Mathematica Pannonica
19/1 (2008), 13–21

REFLECTIONS IN FINITE (K, L)-PLANES

H. **Zeitler**

Bayreuth, Germany

Received: September 2007

MSC 2000: 11 A 05, 11 A 25

Abstract: In this short paper we consider geometries over pairs (K, L) of finite fields. All this is done in complete analogy to the Gauss-plane. We have finite miquelian Möbius-planes. In these geometries we investigate products of reflections. It turns out that there exist two classes of homographies and two classes of anti-homographies as well. With this, some mistakes found in the literature are corrected.

1. Introduction: ingredients

In complete analogy to the Gauss-plane over $(\mathbb{R}, \mathbb{C})$ we develop a finite (K, L)-plane. For better understanding the reader should always have this analogy in the backhead.

1.1. Some algebra

We start with a finite field $K = \mathrm{GF}(q) = \mathrm{GF}(p^e)$, p prime, $p > 2$, $e \in$ $\in \mathbb{N}$. Using a polynomial $f(x) = x^2 + b$ irreducible in K we adjoin an element ε with $\varepsilon^2 = -b \notin (K^*)^2$. In this way a quadratic extension field is obtained. We have $L = \{x_1, x_2 \in K \mid x_1 + \varepsilon x_2\}$.
Notions. $K^* = K \setminus \{0\}, L^* = L \setminus \{0\}$.

$\overline{X} = x_1 - \varepsilon x_2$ is called the *conjugate element* of $X = x_1 + \varepsilon x_2$ and $\mathrm{N}(X) = \overline{X} \cdot X = x_1^2 + bx_2^2$ the norm of X.

Lemmata. *If $N(L^*)$ is the set of norms of all elements in L^* then (only in the finite case) we have $N(L^*) = K^* \subset (L^*)^2$. In L^* there exist squares and non-squares with cardinality $\frac{1}{2}\,(q^2-1)$ each. Fig. 1 shows the situation in the case $L = GF(9)$.*

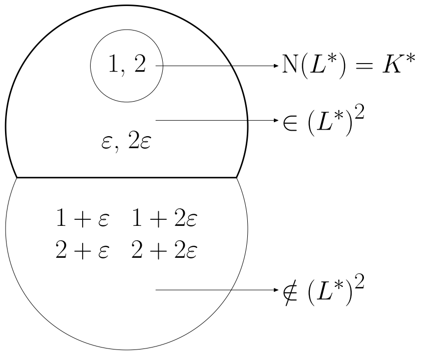
$1, 2$
$\mathrm{N}(L^*) = K^*$
$\in (L^*)^2$
$\varepsilon, 2\varepsilon$
$1+\varepsilon$ $1+2\varepsilon$
$2+\varepsilon$ $2+2\varepsilon$
$\notin (L^*)^2$

Figure 1. The field $L = \mathrm{GF}(9)$.

1.2. The geometric elements in the (K,L)-plane

Points: $\mathcal{P} = L \cup \{\infty\}$, $|\mathcal{P}| = q^2+1$. Lines: $\mathcal{G} = \{X \in L \mid X\overline{M} + \overline{X}M + d = 0\} \cup \{\infty\}$ with $M \in L^*$, $d \in K$.

$X\overline{M} + \overline{X}M + d = 0$ and $\overline{N}X + N\overline{X} + e = 0$ represent the same line if there exists $r \in K^*$ such that $N = rM$, $e = rd$ (equivalence).

With $X = x_1 + \varepsilon x_2$, $M = m_1 + \varepsilon m_2$ the equation may be written as $x_1 m_1 + b x_2 m_2 + \frac{1}{2}d = 0$.

Some properties. $A, B \in \mathcal{P}$, $|\{A, B\}| = 2$. There exists exactly one line $g(A, B)$ with $A, B \in g(A, B)$.

Each line contains exactly $q+1$ points.

Cardinality of $\mathcal{G}$: $|\mathcal{G}| = q(q+1)$.

Circles: $\mathcal{K} = \{X \in L \mid \mathrm{N}(X-M) = c\}$ with $M \in L$, $c \in \mathrm{N}(L^*) = K^*$.

Again it is possible to write the equation in another way:

$$(x_1 - m_1)^2 + b\,(x_2 - m_2)^2 = c.$$

Some properties. $A, B, C \in \mathcal{P}$, $|\{A, B, C\}| = 3$. There exists exactly one circle $k(A, B, C)$ with $A, B, C \in k(A, B, C)$.

Each circle contains exactly $q+1$ points.

Cardinality of $\mathcal{K}$: $|\mathcal{K}| = q^2(q-1)$.

Circles: $\mathcal{Z} = \mathcal{G} \cup \mathcal{K}$, $|\mathcal{Z}| = q(q^2+1)$.

1.3. Mappings

1.3.1. Cycle preserving mappings $\boldsymbol{M}$

$$M: \quad \boxed{\mu(X): \ X' = \frac{S\rho(X)+T}{U\rho(X)+V}} \quad S, T, U, V \in L, \ \det = SV - TU \neq 0.$$

$\rho(X)$ are automorphisms of L: $\rho(X) \in \left\{X^p, X^{p^2}, \ldots, X^q, \ldots, X^{2q}\right\}$.

The case $\rho(X) = X^q$ corresponds to the conjugation $\rho(X) = \overline{X}$ (Frobenius) and $\rho(X) = X^{2q}$ to $\rho(X) = X$ (Fermat).

In respect of the point at infinity ∞ special definitions must be given.

$\mu(\infty) = \frac{S}{U}$ if $U \neq 0$, $\mu(\infty) = \infty$ if $U = 0$ and $\mu(X) = \infty$ if $U\rho(X) + V = 0$.

A mapping is called cycle preserving if not only the set of points $\mathcal{P}$ is mapped bijective on itself but also the set of cycles. It turns out that all the mappings of M are cycle preserving. And much more the mappings M are exactly the cycle preserving mappings (v. Staudt).

Some properties. $|M| = 2eq^2\left(q^4 - 1\right)$.

Remark. Multiplying the numerator and the denominator with $Z \in L^*$ we obtain

$$\det = (SV - TU) \cdot Z^2.$$

The determinant is therefore only determined up to factors from $\left(L^*\right)^2$.

1.3.2. Homographies $\boldsymbol{H}$. We take $\rho(X) = X$ and obtain

$$H: \quad \boxed{\mu(X): \ X' = \frac{SX+T}{UX+V}} \quad S, T, U, V \in L, \ \det = SV - TU \neq 0.$$

Special definitions in connection with the point at infinity as before. These special mappings are called *homographies.*

Some properties. The mappings H are cycle preserving.

Composition of mappings in H yields a group which operates sharply 3-transitive on $\mathcal{P}$.

$|H| = q^2(q^4 - 1)$.

1.3.3. Lemma. *There exist two classes H_1, H_2 of homographies with cardinality $|H_1| = |H_2| = \frac{1}{2}q^2\left(q^4 - 1\right)$.*

Definition. If $\det \in \left(L^*\right)^2$ we speak about homographies of the first class H_1 and in the other case $\det \notin \left(L^*\right)^2$ about homographies of the second class H_2.

There remains only to prove the supposition concerning the cardinality.

Let $\alpha(X)$ a mapping from H_1.

$$\alpha(X):\ X'=\frac{SX+T}{UX+V},\quad \det\ =SV-TU\in\left(L^*\right)^2.$$

We multiply the numerator with $P\notin\left(L^*\right)^2$ and obtain a mapping $\beta(X)$.

$$\beta(X):\ X'=\frac{PSX+PT}{UX+V},\quad \det\ =P(SV-TU)\notin\left(L^*\right)^2.$$

We have a mapping from H_2. Every mapping $\alpha\in H_1$ induces a mapping $\beta\in H_2$. Therefore we have $|H_1|\leq|H_2|$.

Now we start with a mapping $\alpha(X)\in H_2$.

$$\alpha(X):\ X'=\frac{SX+T}{UX+V},\quad \det=A=SV-TU\notin\left(L^*\right)^2.$$

Multiplying the numerator with A yields a new homography

$$\gamma(X):\ X'=\frac{ASX+AT}{UX+V},\quad \det\ =A(SV-TU)=A^2.$$

We have $\gamma(X)\in H_1$ and $|H_2|\leq|H_1|$.

With this we obtain $|H_1|=|H_2|=\frac{1}{2}q^2\left(q^4-1\right)$.

Remark. In the case $K=\mathbb{R}$, $L=\mathbb{C}$ there don't exist two classes H_1 and H_2. Due to the fundamental theorem of algebra the determinant of each homography is a square in $\mathbb{C}$. Therefore there remains only the first class.

1.3.4. Anti-homographies. We take $\rho(X)=\overline{X}$ and obtain

$$\overline{H}:\quad \boxed{\mu(X):\ X'=\frac{S\overline{X}+T}{U\overline{X}+V}},\quad S,T,U,V\in L,\ \det\ =SV-TU\neq 0.$$

These mappings are called *anti-homographies.*

Some properties. The anti-homographies are cycle preserving.

Composition of such mappings does not yield a group.

$|\overline{H}|=q^2(q^4-1)$.

Exactly as in the case of homographies we distinguish two classes $\overline{H_1}$, $\overline{H_2}$ with $|\overline{H_1}|=|\overline{H_2}|=\frac{1}{2}q^2\left(q^4-1\right)$.

1.3.5. Reflections

Definition. Cycle preserving mappings from M with exactly one fixed point cycle k are called reflections σ_k in k. Other fixed points are not allowed.

Reflection in a line: $g = \{X \in L \mid X\overline{M} + \overline{X}M + d = 0\} \cup \infty$

$$\boxed{\sigma_g : X' = \frac{-\overline{X}M - d}{\overline{M}}}\,, \quad \det = -M\overline{M} \in K^* \subset (L^*)^2 .$$

Reflection in a circle: $k = \{X \in L \mid X\overline{X} - X\overline{M} - \overline{X}M + M\overline{M} = c\}$

$$\boxed{\sigma_k : X' = \frac{\overline{X}M - M\overline{M} + c}{\overline{X} - \overline{M}}}\,, \ \det = -M\overline{M} + \overline{M}M - c = -c \in K^* \subset (L^*)^2 .$$

We see that all reflections are elements in $\overline{H}$. If we replace X' by X in the mapping equation we obtain the respective fixed point cycle. Other fixed points cannot exist.

Only now we arrive the end of our ingredients chapter. We had to do with a lot of well-known material.

2. Products of reflections

2.1. Some fundamental homographies

2.1.1. Definitions. In analogy to classical geometry we define some very special homographies.

Translation τ: $X' = X + A$, $A \in L^*$

Reciprocation α: $X' = \dfrac{1}{X}$

Rotation ρ: $X' = DX$, $D \in L^*$, $\mathrm{N}(D) = 1$, $D \neq 1$

Central dilatation ζ: $X' = rX$, $r \in K^*$, $r \neq 1$.

2.1.2. Lemma. *The rotation ρ may be written in the following way*

$$X' = DX = \frac{G}{\overline{G}}X, \quad G \in L^*.$$

Proof.

$$\frac{G}{\overline{G}} = \frac{g_1 + \varepsilon g_2}{g_1 - \varepsilon g_2} = d_1 + \varepsilon d_2, \quad \mathrm{N}(D) = d_1^2 + b d_2^2 = 1.$$

Multiplication yields

$$g_1(1 - d_1) - g_2 b d_2 = 0$$

$$-g_1 d_2 + g_2(1 + d_1) = 0$$

$$\det = (1-d_1)\,(1+d_1) - bd_2^2 = 1 - d_1^2 - bd_2^2 = 0.$$

The system of equations therefore has a non-trivial solution g_1, g_2.

2.1.3. Lemma. *Every special homography in 2.1.1 may be decomposed in two reflections.*

Proof. *Translation* τ:

σ_1: $X_1 = -\dfrac{A}{\overline{A}}\,\overline{X} - A$, reflection in $X\overline{A} + \overline{X}A + A\overline{A} = 0$

σ_2: $X' = -\dfrac{A}{\overline{A}}\,\overline{X_1}$, reflection in $X\overline{A} + \overline{X}A = 0$

$\tau = \sigma_1\sigma_2$.

Reciprocation α

σ_1: $X_1 = \dfrac{1}{\overline{X}}$, reflection in $X\overline{X} = 1$

σ_2: $X' = \overline{X_1}$, reflection in $X - \overline{X} = 0$

$\alpha = \sigma_1\sigma_2$.

Central dilatation ζ

σ_1: $X_1 = \dfrac{1}{\overline{X}}$, reflection in $X\overline{X} = 1$

σ_2: $X' = \dfrac{r}{\overline{X_1}}$, reflection in $X\overline{X} = r$

$\zeta = \sigma_1\sigma_2$.

Rotation ρ. We prefer the presentation with G.

σ_1: $X_1 = -\dfrac{\overline{G}}{G}\,\overline{X}$, reflection in $XG + \overline{X}\,\overline{G} = 0$

σ_2: $X' = -\overline{X_1}$, reflection in $X + \overline{X} = 0$

$\rho = \sigma_1\sigma_2$.

2.1.4. Lemma. *The mapping μ: $X' = AX$, $A \in L^*$ is product of a rotation ρ and a central dilatation ζ if and only if $A \in (L^*)^2$. The center of the dilatation ζ and the center of the rotation ρ coincide.*

Proof. First direction $\mu = \zeta\sigma \Rightarrow A \in (L^*)^2$:

ζ: $X_1 = rX$, $r \neq 1$, $r \in K^* \subset (L^*)^2$

ρ: $X' = \dfrac{G}{\overline{G}}X_1$, $G \in L^*$, $G \neq 1$

$\mu = \zeta\rho$: $X' = \dfrac{G}{\overline{G}}rX = AX$

$$A = \frac{GG}{G\overline{G}}\,r = \frac{G^2}{G\overline{G}}\,r \in \left(L^*\right)^2 .$$

Second direction $A = B^2 \Rightarrow \mu = \zeta\rho$:

μ: $\quad X' = B^2X = \dfrac{BB\overline{B}}{\overline{B}}\,X = (B\overline{B})\dfrac{B}{\overline{B}}\,X$

ρ: $\quad X_1 = \dfrac{B}{\overline{B}}\,X$

ζ: $\quad X' = B\overline{B}X_1$

$$\mu = \rho\zeta.$$

2.2. Theorem. *Every product of an even number of reflections (product of even length) yields a homography of H_1.*

Proof. It is enough to give a proof for two reflections. Here we calculate only the case of two reflections in lines.

$$g_1 : X\overline{M_1} + \overline{X}M_1 + d_1 = 0, \qquad \sigma_{g_1} : \; X_1 = \frac{-\overline{X}M_1 - d_1}{\overline{M_1}}, \qquad \det = -M_1\overline{M_1} \in (L^*)^2,$$

$$g_2 : X_2\overline{M_2} + \overline{X}M_2 + d_2 = 0, \quad \sigma_{g_2} : \; X' = \frac{-\overline{X_1}M_2 - d_2}{\overline{M_2}}, \qquad \det = -M_2\overline{M_2} \in (L^*)^2,$$

$$\sigma_{g_1}\sigma_{g_2}\colon \quad X' = \frac{XM_2\overline{M_1} + M_2d_1 - M_1d_2}{\overline{M_2}M_1}, \qquad \det = \left(M_1\overline{M_1}\right)\left(M_2\overline{M_2}\right) \in (L^*)^2.$$

The multiplication of σ_1 and σ_2 yields a homography of the first class. In the same way the proof works if we have other cycles (line and circle, circle and circle). The proofs are becoming very easy if we use the well-known fact that the determinant of a product in our case is the product of determinants: $\det \sigma_1\sigma_2 = \det \sigma_1 \det \sigma_2$.

2.3. Theorem. *Every first class homography may be represented as a product of reflections with even length.*

Proof. Given the mapping $\mu \in H_1$

$$\mu : \quad X' = \frac{SX + T}{UX + V}, \quad \det = SV - TU \in \left(L^*\right)^2, \; U \neq 0.$$

(In the case $U = 0$ the mapping μ is a translation and all is done.) First of all we decompose μ in the following way.

$$\begin{aligned}
&\mu_1\colon\quad X_1 = -\frac{U^2}{SV-TU}\,X, && \det = -\frac{U^2}{SV-TU}\\
&\mu_2\colon\quad X_2 = X_1 - \frac{UV}{SV-TU}, && \det = 1\\
&\mu_3\colon\quad X_3 = \frac{1}{X_2}, && \det = -1\\
&\mu_4\colon\quad X' = X_3 + \frac{S}{U}, && \det = 1.
\end{aligned}$$

Indeed we obtain

$$\mu_1\ \mu_2\ \mu_3\ \mu_4 :$$

$$\begin{aligned}
X' = X_3 + \frac{S}{U} = \frac{1}{X_2} + \frac{S}{U} &= \frac{1}{X_1 - \frac{UV}{SV-TU}} + \frac{S}{U}\\
&= \frac{SV-TU}{-U(UX+V)} + \frac{S}{U} = \frac{SX+T}{UX+V} = \mu.
\end{aligned}$$

μ_2, μ_4 are translations and μ_3 the reciprocation. With $SV-TU \in$ $\in (L^*)^2$ Lemma 2.1.4 shows that μ_1 is the product of a rotation and a central dilatation. Using Lemma 2.1.3 the proof is perfect. $\Diamond$

2.4. Theorem. *Summarizing 2.2 and 2.3 we obtain our main result:*

The elements of H_1 are exactly the products of reflections with even length. In the case ($\mathbb{R},\mathbb{C}$) H_1 is to be replaced by H.

2.5. Theorem. *The elements of $\overline{H_1}$ are exactly the products of reflections with odd length. In the case* $(\mathbb{R},\mathbb{C})$ *$\overline{H_1}$ is to be replaced by $\overline{H}$.*

The proof is running completely analogous to the case of products with even length.

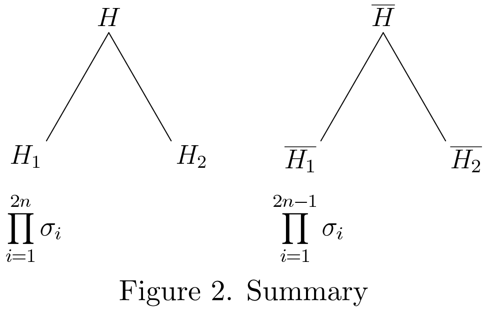

Figure 2. Summary

3. Final comment

It is possible to prove a lot of surprising theorems within the (K,L)-Geometry. Instead of doing in this way we make an important remark concerning the method. We emphasize that all proofs given in this paper are working only by calculation in the fields K, L. No pictures are needed. So we encounter an abstract geometry which can be done also by blind people.

Acknowledgement. The referee has found some mistakes and in this way improved the paper. Many thanks!

References

[1] BENZ, W.: Vorlesungen über Geometrie der Algebren, Berlin, 1973.

[2] DEMBOWSKI, P.: Finite geometries, Berlin, 1968.

[3] SCHROEDER, E. W.: Vorlesungen ber Geometrie I, Mannheim, 1971.

[4] ZEITLER, H. and PAGON, D.: Kreisgeometrie – gestern und heute, Darmstadt, 2007.