzes von F. Radó. Diplomarbeit Universität Hamburg.

Laugwitz, D., 1993. Regular hexagons in normed spaces and a theorem of Walter Benz. Aequat. Math. 45, 163–166.

Lester, J., 1995. Distance preserving transformations. In: Francis, B. (Ed.), Handbook of Incidence Geometry, Elsevier, Amsterdam.

Lester, J., 1981. The Beckman–Quarles theorem in Minkowski space for a spacelike squaredistance. Archiv Math. 37, 561–568.

Radó, F., 1986. On mappings of the Galois space. Israel J. Math. 53, 217–230.

Samaga, H.J., 1982. Zur Kennzeichnung von Lorentztransformationen in endlichen Ebenen. J. Geometry 18, 169–184.

Samaga, H.J., 1984. Über Abstand 1 erhaltende Abbildungen in Minkowski–Ebenen. J. Geometry 22, 183–188.

Schaeffer, H., 1986. Der Satz von Benz–Radó. Aequat. Math. 31, 300–309.

Schaeffer, H., 1984. Eine Kennzeichnung der Dilatationen endlicher desarguesscher Ebenen der Charakteristik $\neq 2,3,5$. J. Geometry 22, 51–56.

Schaeffer, H., 1984. Abbildungen in Ebenen über zweidimensionalen Algebren, die den Lorentz–Minkowski–Abstand 1 invariant lassen. Abh. Math. Sem. Univ. Hamburg 54, 191–198.

Schröder, E.M. On 1-isometries of affine quadrics over finite fields. To appear.