ELATION LAGUERRE PLANES OF ORDER p^2 THAT ADMIT AN AUTOMORPHISM GROUP OF ORDER p^2 IN THE ELATION COMPLEMENT

G.F. STEINKE

Department of Mathematics
University of Canterbury
Christchurch, New Zealand

Dedicated to the memory of Alan Rahilly, 1947 – 1992

ABSTRACT. Following the program for finite translation planes to construct such planes from collineation groups in the translation complement a search for non-Miquelian Laguerre planes of odd order is initiated. In this note finite Laguerre planes of order p^2, p a prime, are investigated. If such a Laguerre plane $\mathcal{L}$ admits a circle-transitive elation group and an automorphism group of order p^2 in the elation complement, then it is proved that $\mathcal{L}$ is Miquelian.

1. Introduction

A *Laguerre plane* $\mathcal{L} = (P, \mathcal{K}, \|)$ consists of a set of points P, a set of at least two circles $\mathcal{K}$ (considered as subsets of P) and an equivalence relation $\|$ on P (parallelism) such that three pairwise non-parallel points can be joined uniquely by a circle, such that the circles which touch a fixed circle K at $p \in K$ partition $P \setminus |p|$ (here $|p|$ denotes the parallel class of p), such that each parallel class meets each circle in a unique point (parallel projection), and such that each circle contains at least three points. If P is finite, any two circles have the same number $n+1$ of points, and n is called the order of $\mathcal{L}$. There are n^2+n points, n^3 circles, and $n+1$ parallel classes in a Laguerre plane of order n, and every parallel class contains n points. The *Miquelian* Laguerre plane of order q (q being a prime power) is obtained as the geometry of non-trivial plane sections of a quadratic cone in the 3-dimensional projective space over $GF(q)$. All known finite Laguerre planes of odd order are Miquelian.

For a point $r \in P$ the internal incidence structure consists of all points of P not parallel to r and, as lines, of all circles passing through r (without the point r) and all parallel classes not passing through r. This is an affine plane, the *derived affine plane* $\mathcal{A}_r$ at r. If $\mathcal{L}$ has order n, then $\mathcal{A}_r$ also has order n. A circle K not passing

1991 *Mathematics Subject Classification.* 51B15, 51E25.
This research was supported by a Feodor Lynen Fellowship.

through the point of derivation r induces an oval in the projective closure of the derived affine plane $\mathcal{A}_r$ by $(K\setminus |r|) \cup \{\omega\}$, where ω denotes the infinite point of lines that come from parallel classes. Moreover, the infinite line is a tangent to this oval.

An automorphism of a Laguerre plane $\mathcal{L}$ is a bijection of the point set that maps circles onto circles. All automorphisms of $\mathcal{L}$ form a group Γ with respect to composition, called the automorphism group of $\mathcal{L}$. As every automorphism maps parallel points onto parallel points, the collection of all automorphisms that map each point onto a parallel point forms a normal subgroup Δ, called the *kernel* of Γ, which is just the kernel of the action of Γ on the set of parallel classes. In [12] finite Laguerre planes which admit a kernel Δ that is transitive on $\mathcal{K}$ were investigated. In this case each derived affine plane is a dual translation plane. From this a description of such Laguerre planes in terms of two matrix-valued maps G and H was developed (see Proposition 2.1). In particular, Δ contains a distinguished normal subgroup Δ_e, called the *elation group* of $\mathcal{L}$: it consists of all members of Δ that fix no circle, together with the identity. The elation group of a finite Laguerre plane plays a role analogous to the translation group of finite projective planes. We call such a Laguerre plane an *elation Laguerre plane.*

In this note we follow the program for finite translation planes to construct new planes from information about a suitable group in the translation complement of the collineation group and to classify all arising planes. For further information and references see [2]. We begin with the case of elation Laguerre planes of order p^2, p a prime, as one could expect that a elation Laguerre plane of order p^h contains such a subplane. More precisely, we apply the structure theorem of [12] to determine elation Laguerre planes of order p^2, p a prime, that admit an automorphism group of order p^2 in the complement of the elation group Δ_e. Similar to the case of translation planes of order p^2 (see [8, §7]) we prove

THEOREM. *A finite elation Laguerre plane of order p^2, p a prime, that admits an automorphism group of order p^2 in the elation complement, is Miquelian.*

Note that even without the additional assumptions on the elation group a Laguerre plane of order 4 or 9 is Miquelian; see [4] and [13] respectively. Furthermore, since a translation plane of prime order is Desarguesian, a finite elation Laguerre plane of prime order is Miquelian (cf. Proposition 2.3).

2. Preliminaries

We begin with a representation of finite elation Laguerre planes as given in [12, Theorem 3].

Proposition 2.1. *Each derived affine plane of a finite elation Laguerre plane $\mathcal{L} = (P, \mathcal{K}, \|)$ is a dual translation plane and $\mathcal{L}$ can be represented in the following form. There is a finite field $\mathbb{F} = GF(q)$, q a prime power, a positive integer m, a symbol $\infty \notin \mathbb{F}$, and a matrix-valued map $D : \mathbb{F}^m \cup \{\infty\} \longrightarrow M(3m, m; \mathbb{F})$ (where $M(3m, m; \mathbb{F})$ denotes the set of all $3m \times m$ matrices over the field $\mathbb{F}$) such that the point set is*

$$P = (\mathbb{F}^m \cup \{\infty\}) \times \mathbb{F}^m,$$

the set of circles is

$$\mathcal{K} = \{K_c \mid c \in \mathbb{F}^{3m}\}$$

where a circle K_c is described as

$$K_c = \{(z, c \cdot D(z)) \in P \mid z \in \mathbb{F}^m \cup \{\infty\}\};$$

two points (z, w) and (u, v) are parallel if and only if $z = u$. The elation group Δ_e consists of all maps

$$(z, w) \mapsto (z, w + c \cdot D(z)),$$

for $c \in \mathbb{F}^{3m}$; also

$$(z, w) \mapsto (z, r \cdot w)$$

is an automorphism in the kernel for all $r \in \mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

More precisely, $D(\infty) = (I\ O\ O)^t$ where ^{t} denotes the transposed matrix and I and O denote the $m \times m$ identity matrix and the $m \times m$ zero matrix respectively. The matrix $D(z)$, $z \in \mathbb{F}^m$, can be written as $(H(z)\ G(z)\ I)^t$ with suitable $m \times m$ matrices $H(z)$ and $G(z)$, where G describes a matrix spread (or spread set) of a translation plane of order q^m (corresponding to the dualisation of the derived affine plane at the infinite point $(\infty, 0)$) and H describes an oval in the projective closure of $\mathcal{A}_{(\infty,0)}$ by $\{(z, c \cdot H(z)) \mid z \in \mathbb{F}^m\} \cup \{\omega\}$ for all $c \in \mathbb{F}^m$, $c \neq 0$.

$\mathcal{K}$ can be made into a 3m-dimensional vector space in a natural way by identifying $c \in \mathbb{F}^{3m}$ with the circle K_c, or equivalently, by transfering the vector space structure of Δ_e via the bijection $\Delta_e \to \mathcal{K} : \delta \mapsto \delta(K_o)$ where o is the zero vector in $\mathbb{F}^{3m}$. Since Δ_e is a normal subgroup of Γ, the automorphism group Γ operates on Δ_e by conjugation. Via the preceding identifications this action agrees with the geometric action of Γ on $\mathcal{K}$, i.e. $\gamma(K_c) = K_{\gamma(c)}$. If $q = p^h$ for some prime p, then the stabilizer of K_o is faithfully and $GF(p)$-linearly represented on the vector space $GF(p)^{3mh} \cong \mathcal{K}$.

Geometrically, a finite elation Laguerre plane of order q^m as described in Proposition 2.1 is equivalent to a $(q^m + 1)$-set of $(m-1)$-dimensional subspaces in the $(3m-1)$-dimensional projective space over $GF(q)$, see [12, Thm 4] and also [3] for odd q and related generalized quadrangles.

In the situation of the Theorem of Section 1 $m = 2$ and D, G, H are 6×2, 2×2, and 2×2 matrices over $GF(p)$ respectively. From results on translation planes of order p^2 we already know the form of G (up to isomorphisms). According to [8, §7], we have

Proposition 2.2. *A finite translation plane of order p^2, p a prime, that admits a collineation group of order p^2 in the translation complement is Desarguesian or is isomorphic to a Betten-Walker plane. In the latter case $p \equiv -1 \pmod 6$, and*

$$G(z) = \begin{pmatrix} y - x^2 & -\frac{1}{3}x^3 \\ x & y \end{pmatrix}, z = (x, y).$$

As $z = (x, y)$ varies through all $GF(p) \times GF(p)$ the $G(z)$ form a matrix spread of the translation plane.

According to the celebrated theorem of Segre [10] an oval in a finite Desarguesian projective plane of odd order is a conic. As a consequence, Chen and Kaerlein proved in [4] by simply counting the conics having a given tangent at a given point:

Proposition 2.3. *A finite Laguerre plane of odd order with at least one Desarguesian derived affine plane is Miquelian.*

To prove the Theorem of §1 we exclude the case that a dual Betten-Walker plane occurs as a derived affine plane of $\mathcal{L}$. As an automorphism fixing a point induces a collineation of the derived affine plane at that point, it is crucial to know the collineation groups of the Betten-Walker planes (see [1] or [14, Thm 4.10]).

To obtain the form we need for those Laguerre planes we are interested in we dualize the Betten-Walker plane such that the infinite line becomes the infinite point ω and vice versa. This yields

Proposition 2.4. *Let p be an odd prime such that $p \equiv -1 \pmod 6$ and let $\mathbb{F} = GF(p)$. The dual (affine) Betten-Walker plane of order p^2 has point set $\mathbb{F}^4$ and lines have the form*

$$L_{a,b} = \{(z, a \cdot G(z) + b) \mid z \in \mathbb{F}^2\},$$

where a, b range over $\mathbb{F}^2$ and $G(z)$ is as in Proposition 2.2, or the form

$$\{(c, w) \mid w \in \mathbb{F}^2\}$$

for all $c \in \mathbb{F}^2$ (vertical lines). The collineation group Γ_{BW} of this plane is the semidirect product of the dual translation group

$$\{(z, w) \mapsto (z, w + cz + d) \mid c, d \in \mathbb{F}^2\},$$

and the stabilizer of the line $L_{0,0}$. Furthermore,

$$\Lambda = \{(z, w) \mapsto (z \cdot \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} + (s, \frac{1}{2}s^2 + t), w \cdot \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}) \mid s, t \in \mathbb{F}\}$$
$$= \{(x, y, u, v) \mapsto (x + s, y + sx + \frac{1}{2}s^2 + t, u, v + su) \mid s, t \in \mathbb{F}\}$$

is an abelian Sylow p-group of the stabilizer of $L_{0,0}$ in Γ_{BW}. In particular, a group of order p^2 in the stabilizer of $L_{0,0}$ is conjugate to Λ. A member $\lambda \in \Lambda$ acts on the set of non-vertical lines like the 4×4 matrix

$$C_{s,t} = \begin{pmatrix} 1 & s & -\frac{1}{2}s^2 - t & -\frac{1}{6}s^3 - st \\ 0 & 1 & -s & -\frac{1}{2}s^2 - t \\ 0 & 0 & 1 & s \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

for $s, t \in \mathbb{F}$, i.e. the coefficient vector $(a, b) \in \mathbb{F}^2 \times \mathbb{F}^2 = \mathbb{F}^4$ of $L_{a,b}$ is mapped to $(a, b) \cdot C_{s,t}$.

Note that $C_{s,t}$ differs slightly from the matrix corresponding to a collineation in the stabilizer of the point $(0, 0)$ in the Betten-Walker plane as given in [1].

3. A Representation of Subgroups in the Elation Complement

The following two lemmata deal with subgroups in the elation complement of a elation Laguerre plane. We state them in a more general form than we need it for the purpose of this paper.

Lemma 3.1. *Let $\mathcal{L}$ be a finite elation Laguerre plane of order q^m, $q = p^h$ for some prime p, and let $\Sigma \leq \Gamma$ be a p-group of automorphisms of $\mathcal{L}$ in the elation complement, i.e. $\Sigma \cap \Delta_e = \{id\}$. Then Σ fixes a parallel class π. Moreover, there is a subgroup $\Sigma' \cong \Sigma$ that fixes the circle $K_o = K_{(0,0,0)}$ (here we use the notation as in Proposition 2.1) and also the parallel class π. Hence Σ' fixes the point $x = \pi \cap K_o$, and Σ' induces a p-group of collineations of the derived affine plane $\mathcal{A} = \mathcal{A}_x$ at x of the same order as Σ.*

Proof. Let Σ be a p-group of automorphisms of $\mathcal{L}$ such that $\Sigma \cap \Delta_e = \{id\}$. Since there are $q^m + 1$ parallel classes in $\mathcal{L}$ and because Σ has only orbits of length a power of p, there must be some parallel class π be fixed by Σ.

Let $\sigma \in \Sigma$. Since Δ_e is sharply transitive on $\mathcal{K}$, there is precisely one $\delta_\sigma \in \Delta_e$ such that $\delta_\sigma\sigma(K_o) = K_o$. Let

$$\Sigma' = \{\delta_\sigma\sigma \mid \sigma \in \Sigma\}.$$

It is easily verified that Σ' is a subgroup of Γ in the elation complement and that

$$\Sigma \to \Sigma' : \sigma \mapsto \delta_\sigma\sigma$$

is an isomorphism from Σ onto Σ'. Since Σ' fixes the parallel class π and the circle K_o, it must also fix $x = \pi \cap K_o$. □

An immediate consequence of the foregoing Lemma and of Propositions 2.2 and 2.3 is the following

Corollary 3.2. *A finite elation Laguerre plane of order p^2, $p \not\equiv -1 \pmod 6$ that admits an automorphism group of order p^2 in the elation complement is Miquelian.*

We say that a group Σ in the stabilizer of the circle K_o is in the *linear* elation complement of a finite elation Laguerre plane $\mathcal{L}$ of order q^2, q a prime power, if it is in the elation complement, and if the action of Σ on the elation group $\Delta_e \cong GF(q)^6$ by conjugation is linear over $GF(q)$. In the coordinatization of $\mathcal{L}$ as given in Proposition 2.1 this is equivalent to Σ acting on $\mathcal{K} \cong GF(q)^6$ as a group of 6×6 matrices over $GF(q)$.

Lemma 3.3. *Assume that Σ is a p-group in the linear elation complement of a finite elation Laguerre plane $\mathcal{L}$ of order q^2, q a power of p, such that Σ fixes the circle K_o and the infinite point $(\infty, 0)$. Then $\mathcal{L}$ can be coordinatized as in Proposition 2.1such that each element of the group Σ can be described by a 6×6 matrix of the form*

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

where

$$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

for some $a \in GF(q)$, B is a suitable 2×4 matrix, and C is a 4×4 matrix that describes the corresponding action on the set of non-vertical lines of the derived affine plane at $(\infty, 0)$. Moreover, Σ fixes at least the 1-dimensional subspace $\{(\infty, (0, z)) | \; z \in GF(q)\}$ on the infinite parallel class $| (\infty, 0) |$ elementwise. That is, a circle K_c passing through such a fixed point is mapped to a circle K_{c+d} where d has the form $(0, \tilde{d}_2, \tilde{d}_3)$, $\tilde{d}_2, \tilde{d}_3 \in GF(q)^2$. If Σ has order greater than q, then $| (\infty, 0) |$ is fixed elementwise by a subgroup of order at least p.

Proof. Let $\mathbb{F} = GF(q)$. In the coordinatization of $\mathcal{L}$ as given in Proposition 2.1 a circle through the infinite point $(\infty, \tilde{c}_1)$ has coordinate vector $(\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$ with $\tilde{c}_1, \tilde{c}_2, \tilde{c}_3 \in \mathbb{F}^2$. As Σ fixes $(\infty, 0)$, it permutes the circles through this point. This shows that $\{(0, \tilde{c}_2, \tilde{c}_3) \mid \tilde{c}_2, \tilde{c}_3 \in \mathbb{F}^2\}$ is an invariant subspace in $\mathbb{F}^6$. Hence, each member of Σ has the form $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ where A, B, C are 2×2, 2×4, and 4×4 matrices respectively.

The map $\rho : \Sigma \to GL(2, q)$ which maps $\sigma \in \Sigma$ corresponding to $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ to the matrix A is a homomorphism from Σ to the general linear group $GL(2, q)$. Thus $\rho(\Sigma)$ is a p-subgroup of $GL(2, q)$. Consequently, $\rho(\Sigma)$ is contained in a Sylow p-subgroup of $GL(2, q)$. Hence $\rho(\Sigma)$ is conjugate to some subgroup of $S = \{\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \mid z \in \mathbb{F}\}$ by the second Sylow theorem, cf. [5, Thm 4.2.2]. ($GL(2, q)$ has order $q \cdot (q-1)^2 \cdot (q+1)$ and $S \cong \mathbb{F}$ has order q, therefore S is a Sylow p-subgroup of $GL(2, q)$.) This shows that, in a suitable coordinatization, $\rho(\Sigma)$ is a subgroup of S. It then readily follows that $\{(\infty, (0, z)) | \; z \in GF(q)\}$ is fixed elementwise.

Let $V_2 = \{(0, x_2, \ldots, x_6) \in \mathbb{F}^6 \mid x_i \in \mathbb{F}\}$. The corresponding subspace of $\mathcal{K}$ is fixed by each $\sigma \in \Sigma$. More precisely, a circle K_c with coefficient vector $c = (0, c_2, \ldots, c_6) \in V_2$ is mapped to a circle whose coefficient vector has the same entries in the first and second positions, i.e. $\sigma(c) = c + (0, 0, d_3, \ldots, d_6)$ for suitable $d_i \in \mathbb{F}$. As the circle K_c passes through the infinite point $(\infty, (0, c_2))$, this point must be fixed by σ. If Σ has order greater than q, then ρ must have a non-trivial kernel because $GL(2,q)$ has order $q \cdot (q-1)^2 \cdot (q+1)$. Obviously, a member of the kernel fixes $\mid (\infty, 0) \mid$ pointwise. This proves the statement about fixed points of Σ on $\mid (\infty, 0) \mid$. □

3.4. General Hypotheses.

For the remainder of this note $\mathcal{L} = (P, \mathcal{K}, \|)$ always denotes a finite elation Laguerre plane of order p^2, p a prime, and let $\mathbb{F} = GF(p)$. Let Δ_e be the elation group of $\mathcal{L}$ and let $\Sigma \leq \Gamma$ be a group of automorphisms of $\mathcal{L}$ of order p^2 in the elation complement such that Σ fixes the circle K_o and the infinite point $(\infty, 0)$.

By Proposition 2.1 the action of Σ on Δ_e and on $\mathcal{K}$ is linear over $GF(p)$, that is, Σ is even in the linear elation complement. We assume that $\mathcal{L}$ is coordinatized as in Lemma 3.3. In view of Corollary 3.2 we further assume that the derived affine plane at the point $(\infty, 0)$ is a dual Betten-Walker plane, and thus $p \equiv -1 \pmod 6$. Note that the condition $p \equiv -1 \pmod 6$ implies that -3 is not a square in $\mathbb{F}$ (cf. [6, Thm 96]) and that the map $\mathbb{F} \to \mathbb{F} : x \mapsto x^3$ is a permutation of $\mathbb{F}$.

Since Σ induces a group of collineations of the derived affine plane at $(\infty, 0)$, the group Λ in Proposition 2.4 and Σ are conjugate. We finally assume that Σ acts on the set of circles through $(\infty, 0)$ like the group $\Lambda \cong \mathbb{F}^2$ on the set of non-vertical lines of the dual Betten-Walker plane.

For the investigation of the possible action of Σ on $\mathcal{K}$ we specialize Lemma 3.3 to our situation.

Proposition 3.5. *Under the general hypotheses 3.4 the group Σ consists of all matrices of the form*

$$\begin{pmatrix} A_{s,t} & B_{s,t} \\ 0 & C_{s,t} \end{pmatrix}$$

for $s, t \in \mathbb{F}$ where

$$A_{s,t} = \begin{pmatrix} 1 & a_1 s + a_2 t \\ 0 & 1 \end{pmatrix}$$

for some $a_1, a_2 \in \mathbb{F}$, $B_{s,t}$ is a suitable 2×4 matrix, and $C_{s,t}$ is the 4×4 matrix as in Proposition 2.4. Σ acts on the point set as

$$(x, y, u, v) \mapsto \begin{cases} (x + s, y + sx + \frac{1}{2}s^2 + t, u, v + su), & \text{for } (x, y) \in \mathbb{F}^2 \\ (\infty, u, a_1 u + a_2 v), & \text{for } (x, y) = \infty. \end{cases}$$

In particular, Σ fixes at least the 1-dimensional subspace $\{(\infty, (0, z)) \mid z \in GF(q)\}$ on the infinite parallel class $\mid (\infty, 0) \mid$ elementwise. Also, $\mid (\infty, 0) \mid$ is fixed by a subgroup of Σ of order at least p pointwise.

Proof. This is an immediate consequence of Lemma 3.3 and Proposition 2.4. The matrix A in $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ corresponding to $\sigma \in \Sigma$ has the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. As σ is parametrized by s, t, we obtain a homomorphism $\mathbb{F}^2 \to \mathbb{F}$ which can be written as $(s,t) \mapsto a_1 s + a_2 t$. The assertion on fixed points on $|\ (\infty, 0)\ |$ follows from the formula for the action of Σ on $|\ (\infty, 0)\ |$, as $a_1 u + a_2 v = v$ determines a 1- or 2-dimensional subspace of $\mathbb{F}^2$, or from Lemma 3.3. □

By the preceding proposition we know the action of Σ on the finite points and also on the infinite parallel class. Since Σ acts transitively on the set of finite parallel classes this allows us to derive equations for circles and thus to determine all the circles explicitly in the next two sections.

If $a_1 = 0$, $a_2 = 1$, then Σ fixes every infinite point (∞, w), $w \in \mathbb{F}^2$. We shall see in Proposition 4.5 that this case cannot occur.

4. Equations of Circles Through an Infinite Point Fixed by Σ

We keep the notation of the preceding section and we assume the general hypotheses 3.4. We first use circles passing through an infinite point fixed by Σ to obtain equations for such circles by using the transitive action of Σ on the set of finite parallel classes. Similarly, in a second step (see section 5) we derive equations for the other circles from the matrix representation given in Proposition 3.5. For later use we note

Lemma 4.1. *Let $a_2, \dots, a_5 \in \mathbb{F}$ and let $\alpha : \mathbb{F} \to \mathbb{F}$ be a map such that*

$$\begin{aligned} \alpha(x+y) =& \alpha(x) + \alpha(y) \\ & + a_2 xy + a_3(x^2 y + xy^2) + a_4(x^3 y + \frac{3}{2} x^2 y^2 + xy^3) \\ & + a_5(x^4 y + 2x^3 y^2 + 2x^2 y^3 + xy^4) \end{aligned}$$

for all $x, y \in \mathbb{F}$. If $p > 5$ or if $a_5 = 0$ for $p = 5$, then there exists $a_1 \in \mathbb{F}$ such that

$$\alpha(x) = a_1 x + \frac{1}{2} a_2 x^2 + \frac{1}{3} a_3 x^3 + \frac{1}{4} a_4 x^4 + \frac{1}{5} a_5 x^5$$

for all $x \in \mathbb{F}$, where $\frac{1}{5} a_5$ is interpreted as 0 if $p = 5$.

Proof. Let $\beta(x) = \alpha(x) - \frac{1}{2} a_2 x^2 - \frac{1}{3} a_3 x^3 - \frac{1}{4} a_4 x^4 - \frac{1}{5} a_5 x^5$ if $p > 5$ and $\beta(x) = \alpha(x) - \frac{1}{2} a_2 x^2 - \frac{1}{3} a_3 x^3 - \frac{1}{4} a_4 x^4$ if $p = 5$. It readily follows that

$$\beta(x+y) = \beta(x) + \beta(y).$$

Thus $\beta(x) = a_1 x$ for some $a_1 \in \mathbb{F}$. □

4.2. In the sequel we describe a circle by a function $f = (u,v) : \mathbb{F}^2 \to \mathbb{F}^2$ as

$$\begin{aligned} K_f &= \{(z, f(z)) \mid z \in \mathbb{F}^2\} \cup \{(\infty, w_f)\} \\ &= \{(x, y, u(x,y), v(x,y)) \mid x, y \in \mathbb{F}\} \cup \{(\infty, w_f)\} \end{aligned}$$

(there shall be no confusion betweeen K_f and K_c as it is always clear whether the index denotes a function of $\mathbb{F}^2$ or a vector in $\mathbb{F}^6$). Let

$$\begin{aligned} g_1 &: \mathbb{F}^2 \to \mathbb{F}^2 : (x,y) \mapsto (y - x^2, -\frac{1}{3}x^3), \\ g_2 &: \mathbb{F}^2 \to \mathbb{F}^2 : (x,y) \mapsto (x,y), \end{aligned} \tag{1}$$

i.e. g_1, g_2 describe respectively the first and second rows of the 2×2 matrix G of Section 2. Furthermore, we identify $c \in \mathbb{F}^2$ with the constant map $(x,y) \mapsto c$. When f and g both describe circles, then $rf + g$ describes a circle too for all $r \in \mathbb{F}$. The coefficient vector of K_{rf+g} is the sum of r times the coefficient vector of K_f and the coefficient vector of K_g. In particular, the coefficient vector of $K_{d_1 g_1 + d_2 g_2 + (d_3, d_4)}$ is $(0, 0, d_1, d_2, d_3, d_4)$. If (∞, w_f) is fixed by $\sigma \in \Sigma$, then Lemma 3.3 shows that K_f is mapped to a circle of the form $K_{f + d_1 g_1 + d_2 g_2 + (d_3, d_4)}$ for some $d_1, d_2, d_3, d_4 \in \mathbb{F}$. If $c \in \mathbb{F}^6$ is the coefficient vector of K_f then $\sigma(K_f)$ must have coefficient vector $c + d$ with $d = (0, 0, d_1, d_2, d_3, d_4) \in \mathbb{F}^6$, which translates into a describing function as above.

We now investigate circles through infinite points that are fixed by Σ. Since the subgroup

$$\Psi = \{\psi_t \mid t \in \mathbb{F}\}$$

where

$$\psi_t : (x, y, u, v) \mapsto (x, y + t, u, v)$$

(that is, the subgroup of Σ with $s = 0$) plays a special role, we consider this subgroup separately.

Proposition 4.3. *If f describes a circle such that $f(0,0) = (0,0)$ and (∞, w_f) is a fixed point of Ψ, then $f = (u,v)$ has the following form :*

$$\begin{aligned} u(x,y) &= u(x,0) + a(\frac{1}{2}y^2 - x^2 y) + bxy + cy \\ v(x,y) &= v(x,0) - \frac{1}{3}ax^3 y + \frac{1}{2}by^2 + dy \end{aligned}$$

for some $a, b, c, d \in \mathbb{F}$.

Proof. ψ_{-t} maps the circle K_f to $K_{f + a_t g_1 + b_t g_2 + c_t}$ for suitable $a_t, b_t \in \mathbb{F}$, $c_t \in \mathbb{F}^2$. Using the action of ψ_{-t} on points as given above and substituting $y + t$ for y, we obtain

$$\begin{aligned} f(x, y+t) &= (f + a_t g_1 + b_t g_2 + c_t)(x,y) \\ &= f(x,y) + a_t \cdot (y - x^2, -\frac{1}{3}x^3) + b_t \cdot (x,y) + c_t \end{aligned} \tag{2}$$

for all $x, y, t \in \mathbb{F}$. Putting $y = 0$ in (2) yields

$$f(x,t) = f(x,0) + a_t \cdot (-x^2, -\frac{1}{3}x^3) + b_t \cdot (x,0) + c_t.$$

For $x = 0$ in the above equation we find

$$c_t = f(0,t),$$

and thus

(3) $$f(x,y) = f(x,0) + f(0,y) + a_y \cdot (-x^2, -\frac{1}{3}x^3) + b_y \cdot (x,0).$$

We set $x = 0$ in (2); this gives us

(4) $$f(0, y+t) = f(0,y) + f(0,t) + (a_t y, b_t y).$$

The left-hand side being symmetrical in y and t implies

$$a_t y = a_y t, \quad \text{and} \quad b_t y = b_y t;$$

therefore

(5) $$\begin{aligned} a_t &= at, \\ b_t &= bt, \end{aligned}$$

for $a = a_1, b = b_1 \in \mathbb{F}$. Substituting (5) into (4) we find

$$\begin{aligned} u(0, y+t) &= u(0,y) + u(0,t) + aty, \\ v(0, y+t) &= v(0,y) + v(0,t) + bty, \end{aligned}$$

and from Lemma 4.1 we infer

(6) $$\begin{aligned} u(0,y) &= \frac{1}{2}ay^2 + cy, \\ v(0,y) &= \frac{1}{2}by^2 + dy, \end{aligned}$$

for some $c, d \in \mathbb{F}$. Substituting (5) and (6) into (3) we finally obtain the stated form of u and v. $\square$

Proposition 4.4. *If f describes a circle such that $f(0,0)=(0,0)$ and (∞, w_f) is a fixed point of Σ, then $f=(u,v)$ has the following form :*

$$u(x,y) = b(xy - \frac{2}{3}x^3) + c(y-x^2) + dx + \alpha x$$
$$v(x,y) = b(\frac{1}{2}y^2 - \frac{1}{4}x^4) - \frac{1}{3}cx^3 + dy + \frac{1}{2}\alpha x^2 + \beta x$$

for some $b, c, d, \alpha, \beta \in \mathbb{F}$.

Proof. As $\Psi \leq \Sigma$, we already know the form of $u(x,y)$ and $v(x,y)$ from Proposition 4.3 up to $u(x,0)$ and $v(x,0)$. Similar to the proof of that proposition we now use the subgroup

$$\Phi = \{\phi_s \mid s \in \mathbb{F}\}$$

where

$$\phi_s : (x,y,u,v) \mapsto (x+s, y+sx+\frac{1}{2}s^2, u, v+su)$$

(that is, the subgroup of Σ with $t=0$) to find $u(x,0)$ and $v(x,0)$. For later use (see Proposition 5.2) let

$$h_2 : \mathbb{F}^2 \to \mathbb{F}^2 : (x,y) \mapsto (xy - \frac{2}{3}x^3, \frac{1}{2}y^2 - \frac{1}{4}x^4)$$

and assume that there is an $a' \in \mathbb{F}$ such that the automorphism ϕ_{-s} maps the circle K_f to $K_{f-a'sh_2+a_sg_1+b_sg_2+(c_s,d_s)}$ for suitable $a_s, b_s, c_s, d_s \in \mathbb{F}$ (for the proof of the proposition we only need $a'=0$). Using the action of ϕ_{-s} on points as given above and substituting $x+s$ for x and $y+sx+\frac{1}{2}s^2$ for y, we obtain

$$\begin{aligned} u(x+s, y+sx+\frac{1}{2}s^2) =& u(x,y) - a's(xy-\frac{2}{3}x^3) + a_s(y-x^2) + b_sx + c_s \\ v(x+s, y+sx+\frac{1}{2}s^2) =& v(x,y) + su(x+s, y+sx+\frac{1}{2}s^2) \\ & - a's(\frac{1}{2}y^2 - \frac{1}{4}x^4) - \frac{1}{3}a_sx^3 + b_sy + d_s. \end{aligned} \tag{7}$$

For $x=y=0$ we find

$$\begin{aligned} c_s &= u(s, \frac{1}{2}s^2), \\ d_s &= v(s, \frac{1}{2}s^2) - su(s, \frac{1}{2}s^2). \end{aligned} \tag{8}$$

We first consider the equation for u. Using the form of $u(x,y)$ in Proposition 4.3 and substituting (8) into (7) yields

$$\begin{aligned} u(x+s,0) - u(x,0) - u(s,0) =& ((a-a')sx + \frac{1}{2}as^2 - bs + a_s)y \\ & + a(sx^3 + 2s^2x^2 + \frac{3}{2}s^3x) + \frac{2}{3}a'sx^3 \\ & - b(sx^2 + \frac{3}{2}s^2x) - csx - a_sx^2 + b_sx. \end{aligned} \tag{9}$$

Since the left-hand side is independent of y we infer

(10)
$$\begin{aligned} a &= a', \\ a_s &= -\frac{1}{2}a's^2 + bs. \end{aligned}$$

The right-hand side in (9) then becomes

$$a'(\frac{5}{3}sx^3 + \frac{5}{2}s^2x^2 + \frac{3}{2}s^3x) - b(2sx^2 + \frac{3}{2}s^2x) - csx + b_s x$$

Furthermore, the left-hand side is symmetrical in x and s. Equating the above expression with the one obtained by interchanging x and s and then substituting $x = 1$ gives us

(11)
$$b_s = (b_1 + \frac{1}{2}b - \frac{1}{6}a')s - \frac{1}{2}bs^2 + \frac{1}{6}a's^3.$$

Now (9) becomes

$$\begin{aligned} u(x+s,0) =& u(x,0) + u(s,0) \\ &+ (b_1 + \frac{1}{2}b - \frac{1}{6}a' - c)sx - 2b(sx^2 + s^2x) + \frac{5}{3}a'(sx^3 + \frac{3}{2}s^2x^2 + s^3x). \end{aligned}$$

Hence by Lemma 4.1

$$u(x,0) = (\alpha + d)x + \frac{1}{2}(b_1 + \frac{1}{2}b - \frac{1}{6}a' - c)x^2 - \frac{2}{3}bx^3 + \frac{5}{12}a'x^4$$

for some $\alpha \in \mathbb{F}$, (with d as in Proposition 4.3). By using Prop.4.3, we finally have

(12)
$$\begin{aligned} u(x,y) =& a'(\frac{1}{2}y^2 - x^2y + \frac{5}{12}x^4) + b(xy - \frac{2}{3}x^3) \\ &+ c(y - x^2) + \frac{1}{2}(b_1 + \frac{1}{2}b - \frac{1}{6}a' + c)x^2 + (\alpha + d)x. \end{aligned}$$

We now consider the equation for v. Substituting (8), (10), (11), and (12) into (7) we obtain

(13)
$$\begin{aligned} v(x+s,0) - v(x,0) - v(s,0) =& (b_1 + \frac{1}{2}b - \frac{1}{6}a' + c)sy \\ &+ a'(sx^4 + 2s^2x^3 + 2s^3x^2 + s^4x) \\ &- b(sx^3 + \frac{3}{2}s^2x^2 + s^3x) \\ &+ (b_1 + \frac{1}{2}b - \frac{1}{6}a')(s^2x + \frac{1}{2}sx^2) - \frac{1}{2}csx^2 \\ &+ \alpha sx. \end{aligned}$$

Since the left-hand side is independent of y we infer

$$b_1 + \frac{1}{2}b - \frac{1}{6}a' + c = 0,$$

and (13) becomes

$$\begin{aligned} v(x+s,0) =& v(x,0) + v(s,0) \\ &+ a'(sx^4 + 2s^2x^3 + 2s^3x^2 + s^4x) - b(sx^3 + \frac{3}{2}s^2x^2 + s^3x) \\ &- c(sx^2 + s^2x) + \alpha sx. \end{aligned}$$

As mentioned before we need only $a' = 0$ for the proof of the proposition; in Proposition 5.2 we will have $p > 5$. So Lemma 4.1 can be applied in any case. Thus

$$v(x,0) = \beta x + \frac{1}{2}\alpha x^2 - \frac{1}{3}cx^3 - \frac{1}{4}bx^4 + \frac{1}{5}a'x^5$$

for some $\beta \in \mathbb{F}$. From Proposition 4.3 we finally obtain

$$v(x,y) = a'(\frac{1}{5}x^5 - \frac{1}{3}x^3y) + b(\frac{1}{2}y^2 - \frac{1}{4}x^4) - \frac{1}{3}cx^3 + dy + \frac{1}{2}\alpha x^2 + \beta x. \tag{14}$$

This proves the stated form of u and v (because $a' = 0$ in this case). □

To distinguish between $\mathbb{F}^2 = \mathbb{F} \times \mathbb{F}$ and the set of squares of $\mathbb{F}$ we denote the latter set by $\mathbb{F}_2$.

Proposition 4.5. *$\alpha = \beta = 0$ in Proposition 4.4. In particular, there is only a 1-dimensional subspace of infinite points fixed by Σ.*

Proof. Since $f - cg_1 - dg_2$ describes a circle if f does so, we may assume that $c = d = 0$. Let

$$\begin{aligned} &h_2 : \mathbb{F}^2 \to \mathbb{F}^2 : (x,y) \mapsto (xy - \frac{2}{3}x^3, \frac{1}{2}y^2 - \frac{1}{4}x^4), \quad \text{and} \\ &k_1 : \mathbb{F}^2 \to \mathbb{F}^2 : (x,y) \mapsto (x, \frac{1}{2}x^2), \\ &k_2 : \mathbb{F}^2 \to \mathbb{F}^2 : (x,y) \mapsto (0,x). \end{aligned} \tag{15}$$

With this notation Proposition 4.4 implies that $f = bh_2 + \alpha k_1 + \beta k_2$ is the describing function of a circle. If $b = 0$, then the circle $K_{\alpha k_1 + \beta k_2}$ intersects $K_{(0,0)} = \{(z,0) | \; z \in \mathbb{F}^2 \cup \{\infty\}\}$ in at least the points $(0,y,0,0)$ for arbitrary $y \in \mathbb{F}$. Thus $\alpha = \beta = 0$ in this case.

We now assume that $b \neq 0$. Since K_{rf} is also a circle if K_f is one, we may even assume that $b = 1$. We consider the intersection of the circles $K_{h_2 + \alpha k_1 + \beta k_2}$ and

$K_{(0,\frac{1}{2}r^2)}$ for suitable $r \in \mathbb{F}$. To find the points of intersection we solve the system of equations

$$(16)\qquad \begin{aligned} xy - \frac{2}{3}x^3 + \alpha x &= 0 \\ \frac{1}{2}y^2 - \frac{1}{4}x^4 + \frac{1}{2}\alpha x^2 + \beta x &= \frac{1}{2}r^2 \end{aligned}$$

in x and y. The first equation yields

$$x = 0 \quad \text{or} \quad y = \frac{2}{3}x^2 - \alpha.$$

The first alternative gives us the two solutions $(0, \pm r)$ if $r \neq 0$. The second alternative leads to the equation

$$x^4 + 6\alpha x^2 - 36\beta x + 18(r^2 - \alpha^2) = 0.$$

Note that there can be at most two distinct solutions of (16) because such a solution corresponds to a point of intersection of two different circles in the Laguerre plane. Hence, the above equation must have no solution or precisely one solution if $r \neq 0$ or $r = 0$ respectively, since the corresponding circles pass through different infinite points.

We begin with the case $\beta \neq 0$. Since $x \mapsto x^3$ is a permutation of $\mathbb{F}$, we can write β as $\beta = \frac{1}{24}\xi^3$ for some $\xi \in \mathbb{F}^*$; we set $r = \alpha - \frac{1}{6}\xi^2$. If $\alpha \neq \frac{1}{6}\xi^2$, then the equations (16) have the three solutions $(0, \pm r)$, and $(\xi, \frac{2}{3}\xi^2 - \alpha)$. Similarly, if $\alpha = \frac{1}{6}\xi^2$, we find the three solutions $(0,0)$, $(\xi, \frac{1}{2}\xi^2)$, and $(\frac{1}{6}\xi(\rho^2 - 2\rho - 2), \frac{1}{6}\xi^2(2\rho - 5))$ where $\rho = \sqrt[3]{10} \in \mathbb{F}$. (Note that $x \mapsto x^3$ is a permutation of $\mathbb{F}$ and that $\xi \neq \frac{1}{6}\xi(\rho^2 - 2\rho - 2)$ as $p \neq 2, 3$.)

We now assume that $\beta = 0$ and $\alpha \neq 0$. If $-6\alpha \in \mathbb{F}_2$, i.e. $-6\alpha = \rho_1^2$ for some $\rho_1 \in \mathbb{F}$, we set $r = \alpha$ and we obtain the four solutions $(0, \pm\alpha)$, and $(\pm\rho_1, -5\alpha)$. If finally $-6\alpha \notin \mathbb{F}_2$, then $2\alpha = \rho_2^2$ for some $\rho_2 \in \mathbb{F}$ (note that $-3 \notin \mathbb{F}_2$). For $r = \frac{1}{3}\alpha$ we have the four solutions $(0, \pm r)$, $(\pm\rho_2, r)$.

In any case we have at least three solutions of the system (16). As this is not possible in a Laguerre plane, the parameters α and β must be both 0. Thus there enter only three parameters in the describing function f. Up to functions that describe a line only multiples of the special function h_2 occur. So the subspace of infinite points fixed by Σ must be 1-dimensional. □

In a Laguerre plane the circle K_{h_2} must induce an oval

$$\mathcal{O}_2 = \{(x, y, xy - \frac{2}{3}x^3, \frac{1}{2}y^2 - \frac{1}{4}x^4) \mid x, y \in \mathbb{F}\} \cup \{\omega\}$$

in the dual Betten-Walker plane over $\mathbb{F}$ (= derived projective plane at $(\infty, 0)$). This allows us to exclude some of the possible primes p.

Proposition 4.6. *If $\mathcal{O}_2$ describes an oval in the dual Betten-Walker plane over $\mathbb{F}$, then -1 and -2 are non-squares in $\mathbb{F}$ and $p \equiv -1 \pmod{24}$.*

Proof. The intersection of $\mathcal{O}_2$ with the horizontal line

$$\{(x, y, 0, -\frac{1}{36}) \mid x, y \in \mathbb{F}\}$$

gives the system of equations

$$\begin{aligned} xy - \frac{2}{3}x^3 &= 0 \\ \frac{1}{2}y^2 - \frac{1}{4}x^4 &= -\frac{1}{36} \end{aligned}$$

in x and y. The first equation yields

$$x = 0 \quad \text{or} \quad y = \frac{2}{3}x^2.$$

The first alternative gives us

$$x = 0, \quad y^2 = -\frac{1}{18}; \tag{17}$$

the second case leads to

$$y = \frac{2}{3}x^2, \quad x^4 = 1 \tag{18}$$

which gives us the two solutions $(\pm 1, \frac{2}{3})$. Then (17) cannot contribute a solution, hence $-\frac{1}{18} \notin \mathbb{F}_2$ or equivalently -2 is a non-square in $\mathbb{F}$. Similarly, if $-1 = i^2$ for some $i \in \mathbb{F}$, then (18) yields the two additional solutions $(\pm i, -\frac{2}{3})$ which is not possible. This shows that $-1, -2$ and -3 (see 3.4) are non-squares in $\mathbb{F}$. From [6, Theorems 82, 95, 96] it readily follows that $p \equiv -1 \pmod{24}$. □

Corollary 4.7. *A finite elation Laguerre plane of order p^2, $p \not\equiv -1 \pmod{24}$ that admits an automorphism group of order p^2 in the elation complement is Miquelian.*

Remark 4.8. Obviously, vertical lines intersect $\mathcal{O}_2$ in at most two points. Using the group Σ and other simplifications, it suffices to consider only the intersections of $\mathcal{O}_2$ with the horizontal lines $\{(x, y, \frac{1}{3}, \frac{1}{4}a) \mid x, y \in \mathbb{F}\}$ for $a \in \mathbb{F}$ instead of all non-vertical lines. Then $\mathcal{O}_2$ describes an oval in the dual Betten-Walker plane over $\mathbb{F} = GF(p)$, $p \equiv -1 \pmod{24}$, if and only if each polynomial

$$X^6 - 8X^3 + 9aX^2 - 2$$

has at most two distinct roots in F for all $a \in \mathbb{F}$. It is easy to see that this polynomial has no multiple roots except when $a = 1$. In this case $X^6 - 8X^3 + 9X^2 - 2 = (X-1)^3(X^3 + 3X^2 + 6X + 2)$ and the cubic factor has precisely one root in $\mathbb{F}$.

A computer search for roots of the above polynomials in $\mathbb{F} = GF(p)$, where $p \equiv -1 \pmod{24}$ and $p < 10000$, always found at least three distinct roots in $\mathbb{F}$ for some a. We therefore conjecture that $\mathcal{O}_2$ never describes an oval in a dual Betten-Walker plane of odd order. If this were true our Theorem would be already proved at this stage.

5. Equations of Circles Through a General Infinite Point

In this section we determine the form all circles of the possible Laguerre plane. We keep the notation of the preceding sections. In particular, we assume the general hypotheses 3.4, and $\mathbb{F}_2$ denotes the set of squares of $\mathbb{F} = GF(p)$. We follow a similar approach as in section 4. By Proposition 4.5 the group Σ cannot fix each infinite point so there must be subgroups $\Xi, \Lambda \leq \Sigma$ of order p such that Ξ fixes each infinite point and Λ acts equivalently to

$$\{\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \mid z \in GF(p)\}$$

on $\mid (\infty, 0) \mid \cong \mathbb{F}^2$. In the coordinatization of the infinite parallel class $\mid (\infty, 0) \mid$ as given in Proposition 2.1 this means that $\lambda \in \Lambda$ maps a circle K_f through an infinite point (∞, w_f) not fixed by λ onto a circle $K_{f+zh_2+\tilde{a}g_1+\tilde{b}g_2+\tilde{c}}$ for suitable $z, \tilde{a}, \tilde{b} \in \mathbb{F}$, $\tilde{c} \in \mathbb{F}^2$ (h_2 and g_i as in (15) and (1)); cf. 4.2, and note that K_{h_2} has coefficient vector $(0,1,0,0,0,0)$. Once we have found Ξ we can take any subgroup that intersects Ξ trivially for Λ. In the proposition below we show that Ξ must be the group Ψ as defined after 4.2.

Proposition 5.1. $\Xi = \Psi$.

Proof. Assume that $\Xi \neq \Psi$; then we may choose Ψ as the subgroup Λ. As now Ψ acts equivalently to $\{\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \mid z \in \mathbb{F}\}$ on $\mid (\infty, 0) \mid$, the automorphism ψ_{-t} maps the circle K_f to $K_{f+rth_2+a_tg_1+b_tg_2+f(0,t)}$ for suitable $r, a_t, b_t \in \mathbb{F}$, $r \neq 0$, where we assume that $f(0,0) = (0,0)$. Using the action of ψ_{-t} on points and substituting $y+t$ for y we obtain

$$(19) \qquad \begin{aligned} f(x, y+t) =& f(x,y) + rt \cdot (xy - \frac{2}{3}x^3, \frac{1}{2}y^2 - \frac{1}{4}x^4) \\ &+ a_t \cdot (y - x^2, -\frac{1}{3}x^3) + b_t \cdot (x,y) + f(0,t) \end{aligned}$$

for all $x, y, t \in \mathbb{F}$. Putting $y = 0$ yields

$$(20) \quad f(x,t) = f(x,0) + f(0,t) + rt \cdot (-\frac{2}{3}x^3, -\frac{1}{4}x^4) + a_t \cdot (-x^2, -\frac{1}{3}x^3) + b_t \cdot (x, 0).$$

Substituting $x = 0$ in (19) gives us

$$(21) \qquad f(0, y+t) = f(0,y) + f(0,t) + (a_t y, \frac{1}{2}rty^2 + b_t y).$$

The left-hand side being symmetrical in y and t implies

$$a_t y = a_y t, \quad \text{and} \quad \frac{1}{2}rty^2 + b_t y = \frac{1}{2}rt^2 y + b_y t;$$

thus

$$(22)\qquad \begin{aligned} a_t &= at, \\ b_t &= \frac{1}{2}rt^2 + bt, \end{aligned}$$

where $a = a_1, b = b_1 - \frac{1}{2}r \in \mathbb{F}$. In the sequel we only consider the function u. Substituting (22) into (21) we find

$$u(0, y + t) = u(0, y) + u(0, t) + aty.$$

From Lemma 4.1 we infer

$$u(0, y) = \frac{1}{2}ay^2 + cy$$

for some $c \in \mathbb{F}$. Then (20) gives us

$$(23)\qquad \begin{aligned} u(x, y) &= u(x, 0) + \frac{1}{2}ay^2 + cy - \frac{2}{3}rx^3y - ax^2y + \frac{1}{2}rxy^2 + bxy \\ &= \frac{1}{2}(rx + a)y^2 + R(x)y + S(x) \end{aligned}$$

where $R(x)$ is a polynomial function of degree 3 in x and $S(x)$ is some function depending only on x.

We now use the group Ξ. Since $\Sigma \simeq \mathbb{F}^2$, each non-trivial subgroup of Σ is described by a line. So there is some $\eta \in \mathbb{F}$ such that Ξ consists of all automorphisms ξ_s, $s \in \mathbb{F}$, of the form

$$(x, y, u, v) \mapsto (x + s, y + sx + \frac{1}{2}s^2 + \eta s, u, v + su).$$

As Ξ fixes every infinite point, ξ_{-s} maps the circle K_f to $K_{f+\alpha_s g_1 + \beta_s g_2 + f(s, \frac{1}{2}s^2 + \eta s)}$ for suitable $\alpha_s, \beta_s \in \mathbb{F}$, see 4.2. Using the action of ξ_{-s} on points and substituting $x + s$ for x and $y + sx + \frac{1}{2}s^2 + \eta s$ for y we obtain

$$u(x + s, y + sx + \frac{1}{2}s^2 + \eta s) = u(x, y) + \alpha_s(y - x^2) + \beta_s x + u(s, \frac{1}{2}s^2 + \eta s).$$

Substituting (23) into this equation we find for the coefficient of y^2

$$\frac{1}{2}(r(x + s) + a) = \frac{1}{2}(rx + a).$$

Hence

$$r = 0$$

contrary to the action of Ψ being equivalent to $\{\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \mid z \in \mathbb{F}\}$. This shows that $\Xi = \Psi$. $\square$

Proposition 5.2. *Assume that Ψ fixes each infinite point and let $f = (u, v)$ describe a circle. Then u and v have the following form :*

$$u(x,y) = a(\frac{1}{2}y^2 - x^2y + \frac{5}{12}x^4) + b(xy - \frac{2}{3}x^3) + c(y - x^2) + dx + e_1$$
$$v(x,y) = a(\frac{1}{5}x^5 - \frac{1}{3}x^3y) + b(\frac{1}{2}y^2 - \frac{1}{4}x^4) - \frac{1}{3}cx^3 + dy + e_2$$

for some $a, b, c, d, e_1, e_2 \in \mathbb{F}$.

Proof. Without loss of generality we may assume that $f(0,0) = (0,0)$. From the proof of Proposition 4.4 (see (12) and (14), note that $p > 5$) we already know

$$u(x,y) = a(\frac{1}{2}y^2 - x^2y + \frac{5}{12}x^4) + b(xy - \frac{2}{3}x^3) + c(y - x^2) + dx + \alpha x$$
$$v(x,y) = a(\frac{1}{5}x^5 - \frac{1}{3}x^3y) + b(\frac{1}{2}y^2 - \frac{1}{4}x^4) - \frac{1}{3}cx^3 + dy + \frac{1}{2}\alpha x^2 + \beta x$$

for suitable $a, b, c, d, \alpha, \beta \in \mathbb{F}$ (here we write again a instead of a'). Since $f - bh_2 - cg_1 - dg_2$ describes a circle if f does so, we may assume that $b = c = d = 0$. Analogously to the proof of Proposition 4.5 we obtain $\alpha = \beta = 0$ if $a = 0$, and as there we may assume that $a = 1$ if $a \neq 0$. Let

$$h_1 : \mathbb{F}^2 \to \mathbb{F}^2 : (x,y) \mapsto (\frac{1}{2}y^2 - x^2y + \frac{5}{12}x^4, \frac{1}{5}x^5 - \frac{1}{3}x^3y). \tag{24}$$

We consider the intersection of the circles $K_{h_1+\alpha k_1+\beta k_2}$ and $K_{(\frac{1}{2}r^2,0)}$ for suitable $r \in \mathbb{F}$, where k_1 and k_2 are as in (15). To find the points of intersection we solve the system of equations

$$\begin{aligned} \frac{1}{2}y^2 - x^2y + \frac{5}{12}x^4 + \alpha x &= \frac{1}{2}r^2 \\ \frac{1}{5}x^5 - \frac{1}{3}x^3y + \frac{1}{2}\alpha x^2 + \beta x &= 0 \end{aligned} \tag{25}$$

in x and y. The second equation yields

$$x = 0 \quad \text{or} \quad \frac{1}{3}x^2y = \frac{1}{5}x^4 + \frac{1}{2}\alpha x + \beta.$$

The first alternative results in the two solutions $(0, \pm r)$ if $r \neq 0$. After multiplying the first equation in (25) by x^4 the second alternative leads to the equation

$$x^8 - 120\alpha x^5 + 30(5r^2 + 12\beta)x^4 - 1350(\frac{1}{2}\alpha x + \beta)^2 = 0. \tag{26}$$

Note that there can be at most two distinct solutions of (25) as we intersect different circles in the Laguerre plane. Hence the above equation must have no solution or precisely one solution if $r \neq 0$ or $r = 0$ respectively.

We begin with the case $\alpha \neq 0$. Since the map $x \mapsto x^3$ is a permutation of $\mathbb{F}$, we can write α as $\alpha = \frac{1}{12}\xi^3$ for some $\xi \in \mathbb{F}^*$. If $\beta \neq \frac{11}{120}\xi^4$, let $r = \frac{3\beta}{\xi^2} - \frac{11}{40}\xi^2$; then the equations (25) have the three solutions $(0, \pm r)$, and $(\xi, r + \xi^2)$. If $\beta = \frac{11}{120}\xi^4$, we distinguish between the cases $157 \notin \mathbb{F}_2$ and $157 \in \mathbb{F}_2$. In the first case let $r = \frac{1}{32}\rho_1\xi^2$ where $\rho_1 \in \mathbb{F}$ such that ${\rho_1}^2 = -3 \cdot 157$ (note that $-3 \notin \mathbb{F}_2$); then we find the three solutions $(0, \pm r)$, and $(-2\xi, \frac{77}{32}\xi^2)$. In the second case let $r = \frac{1}{24}\rho_2\xi^2$ where $\rho_2 \in \mathbb{F}$ such that ${\rho_2}^2 = 6 \cdot 157$ (note that $6 \in \mathbb{F}_2$ by Proposition 4.6); we then obtain the three solutions $(0, \pm r)$, and $(\frac{1}{2}\xi, \frac{3}{2}\xi^2)$.

We now assume that $\alpha = 0$ and $\beta \neq 0$ and we set $r = 0$ in (25). Then (26) becomes a quadratic equation in x^4

$$x^8 + 360\beta x^4 - 1350\beta^2 = 0.$$

Since $6 \in \mathbb{F}_2$ and $-1 \notin \mathbb{F}_2$, there is an $\eta \in \mathbb{F}$, $\eta^2 = 6$ such that $\rho = 15(-12 + 5\eta)\beta \in \mathbb{F}_2$ (note that $15(-12 + 5\eta)\beta \cdot 15(-12 - 5\eta)\beta = -6(15\beta)^2 \notin \mathbb{F}_2$). Furthermore, we may choose $\zeta \in \mathbb{F}$ such that $\rho = \zeta^4$. (Because $-1 \notin \mathbb{F}_2$ and $\rho \in \mathbb{F}_2$ one of the two roots of $X^2 - \rho$ is a square in $\mathbb{F}$.) Then we obtain the three solutions $(0,0)$, $(\zeta, (1 + \frac{1}{6}\eta)\zeta^2)$, and $(-\zeta, (1 + \frac{1}{6}\eta)\zeta^2)$.

In any case we have at least three solutions of the system (25). As this is not possible in a Laguerre plane, the parameters α and β must be both 0. □

In a Laguerre plane the circle K_{h_1} must induce an oval

$$\mathcal{O}_1 = \{(x, y, \frac{1}{2}y^2 - x^2y + \frac{5}{12}x^4, \frac{1}{5}x^5 - \frac{1}{3}x^3y) \mid x, y \in \mathbb{F}\} \cup \{\omega\}$$

in the dual Betten-Walker plane over $\mathbb{F}$ (= derived projective plane at $(\infty, 0)$). As in Proposition 4.6 this allows us to obtain further restrictions on the possible primes p. Using the Hasse-Weil theorem for equations over $GF(p)$, to which D.G. Glynn called my attention, we will eventually exclude the occurence of a dual Betten-Walker plane as derived projective plane altogether.

Lemma 5.3. *If $\mathcal{O}_1$ describes an oval in the dual Betten-Walker plane over $\mathbb{F} = GF(p)$, $p \equiv -1 \pmod{24}$, then*

$$g(X) = X^4 + 6X^3 + 21X^2 + 26X + 21 \tag{27}$$

must map $\mathbb{F}$ into $\mathbb{F}_2$, i.e. $g(x)$ is a square for all $x \in \mathbb{F}$.

In particular, 7 is a square in $\mathbb{F}$ and $p \geq 47$.

Proof. We consider the intersection of $\mathcal{O}_1$ with a line of the form

$$\{(x, y, -\frac{1}{3}x + \frac{1}{2}b^2 + \frac{1}{4}, -\frac{1}{3}y + \frac{1}{5}) \mid x, y \in \mathbb{F}\}$$

for some $b \in \mathbb{F}$ (the line corresponding to the circle $K_{-\frac{1}{3}g_2+(\frac{1}{2}b^2+\frac{1}{4},\frac{1}{5})}$). Now we obtain the system of equations

$$(28)\qquad \begin{aligned} \frac{1}{2}y^2 - x^2y + \frac{5}{12}x^4 &= -\frac{1}{3}x + \frac{1}{2}b^2 + \frac{1}{4} \\ \frac{1}{5}x^5 - \frac{1}{3}x^3y &= -\frac{1}{3}y + \frac{1}{5}. \end{aligned}$$

The second equation yields

$$x = 1 \quad \text{or} \quad y(x^2+x+1) = \frac{3}{5}(x^4+x^3+x^2+x+1).$$

In the first case we find two solutions $(1, 1 \pm b)$. After multiplying the first equation in (28) by $(x^2+x+1)^2$ the second alternative leads to

$$(29)\qquad \begin{aligned} (x-1)^4(x^4+6x^3+21x^2+26x+21) &= -150b^2(x^2+x+1)^2, \\ y(x^2+x+1) &= \frac{3}{5}(x^4+x^3+x^2+x+1). \end{aligned}$$

Note that $x^2+x+1 \neq 0$ for all $x \in \mathbb{F}$; so any solution of the first equation in (29) leads to a point of intersection. Since b can be chosen arbitrarily, the first equation in (27) cannot have a solution. Thus

$$g(x) = x^4 + 6x^3 + 21x^2 + 26x + 21 \in \mathbb{F}_2$$

for all $x \in \mathbb{F}$ (note that $g(1) = 75 = (-1)\cdot(-3)\cdot 5^2 \in \mathbb{F}_2$).

Therefore $g(0) = 21 = 3 \cdot 7$, and thus 7 must be a square in $\mathbb{F}$. Using the law of quadratic reciprocity (see [6, §6.12]), one finds that p must be congruent to -1, -2, or 3 modulo 7. But then $p \equiv -1, -25$, or 47 (mod 168). In particular, $p \geq 47$. □

Proposition 5.4. *$\mathcal{O}_1$ is no oval in the dual Betten-Walker plane over $GF(p)$, $p \equiv -1 \pmod{24}$.*

Proof. We show that there must be some $x \in \mathbb{F}$ such that $g(x) \notin \mathbb{F}_2$, where $g(X)$ denotes the polynomial in (27). We study the polynomial

$$G(X,Y) = Y^2 - g(X)$$

in two indeterminates X and Y. Suppose that $G(X,Y)$ is reducible over the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. A factorization must have the form $(Y - h(X))\cdot(Y + h(X))$ for some polynomial $h(X) \in \overline{\mathbb{F}}[X]$. Thus $g(X) = h(X)^2$ and $h(X)$ is of degree 2, i.e. without loss of generality $h(X) = X^2 + aX + b$ for some $a, b \in \overline{\mathbb{F}}$. A comparison of the coefficients of X^3 and X^2 in $g(X)$ and $h(X)^2$ respectively yields $a = 3$, $b = 6$. But then $h(X)^2 = g(X) + 10X + 15$ and $g(X) = h(X)^2$ if and only if $p = 5$. Since $p \geq 47$ by Lemma 5.3, it follows that $G(X,Y)$ is absolutely irreducible.

According to the Hasse-Weil Theorem for equations over $GF(p)$ (see [7, Thm 10.2.1] for a projective version, compare also [9]) the number of solutions of the equation $G(X,Y) = 0$ is at most $p + 1 + 2\gamma\sqrt{p}$ where γ denotes the genus of G. Since the degree of $G(X,Y)$ is 4, one obtains that $\gamma \leq 3$, cf. [7, §10.2].

We now assume that $g(x) \in \mathbb{F}_2$ for all $x \in \mathbb{F}$. Since $g(X)$ has at most four roots in $\mathbb{F}$ and because $g(X)$ has no multiple roots, this assumption implies that the equation $G(X,Y) = 0$ has at least $2p-4$ solutions. Hence $2p-4 \leq p+1+6\sqrt{p}$, and so $p < 46$ contrary to $p \geq 47$ by Lemma 5.3. This proves that there is some $x \in \mathbb{F}$ such that $g(x) \notin \mathbb{F}_2$. Consequently, $\mathcal{O}_1$ is not an oval. □

Proposition 5.4 and Corollary 4.7 now prove the Theorem of Section 1.

Remark 5.5. Let $\mathbb{E}$ be a field of characteristic $\neq 2, 3, 5$. For $z = (x,y) \in \mathbb{E}^2$ let $D(z)$ be the 6×2 matrix

$$D(z) = \begin{pmatrix} \frac{1}{2}y^2 - x^2y + \frac{5}{12}x^4 & \frac{1}{5}x^5 - \frac{1}{3}x^3y \\ xy - \frac{2}{3}x^3 & \frac{1}{2}y^2 - \frac{1}{4}x^4 \\ y - x^2 & -\frac{1}{3}x^3 \\ x & y \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and define

$$D(\infty) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}^t .$$

Let $\mathcal{L}(\mathbb{E})$ denote the following incidence structure: The point set is $P = (\mathbb{E}^2 \cup \{\infty\}) \times \mathbb{E}^2$, the set of circles is $\mathcal{K}(\mathbb{E}) = \{K_c \mid c \in \mathbb{E}^6\}$ where $K_c = \{(z, c \cdot D(z)) \in P \mid z \in \mathbb{E}^2 \cup \{\infty\}\}$. Two points (z,w) and (u,v) are parallel if and only if $z = u$. That is, $\mathcal{L}(\mathbb{E})$ is constructed analogously to the elation Laguerre plane as given in Proposition 2.1. Then the full collineation group of the dual Betten-Walker plane is induced by the stabilizer of the infinite point $(\infty, 0)$.

As shown in [11, §8] one obtains indeed a Laguerre plane for $\mathbb{E}$ being the field of reals. Furthermore, it readily follows that one also obtains a Laguerre plane for the field of all real algebraic numbers. Since $\mathcal{L}(\mathbb{E}')$, $\mathbb{E}'$ a finite subfield of $\mathbb{E}$, is a Laguerre plane if $\mathcal{L}(\mathbb{E})$ is one, the main theorem shows that $\mathcal{L}(\mathbb{E})$ can only be a Laguerre plane if $\mathbb{E}$ has characteristic 0.

References

1. D. Betten, *4-dimensionale Translationsebenen mit 8-dimensionaler Kollineationsgruppe*, Geom. Dedicata **2** (1973), 327–339.
2. M. Biliotti, V. Jha, N.L. Johnson, and G. Menichetti, *A structure theory for two-dimensional translation planes of order q^2 that admit a collineation group of order q^2*, Geom. Dedicata **29** (1989), 7–43.
3. L.R.A. Casse, J.A. Thas and P.R. Wild, *(q^n+1)-sets of $PG(3n-1,q)$, generalized quadrangles and Laguerre planes*, Simon Stevin **59** (1985), 21–42.
4. Y. Chen and G. Kaerlein, *Eine Bemerkung über endliche Laguerre- und Minkowski-Ebenen*, Geom. Dedicata **2** (1973), 193–194.
5. M. Hall, *The Theory of Groups*, 2^{nd} Edition, Chelsea, New York, 1976.
6. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5^{th} Edition, Clarendon Press, Oxford, 1979.
7. J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.
8. N.L. Johnson and F.W. Wilke, *Translation planes of order q^2 that admit a collineation group of order q^2*, Geom. Dedicata **15** (1984), 293–312.
9. W.M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Mathematics, vol. 536, Springer Verlag, Berlin, Heidelberg, New York, 1976.
10. B. Segre, *Ovals in a finite projective plane*, Canad. J. Math. **7** (1955), 414–416.
11. G.F. Steinke, *Eine Klassifikation 4-dimensionaler Laguerre-Ebenen mit grosser Automorphismengruppe*, Habilitationsschrift, Kiel, 1987.
12. G.F. Steinke, *On the structure of finite elation Laguerre planes*, J. Geom. **41** (1991), 162–179.
13. G.F. Steinke, *A remark on Benz planes of order 9*, Ars Comb. (to appear).
14. M. Walker, *A class of translation planes*, Geom. Dedicata **5** (1976), 135–146.

(Received 10/12/90; revised 20/7/92)