Note di Matematica
Note Mat. 28 (2008), n. 2, 175-185
ISSN 1123-2536, e-ISSN 1590-0932
DOI 10.1285/i15900932v28n2p175
http://siba-ese.unisalento.it, © 2008 Università del Salento

Matrix forms for isometries of the affine plane $AG(2,q)$ and of the corresponding Miquelian Möbius plane

Sunčica Blažev
susa7777@yahoo.com

Vlado Cigić
Fakultet strojarstva i računarstva,
University of Mostar, BiH

Received: 18/05/2006; accepted: 30/01/2008.

Abstract. We give the matrix form for the isometries of $AG(2,q)$ and the corresponding Miquelian Möbius plane depending on the choice of an irreducible polynomial of second degree over $GF(q)$. In particular we provide the above matrix form for the automorphisms of these planes preserving the set of the affine ellipses of $AG(2,q)$.

Keywords: finite affine plane, Miquelian Möbius plane, squared length, squared distance, isometry

MSC 2000 classification: 05B25

1 Introduction and preliminaries

Let $q = p^n$ be a power of the prime p.

It is known ([12]) that the affine plane $AG(2,q)$ of odd order q can be extended in the unique way (up to isomorphism) to the Möbius plane of order q denoted by $M(q)$ (in sense of extending $2-(q^2,q,1)$ design to $3-(q^2+1,q+1,1)$ design). $M(q)$ is a Miquelian Möbius plane, namely it is isomorphic to the Möbius plane of the elliptic quadric in $PG(3,q)$.

When q is even, the plane $AG(2,q)$ can be extended, in the unique way (up to isomorphism), to $M(q)$ since the group $PGL(4,q)$ is transitive on the set of all elliptic quadrics in the projective space $PG(3,q)$ (see [8]).

The plane $M(q)$ is going to be observed in the way of associating it with the projective line $PG(1,q^2)$.

According to [5], 4.3., once the frame for $PG(1,q^2)$ (a set of three different points in $PG(1,q^2)$) has been chosen the projective line $PG(1,q)$ is naturally embedded into $PG(1,q^2)$. The sublines $PG(1,q)$ of $PG(1,q^2)$ embedded into $PG(1,q^2)$ are called the *Baer sublines* (see [10]). Since $PGL(2,q^2)$ is transitive

on frames of $PG(1,q^2)$, then it is transitive on the set of all the Baer sublines of $PG(1,q^2)$. According to [2], 6.4, the incidence structure, in which the points are all points of $PG(1,q^2)$ and the circles are all the Baer sublines of $PG(1,q^2)$, together with the natural relation of incidence, is the Miquelian Möbius plane $M(q)$.

The points of $PG(1,q^2)$ can be expressed, in parametric form, as the elements of $GF(q^2)\cup\{\infty\}$. The Baer sublines $PG(1,q)$ of the line $PG(1,q^2)$ are exactly the regular Hermitian varieties of $PG(1,q^2)$ ([5], 6.2.1). According to [5], 5.1., and [4], p. 21, the circles of $M(q)$ are the sets of the form

$$\{z\in GF(q^2) : az\overline{z}+h\overline{z}+\overline{h}z+d=0\}, \tag{1}$$

where $a,d\in GF(q)$, $h\in GF(q^2)$ and $ad-h\overline{h}\neq 0$. The mapping

$$z\to\overline{z}=z^q, \qquad \text{for each } z\in GF(q^2),$$

is the unique involutory automorphism of $GF(q^2)$ ([2], 6.4.2), which is called the *conjugation* on $GF(q^2)$. Note that in case $a=0$, the circle (1) also contains the point ∞.

It is well known that we can identify the points of $AG(2,q)$ with the elements of the finite field $GF(q^2)$ and with the points of the affine line $AG(1,q^2)$. In Section 2, we show that the circles (1) of $M(q)$ with $a=0$ are exactly the lines of $AG(2,q)$ extended with the point ∞ and the circles (1) with $a\neq 0$, which we call the *regular circles*, are affine ellipses of $AG(2,q)$.

For the point z of $M(q)$ which is the vector of $2-$dim vector space $GF(q^2)$ over $GF(q)$, we define the *"squared length"* by

$$\|z\|^2 := z\overline{z}\in GF(q),$$

while for the point ∞ by definition we state

$$\|\infty\|^2 := \infty.$$

The vector $\overline{z}$ is called the *conjugated vector* of the vector z.

Likewise, for each $z,t\in GF(q^2)$, the *"squared distance"* of any two points of $AG(2,q)$ is defined by

$$d^{(2)}(z,t) := \|z-t\|^2.$$

The previous definition is extended by

$$d^{(2)}(z,\infty) := \infty \text{ and } d^{(2)}(\infty,\infty) := 0.$$

It is known ([2], 6.4.1) that the group $\mathrm{Aut}M(q) \cong P\Gamma L(2,q^2)$, which consists of the mappings

$$z \mapsto \frac{az^{\psi}+b}{cz^{\psi}+d},$$

for each $z \in GF(q^2) \cup \{\infty\}$, where $a,b,c,d \in GF(q^2)$, so that $ad-bc \neq 0$ and $\psi \in \mathrm{Aut}GF(q^2)$. $\mathrm{Aut}M(q)_{\infty} \cong A\Gamma L(1,q^2)$, where the elements of $A\Gamma L(1,q^2)$ are the automorphisms of the form

$$z \mapsto gz^{\psi}+h,$$

for each $z \in GF(q^2) \cup \{\infty\}$, $g,h \in GF(q^2)$, so that $g \neq 0$ and $\psi \in \mathrm{Aut}GF(q^2)$. These are exactly all automorphisms of $M(q)$ which send regular circles to regular circles.

The automorphisms of $M(q)$ which preserve the "squared distance" of any two points are called the *isometries*. Let ω be an isometry of $M(q)$. By the definition of the "squared distance" of two points of $M(q)$, for each $z \in GF(q^2)$, it follows

$$d^{(2)}(z^{\omega},\infty^{\omega}) = d^{(2)}(z,\infty) = \infty.$$

So, ω fixes the point ∞. Therefore, isometries of $M(q)$ send regular circles to regular circles.

In this paper, we find the matrix representations of isometries of $AG(2,q)$ and of the automorphisms of $AG(2,q)$ which send regular circles to regular circles. We will derive the vector forms of isometries (which can be found also in [11]) from the corresponding matrix forms. Our method depends on the choice of an irreducible polynomial $\lambda(x)$ over $GF(q)$.

Besides, we are going to observe the action of automorphisms of $M(q)$ and $AG(2,q)$, which send regular circles to regular circles, to the centre, to the "squared radius" (which we will define for each regular circle) and also to the "squared distance" of two points.

2 Construction of the field $GF(q^2)$ and of the planes $AG(2,q)$ and $M(q)$

Let $\lambda(x) = x^2 - ex - f \in GF(q)[x]$ be an irreducible polynomial over the finite field $GF(q)$ of order $q = p^n$, p prime. We denote the roots of $\lambda(x)$ in a quadric extension of the field $GF(q)$, by $-\alpha$ and $-\beta$. These roots are different and the discriminant $\Delta = e^2 + 4f \neq 0$ ([5], 1.4.). So, when $p = 2$, we have $e \neq 0$. It is also known ([6], [9]) that the quotient ring

$$GF(q)[x]/(\lambda(x)) \cong GF(q)[-\alpha] = \{a + (-\alpha)b \mid a,b \in GF(q)\}$$

is the field $GF(q^2)$. The set $\{1, \alpha\}$ is one of corresponding bases. Consequently, we can write elements of $GF(q^2)$ in the form $z = x + \alpha y = (x, y)$, where $x, y \in GF(q)$. If we add the point ∞ to them, according to Section 1, we get the set of all points of $M(q)$.

The group $\mathrm{Aut}GF(q^2)$ is a cyclic group of order $2n$ which consists of the mappings

$$z \mapsto z^{p^i}, \qquad 0 \leq i < 2n,$$

for each $z \in GF(q^2)$.

Considering that $(-\alpha)^q = -\beta$ ([5], 1.2.(iii)), i.e. $(-\beta)^q = -\alpha$ (using the Binomial theorem), the conjugate vector of the vector $z = x + \alpha y$ is the vector $\overline{z} = x + \beta y$. So, for each $x, y \in GF(q)$, the conjugation on $GF(q^2)$ can be written as

$$x + \alpha y \mapsto x + \beta y.$$

For the point ∞ we define $\overline{\infty} := \infty$.

It is easy to show that

$$\|z\|^2 = z\overline{z} = (x + \alpha y)(x + \beta y) = x^2 - exy - fy^2$$

for any vector of the form $z = x + \alpha y$ in the Möbius plane $M(q)$. Likewise, the "squared distance" of any two points $z_1 = x_1 + \alpha y_1 = (x_1, y_1)$ and $z_2 = x_2 + \alpha y_2 = (x_2, y_2)$ of the field $GF(q^2)$ is

$$d^{(2)}(z_1, z_2) = \|z_2 - z_1\|^2 = (x_2 - x_1)^2 - e(x_2 - x_1)(y_2 - y_1) - f(y_2 - y_1)^2.$$

From the irreducibility of $\lambda(x) = x^2 - ex - f \in GF(q)[x]$, it follows that

$$\begin{aligned} \|z\|^2 = 0 \Leftrightarrow z = 0, \text{ where } z \in GF(q^2) \text{ and} \\ d^{(2)}(z, w) = 0 \Leftrightarrow z = w, \quad \text{for each } z, w \in GF(q^2) \cup \{\infty\}. \end{aligned}$$

From (1), it can be derived, that the circles of $M(q)$ are all the lines of $AG(2, q)$ extended with the point ∞, i.e. the sets

$$\begin{aligned} &\big\{(x, y) \in GF(q^2) \mid y = ax + b\big\} \cup \{\infty\}, \\ &\big\{(x_0, y) \in GF(q^2) \mid y \in GF(q)\big\} \cup \{\infty\}, \end{aligned}$$

where $x_0, a, b \in GF(q)$, along with the regular circles:

$$\mathcal{K}\left((x_0, y_0), R\right) = \big\{(x, y) \mid (x - x_0)^2 - e(x - x_0)(y - y_0) - f(y - y_0)^2 = R\big\}$$

where $(x_0, y_0) \in GF(q^2)$ and $R \in GF(q)^* = GF(q)\backslash\{0\}$. We say that the regular circle $\mathcal{K}\left((x_0, y_0), R\right) \in AG(2, q)$ has the *"squared radius"* R and the

centre (x_0, y_0). It is obvious that the regular circle $\mathcal{K}(z_0, R)$ of the plane $M(q)$ is the set of the points of $M(q)$ whose the "squared distance" from the centre z_0 is equal to R. Hence,

$$\mathcal{K}(z_0, R) = \left\{ z \in GF(q^2) \mid \|z - z_0\|^2 = R \right\}.$$

It is easy to show that the regular circles are ellipses in $PG(2,q)$.

Furthermore, the Miquelian Möbius plane $M(q)$ can be obtained by stereographic projection of the Möbius plane of the elliptic quadric

$$\mathcal{O} = \{\langle (x_1, x_2, x_3, x_4)\rangle \mid x_1^2 - ex_1x_2 - fx_2^2 = x_3x_4\} \subset PG(3,q)$$

from the pole $\langle (0,0,1,0)\rangle$ to the affine plane $x_3 = 0$ (the pole is mapped to the point ∞).

Henceforth, we suppose that coefficients of polynomial $\lambda(x)$ are the elements of the prime subfield of the field $GF(q)$, i.e. $\lambda(x) = x^2 - ex - f \in GF(p)[x]$. Let us observe the automorphisms of the field $GF(q^2)$.

1 Lemma. *A mapping $\psi : GF(q^2) \to GF(q^2)$ is an automorphism of $GF(q^2)$ if and only if for each $x, y \in GF(q)$ it can be written as*

$$(x + \alpha y)^\psi = x^\phi + \alpha y^\phi \tag{2}$$

or

$$(x + \alpha y)^\psi = x^\phi + \beta y^\phi, \tag{3}$$

where $\phi \in \mathrm{Aut}GF(q)$.

Proof. Let ϕ be an automorphism of $GF(q)$. If we define $\psi : GF(q^2) \to GF(q^2)$ as in (2) or (3), it is not difficult to show (using $\alpha^2 = -e\alpha + f$, $\beta^2 = -e\beta + f$, $e^\phi = e$, $f^\phi = f$) that ψ is an automorphism of the finite field $GF(q^2)$ with the property $GF(q)^\psi = GF(q)^\phi = GF(q)$.

To prove the reverse, suppose ψ is an automorphism of $GF(q^2)$. Let us show that ψ is of the form (2) or (3). It is obvious that $(GF(q))^\psi = GF(q)$, since $GF(q)$ is the unique subfield of order q, of the field $GF(q^2)$. So if we define $\phi := \psi|GF(q)$, it follows that $\phi \in \mathrm{Aut}GF(q)$ and $(x + \alpha y)^\psi = x^\phi + \alpha^\psi y^\phi$, for each $x, y \in GF(q)$. To prove the assertion, it is only necessary to prove the bijectivity of the automorphism ψ on the set $\{-\alpha, -\beta\}$ of the roots of $\lambda(x)$.

Let $s(x) = a_m x^m + \cdots + a_1 x + a_0 \in GF(q^2)[x]$ be a polynomial over $GF(q^2)$. When we define $\overline{\psi}(s(x)) := a_m^\psi x^m + \cdots + a_1^\psi x + a_0^\psi$ then $\overline{\psi}$ is an automorphism of the ring $GF(q^2)[x]$ of polynomials over $GF(q^2)$. It is easy to show that $\gamma \in GF(q^2)$ is a root of $s(x)$ if and only if $\gamma^\psi \in GF(q^2)$ is a root of $\overline{\psi}(s(x))$.

Since each automorphism of $GF(q^2)$ fixes $e, f \in GF(p)$, we conclude that

$$\overline{\psi}(\lambda(x)) = x^2 - e^{\phi}x - f^{\phi} = x^2 - ex - f = \lambda(x).$$

So $(-\alpha)^{\psi}$, $(-\beta)^{\psi}$ are the roots of $\lambda(x)$ in $GF(q^2)$, i.e. ψ is a bijection on the set $\{-\alpha, -\beta\}$ of the roots of $\lambda(x)$. Hence, the claim is proven. QED

3 Automorphisms of the planes $AG(2,q)$ and $M(q)$ which send regular circles to regular circles

Let $(x, y) \in GF(q^2)$ be arbitrary. It is well known that the group $A\Gamma L(2,q)$ of all automorphisms of $AG(2,q)$ consists exactly of mappings

$$(x, y) \to (x^{\phi}, y^{\phi}) \begin{pmatrix} a & c \\ b & d \end{pmatrix} + (r, s), \tag{4}$$

where $r, s, a, b, c, d \in GF(q)$, $ad - bc \neq 0$ and $\phi \in \mathrm{Aut}GF(q)$.

In Section 1, we have seen that all automorphisms of $M(q)$ which send regular circles to regular circles are exactly automorphisms

$$z \mapsto gz^{\psi} + h, \tag{5}$$

for each $z \in GF(q^2) \cup \{\infty\}$, where $g, h \in GF(q^2)$, such that $g \neq 0$ and $\psi \in \mathrm{Aut}GF(q^2)$.

Let us observe the matrix representations of these automorphisms.

2 Theorem. *An automorphism of $AG(2,q)$ sends regular circles to regular circles if and only if for each $(x, y) \in GF(q^2)$ its matrix form is*

$$(x, y) \to (x^{\phi}, y^{\phi}) \begin{pmatrix} k & l \\ fl & k - el \end{pmatrix} + (r, s) \tag{6}$$

or

$$(x, y) \to (x^{\phi}, y^{\phi}) \begin{pmatrix} k & l \\ -fl - ek & -k \end{pmatrix} + (r, s), \tag{7}$$

where $\phi \in \mathrm{Aut}GF(q)$ and $r, s, k, l \in GF(q)$, satisfying $k^2 - ekl - fl^2 \neq 0$. All these automorphisms form a subgroup of $A\Gamma L(2,q)$ of order $2nq^2(q^2 - 1)$.

Proof. We have seen that each automorphism of $AG(2,q)$ which sends regular circles to regular circles, if we additionally define it to fix the point ∞, can be written in the form (5). Let ω be one of such automorphisms.

Let us label $z := x + \alpha y = (x, y)$, $g := k + \alpha l = (k, l)$ and $h := r + \alpha s = (r, s)$, where x, y, k, l, r, s are the elements of the field $GF(q)$.

Considering that $g \neq 0$ and $\lambda(x) = x^2 - ex - f \in GF(p)[x]$ is an irreducible polynomial over $GF(q)$, it is obvious that $\|g\|^2 = k^2 - ekl - fl^2 \neq 0$.

We have also seen (Lemma 1) that the automorphism $\psi \in \mathrm{Aut}GF(q^2)$ associated with ω, can be written as (2) or (3). Let us suppose that (2) holds, i.e. $(x+\alpha y)^\psi = x^\phi + \alpha y^\phi$, for each $x, y \in GF(q)$, where $\phi = \psi | GF(q) \in \mathrm{Aut}GF(q)$.

If we use $0 = \lambda(-\alpha) = \alpha^2 + e\alpha - f$ then, from (5), it follows

$$\begin{aligned}\omega(x+\alpha y) &= (k+\alpha l)(x^\phi + \alpha y^\phi) + r + s\alpha = \\ &= kx^\phi + \alpha^2 l y^\phi + \alpha(lx^\phi + ky^\phi) + r + s\alpha = \\ &= kx^\phi + fly^\phi + \alpha(lx^\phi + ky^\phi - ely^\phi) + r + s\alpha = \\ &= (x^\phi, y^\phi)\begin{pmatrix} k & l \\ fl & k - el \end{pmatrix} + (r,s).\end{aligned}$$

Similarly if (3) holds, using the fact that $\alpha + \beta = -e$ and $\alpha\beta = -f$, we obtain (7).

To prove the reverse, let us suppose an automorphism ω of $AG(2,q)$ to be of the form (6), i.e. for each $(x,y) \in GF(q^2)$

$$\omega((x,y)) = (x^\phi, y^\phi)\begin{pmatrix} k & l \\ fl & k - el \end{pmatrix} + (r,s)$$

where $r, s, k, l \in GF(q)$, satisfying $k^2 - ekl - fl^2 \neq 0$ and $\phi \in \mathrm{Aut}GF(q)$. Since $0 = \lambda(-\alpha) = \alpha^2 + e\alpha - f$, we get

$$\begin{aligned}\omega((x,y)) &= \left(kx^\phi + fly^\phi + r, lx^\phi + (k-el)y^\phi + s\right) \\ &= (k+\alpha l)(x^\phi + \alpha y^\phi) + r + s\alpha.\end{aligned}$$

Once again, if we label $z := x + \alpha y = (x,y)$, $g := k + \alpha l = (k,l)$, $h := r + \alpha s = (r,s)$ and define $z^\psi = (x+\alpha y)^\psi := x^\phi + \alpha y^\phi$, it follows that $\psi \in \mathrm{Aut}\, GF(q^2)$, $\psi | GF(q) = \phi \in \mathrm{Aut}GF(q)$ (according to Lemma 1) and $\|g\|^2 = k^2 - ekl - fl^2 \neq 0$. Finally, we get $\omega(z) = gz^\psi + h$, so ω sends regular circles of $AG(2,q)$ to regular circles of that plane.

The proof is similar in the case when $\omega \in A\Gamma L(2,q)$ is of the matrix form (7). QED

It is very important to observe the effect of automorphisms of $AG(2,q)$ and $M(q)$ which send regular circles to regular circles, to the centre and to the "squared radius" of a regular circle. Now, we have

3 Lemma. *An automorphism $\omega \in A\Gamma L(2,q)$ of the form (6) or (7) sends the regular circle $\mathcal{K}((x_0,y_0),R)$ of the affine plane $AG(2,q)$ to the regular circle $\mathcal{K}\left((x_0,y_0)^\omega, R^\phi(k^2 - ekl - fl^2)\right)$, where $x_0, y_0 \in GF(q)$ and $R \in GF(q)^*$.*

PROOF. Let ω be an automorphism of $AG(2,q)$ with the matrix form (6), i.e.

$$\omega((x,y)) = (x^\phi, y^\phi)\begin{pmatrix} k & l \\ fl & k-el \end{pmatrix} + (r,s),$$

for each $(x,y) \in GF(q^2)$, where r,s,k,l are elements of the field $GF(q)$, such that $k^2-ekl-fl^2 \neq 0$, $\phi \in \mathrm{Aut}GF(q)$. Then, for any $(x,y) \in GF(q^2)$, we obtain $\omega((x,y)) = (kx^\phi + fly^\phi + r, lx^\phi + (k-el)y^\phi + s) = (k+l\alpha)(x^\phi + y^\phi\alpha) + (r+s\alpha)$ (using $\alpha^2 = -e\alpha + f$). For each $(x,y) \in GF(q^2)$, let us label $\omega((x,y)) = (\widetilde{x},\widetilde{y})$. Using $e^\phi = e$ and $f^\phi = f$ (since $e, f \in GF(p)$), for any point (x,y) of the circle $\mathcal{K}((x_0,y_0),R) \in AG(2,q)$, we get

$$\begin{aligned}
&(\widetilde{x}-\widetilde{x_0})^2 - e(\widetilde{x}-\widetilde{x_0})(\widetilde{y}-\widetilde{y_0}) - f(\widetilde{y}-\widetilde{y_0})^2 = [k(x-x_0)^\phi + fl(y-y_0)^\phi]^2 + \\
&\quad - e[k(x-x_0)^\phi + fl(y-y_0)^\phi][l(x-x_0)^\phi + (k-el)(y-y_0)^\phi] + \\
&\quad - f[l(x-x_0)^\phi + (k-el)(y-y_0)^\phi]^2 = \cdots = \\
&= (k^2-ekl-fl^2)\{[(x-x_0)^\phi]^2 - e(x-x_0)^\phi(y-y_0)^\phi - f[(y-y_0)^2]\}^\phi = \\
&= (k^2-ekl-fl^2)[(x-x_0)^2 - e(x-x_0)(y-y_0) - f(y-y_0)^2]^\phi = \\
&= (k^2-ekl-fl^2)R^\phi.
\end{aligned}$$

So, for each $(x,y) \in \mathcal{K}((x_0,y_0),R)$, we have

$$(\widetilde{x},\widetilde{y}) = \omega((x,y)) \in \mathcal{K}\left((x_0,y_0)^\omega, R^\phi(k^2-ekl-fl^2)\right).$$

Hence, the circle $\mathcal{K}\left((x_0,y_0)^\omega, R^\phi(k^2-ekl-fl^2)\right)$ is the image of $\mathcal{K}((x_0,y_0),R)$ under the automorphism ω.

The proof is similar in the case when ω is of the form (7). QED

4 Remark. From Lemma 3, it is obvious that automorphisms of $AG(2,q)$ which send regular circles to regular circles preserving the set of those having equal "squared radius".

5 Corollary. *An automorphism $\omega \in A\Gamma L(2,q)$ of the form (6) or (7) sends the points with the "squared distance" d to the points with the "squared distance" $d^\phi(k^2-ekl-fl^2)$. That is, for any two points $(x_1,y_1),(x_2,y_2) \in GF(q^2) \subset AG(2,q)$ we have*

$$d^{(2)}((x_1,y_1)^\omega,(x_2,y_2)^\omega) = [d^{(2)}((x_1,y_1),(x_2,y_2))]^\phi(k^2-ekl-fl^2).$$

Proof. The assertion is true if $(x_1,y_1) = (x_2,y_2)$.

In case $(x_1,y_1) \neq (x_2,y_2)$ we observe the circle with the centre (x_2,y_2) which contains the point (x_1,y_1) and the claim follows from Lemma 3. QED

6 Remark. Let us suppose ω is an automorphism of $M(q)$ which sends regular circles to regular circles, i.e. $\omega(z) = gz^{\psi}+h$, where $g,h \in GF(q^2)$, $g \neq 0$, $z \in GF(q^2) \cup \{\infty\}$, $\psi \in \mathrm{Aut}GF(q^2)$. If we use $g := k + \alpha l \in GF(q^2))$, then from Lemma 3 and the proof of Theorem 2 it follows that ω sends the regular circle $\mathcal{K}(z_0, R) \subseteq M(q)$ to the regular circle $\mathcal{K}(z_0^{\omega}, R^{\phi}\|g\|^2)$, where $z_0 \in GF(q^2)$, $R \in GF(q)^*$ and $\phi = \psi|GF(q) \in \mathrm{Aut}GF(q)$.

Also, since $(\infty)^{\omega} = \infty$, then for each $z \in GF(q^2)$ we obtain

$$d^{(2)}(z^{\omega}, \infty^{\omega}) = d^{(2)}(z^{\omega}, \infty) = \infty = d^{(2)}(z, \infty),$$

as well as $d^{(2)}(\infty^{\omega}, \infty^{\omega}) = d^{(2)}(\infty, \infty) = 0$. Let us define $(\infty)^{\phi} := \infty$. Then, from Corollary 5, for the "squared distance" of images of any two points $z, t \in GF(q^2) \cup \{\infty\}$ under ω, we have

$$d^{(2)}(z^{\omega}, t^{\omega}) = [d^{(2)}(z,t)]^{\phi}\|g\|^2.$$

Remark 6 leads to the following characterization of isometries.

7 Theorem. *An automorphism of $AG(2,q)$ is an isometry if and only if it sends regular circle to regular circle preserving the "squared radius".*

Proof. Suppose that ω is an isometry of $AG(2,q)$. Let us take the circle $\mathcal{K}_1 = \mathcal{K}(z_0, R)$. According to the definition of isometry, ω preserves the "squared distance" of any two points of $AG(2,q)$. So, if we take an arbitrary point $z_1 \in \mathcal{K}_1$, then from $d^{(2)}(z_0, z_1) = R$, it follows $d^{(2)}(z_0^{\omega}, z_1^{\omega}) = R$, i.e. $z_1^{\omega} \in \mathcal{K}(z_0^{\omega}, R)$. Hence, it is shown that $\mathcal{K}(z_0^{\omega}, R)$ is the image of the circle $\mathcal{K}_1$. Therefore, we can conclude that ω sends regular circle to regular circle with the same "squared radius".

To prove the reverse let us assume that ω is an automorphism of $AG(2,q)$ which sends regular circle to regular circle preserving the "squared radius". So ω is of the form (5). From Remark 6, it follows that ω sends arbitrary regular circle with the "squared radius" $R \in GF(q)^*$ to regular circle with the "squared radius" $R^{\phi}\|g\|^2$ (where $\phi = \psi|GF(q) \in \mathrm{Aut}GF(q)$). Therefore, for each $R \in GF(q)^*$, we obtain

$$R = R^{\phi}\|g\|^2. \tag{8}$$

If we put $R = 1$ into the previous equation, we get $\|g\|^2 = 1$. So, from (8), for each $R \in GF(q)^*$, we have $R = R^{\phi}$. Hence, ϕ is an identity of $\mathrm{Aut}GF(q)$. From Remark 6, it follows $d^{(2)}(z^{\omega}, t^{\omega}) = d^{(2)}(z,t)$, where z, t are any of two points of $M(q)$. So ω is an isometry of $M(q)$. QED

Finally, we obtain the matrix representations for isometries of $AG(2,q)$ and $M(q)$.

8 Theorem. *An automorphism of $AG(2,q)$ is an isometry if and only if for each $(x,y) \in GF(q^2)$ its matrix form is one of the following*

$$(x,y) \rightarrow (x,y)\begin{pmatrix} k & l \\ fl & k-el \end{pmatrix} + (r,s) \tag{9}$$

or

$$(x,y) \rightarrow (x,y)\begin{pmatrix} k & l \\ -fl-ek & -k \end{pmatrix} + (r,s), \tag{10}$$

where $r,s,k,l \in GF(q)$, satisfying $k^2 - ekl - fl^2 = 1$. All isometries of $AG(2,q)$ form a subgroup of $A\Gamma L(2,q)$ of order $2(q+1)q^2$.

Proof. According to Theorem 7, an isometry of $AG(2,q)$ sends any regular circle to regular circle. So, by Theorem 2, an isometry of $AG(2,q)$ is of the form (6) or (7). Besides, according to the proof of Theorem 2 (where we have labeled $g = k + \alpha l$) we get $\phi = id$ and $k^2 - ekl - fl^2 = 1$. Hence, isometries are of the form (9) or (10).

To prove the reverse, it has to be shown that each automorphism of $AG(2,q)$ with the matrix form (9) or (10) is an isometry of $AG(2,q)$. Let us suppose ω is of the form (9). From Theorem 2 and Corollary 5, for each $(x_1,y_1),(x_2,y_2) \in AG(2,q)$, it follows that

$$d^{(2)}\left((x_1,y_1)^\omega,(x_2,y_2)^\omega\right) = d^{(2)}\left((x_1,y_1),(x_2,y_2)\right).$$

Hence, ω is an isometry of $AG(2,q)$. Similar proof holds in the case when ω is of the form (10).

It is easy to verify that all isometries of $AG(2,q)$ form a subgroup of $A\Gamma L(2,q)$. Let us find the order of that group.

There are exactly $2q^2$ isometries of $AG(2,q)$ associated with each ordered pair $(k,l) \in GF(q)^2$ satisfying the condition $k^2 - ekl - fl^2 = 1$. The number of such ordered pairs is equal to the number of points of the circles

$$\mathcal{K}\left((0,0),1\right) = \left\{(x,y) \in GF(q^2) \mid x^2 - exy - fy^2 = 1\right\}.$$

This number is $q+1$, hence, there are exactly $2(q+1)q^2$ of isometries of $AG(2,q)$. QED

References

[1] W. Benz: Vorlesungen über Geometrie der Algebren, Springer V., Berlin - Heidelberg - New York, (1973).

[2] P. Dembowski: Finite Geometries, Springer V., Berlin - Heidelberg - New York, (1968).

[3] E. Hartmann: Planar Circle Geometries, lecture notes, Darmstadt, (2004).

[4] J.W.P.Hirschfeld: Finite Projective Spaces of Three Dimensions, Oxford University Press, Oxford, (1985).

[5] J.W.P. Hirschfeld: Projective geometries over finite fields, Oxford University Press, Oxford, (1979).

[6] B. Hornfeck: Algebra, 3 Auflage, Walter de Gruyter, Berlin - New York, (1976).

[7] D.R. Hughes and F.C. Piper: Projective Planes, Springer V., New York, (1973).

[8] C.M. O'Keefe: *Ovoids in $PG(3,q)$: a survey*, Discrete Mathematics, **151** (1996), 175–188.

[9] R. Lidl, H. Niederreiter: Finite Fields, Cambridge University Press, Cambridge, (1985).

[10] H. Pralle, J. Ueberberg: *Linear Geometries of Baer subspaces*, Bull. Belg. Math. Soc., **6** (1999), 559–569.

[11] E. M. Schröder: *Metric geometry*, in: F. Buekenhout, ed., Handbook of incidence geometry, Elsevier, Amsterdam, (1995), 945–1013.

[12] J.A. Thas: *The affine plane $AG(2,q)$, q odd, has a unique one point extension*, Invent. math. **118** (1994), 133–139.