Lecture Notes of
Seminario Interdisciplinare di Matematica
Vol. 2 (2003), pp. 101 - 148.

Symplectic translation planes

by Antonio Maschietti

Abstract[1]. A great deal of important work on symplectic translation planes has occurred in the last two decades, especially on those of even order, because of their link with non-linear codes. This link, which is the central theme of this paper, is based upon classical groups, particularly symplectic and orthogonal groups. Therefore I have included an Appendix, where standard notation and basic results are recalled.

1. Translation planes

In this section we give an introductory account of translation planes. Comprehensive textbooks are for example [17] and [3].

1.1. **Notation.** We will use linear algebra to construct interesting geometrical structures from vector spaces, with special regard to vector spaces over finite fields. Any finite field has prime power order and for any prime power q there is, up to isomorphisms, a unique finite field of order q. This unique field is commonly denoted by $GF(q)$ (*Galois Field*); but also other symbols are usual, such as $\mathbf{F}_q$. If $q = p^n$ with p a prime, the additive structure of $\mathbf{F}_q$ is that of an $n-$dimensional vector space over $\mathbf{F}_p$, which is the field of integers modulo p. The multiplicative group of $\mathbf{F}_q$, denoted by $\mathbf{F}_q^*$, is cyclic. Finally, the automorphism group of the field $\mathbf{F}_q$ is cyclic of order n.

Let A and B be sets. If $f : A \to B$ is a *map* (or function or else mapping), then the image of $x \in A$ will be denoted by $f(x)$ (*functional notation*). Also, to denote the *image* of f the symbol $\mathrm{Im}(f)$ or $f(A)$ will be used. If $f : A \to B$ and $g : B \to C$ are maps then their composition is denoted by $g \circ f : A \to C$, where $(g \circ f)(x) = g(f(x))$ for all $x \in A$. We write also gf, when there is no danger of confusion.

If K is a field, its automorphism group is $\mathrm{Aut}(K)$; its elements will be represented by greek letters. We use the *exponential notation* to denote the image of elements of K under the action of elements of $\mathrm{Aut}(K)$; that is, the image of $x \in K$ under $\sigma \in \mathrm{Aut}(K)$ is x^σ. So we have

$$(x+y)^\alpha = x^\alpha + y^\alpha\,,\ (xy)^\alpha = x^\alpha y^\alpha \quad \text{for all} \quad x, y \in K \quad \text{and} \quad \sigma \in \mathrm{Aut}(K).$$

If A is a set, we write $|A|$ to denote the *cardinality* of A.

---

[1]Author's address: A. Maschietti, Università degli Studi di Roma "La Sapienza", Dipartimento di Matematica "Guido Castelnuovo", Piazzale Aldo Moro, 2, I00185 Roma, Italy; e-mail: maschiet@mat.uniroma1.it .

Notes of the course held during the Summer School in Potenza, September 1 - 6, 2003.

Definition 1.1. Let Ω be a set and G a group. We say that G *acts on* Ω when there is given a map $G \times \Omega \to \Omega$, written $(g, x) \mapsto g(x)$ and called the *action* of $g \in G$ on $x \in \Omega$, such that, for all $x \in \Omega$ and $g \in G$

(1) $h(g(x)) = (hg)(x)$; and
(2) $1(x) = x$, where 1 is the identity element of G.

If G acts on Ω, then each element of G determines a permutation (bijective map) of Ω. Precisely, if $g \in G$, then the map $f_g : \Omega \to \Omega$, such that $f_g(x) = g(x)$ for all $x \in \Omega$, is a permutation of Ω. Therefore if $S_{|\Omega|}$ is the *symmetric group* on Ω, there is a group homomorphism $\theta : G \to S_{|\Omega|}$. The kernel K of θ is the *kernel of the action* of G on Ω. If $K = \{1\}$ the action is called *faithful*.

Let G be a group acting on a set Ω. We say that two points $x, y \in \Omega$ are equivalent if there is $g \in G$ such that $g(x) = y$. This is clearly an equivalence relation and its equivalence classes are the *orbits* of G on Ω. The orbit of the point $x \in \Omega$ is denoted by $O(x)$. When G has only one orbit, then G is said to be *transitive* (or to act transitively) on Ω.

Let $A \subseteq \Omega$. We define

$$G_A := \{g \in G \mid g(x) \in A \text{ for all } x \in A\}.$$

G_A is a subgroup of G, called the *stabilizer* of A in G. When $A = \{x\}$ we write G_x instead of $G_{\{x\}}$. Then G is said to be *sharply transitive* or *regular* (or to act regularly) on Ω if it is transitive on Ω and $G_x = \{1\}$ for all $x \in \Omega$.

1.2. **Generalities on projective and affine planes.** We begin by recalling some basic properties of projective and affine planes.

Definition 1.2. A *projective plane* is an incidence structure $\mathbf{P} = (\mathcal{P}, \mathcal{L}, I)$ of points and lines such that

(P1) Any two distinct points are incident with a unique line;
(P2) Any two distinct lines are incident with a unique point;
(P3) There are four distinct points any three of which are not incident with the same line.

Remark 1.1. 1. From the above axioms it follows that any line of $\mathbf{P}$ is completely determined by the set of points it is incident. So lines can be regarded as subsets of the set of points $\mathcal{P}$ and incidence reduces to set-theoretic inclusion $\in$. Because of this, familiar locutions from elementary geometry are used, such as "the point P is on the line ℓ", "ℓ passes through P", "the lines ℓ and m meet in the point P".

2. The theory of projective planes is *self-dual*, in the sense that the *dual* incidence structure $\mathbf{P}^0 = (\mathcal{L}, \mathcal{P}, J)$, where $\ell J P$ if and only if $P I \ell$, is a projective plane.

3. A projective plane is called *finite* if its set of points is finite. Then also its set of lines is finite and each line contains a finite number of points. It can be easily proven that this number is a constant, say $n + 1$. The number n is called *the order* of the finite projective plane. For a finite projective plane of order n the following propositions hold.

(i) The number of points is $n^2 + n + 1$.
(ii) *The number of lines is* $n^2 + n + 1$.
(iii) *Every line contains* $n + 1$ *points.*
(iv) *Through any point there pass* $n + 1$ *lines.*

Definition 1.3. An *affine plane* is an incidence structure $\mathbf{A} = (\mathcal{P}, \mathcal{L}, I)$ of points and lines such that

(A1) Any two distinct points are incident with a unique line;
(A2) For any non-incident point-line pair (P, ℓ) there is a unique line incident with P and not incident with any point incident with ℓ;
(A3) There are three distinct points not incident with the same line.

Note that the dual structure of an affine plane is not an affine plane.

There is a classical relation between projective and affine planes. Let $\mathbf{A}$ be an affine plane. Define the relation of parallelism (symbol $\|$) on the set of lines as follows:

$$\ell \parallel m \text{ if and only if } \ell = m \text{ or } \ell \cap m = \emptyset.$$

It is an equivalence relation, and its equivalence classes are the *ideal points* (or points at infinity) of $\mathbf{A}$. Introduce now an *ideal line* ℓ_∞ incident with all the ideal points. In this way the incidence structure

$$\mathbf{P} = (\mathcal{P} \cup \mathcal{I}, \mathcal{L} \cup \{\ell_\infty\}, J),$$

where $\mathcal{I}$ is the set of ideal points and $J_{|\mathcal{P}\times\mathcal{L}} = I$, is a projective plane. Conversely, if ℓ is a line of a projective plane $\mathbf{P}$, then the incidence structure $\mathbf{A} = \mathbf{P}^\ell$ obtained from $\mathbf{P}$ by deleting ℓ and all its points is an affine plane.

Example 1.1. Let V be a vector space of three dimensions over a not necessarily commutative field F. Then $PG(V)$ is a projective plane (for the definition of $PG(V)$, see Appendix). It is a *desarguesian* projective plane, because Desargues' theorem holds in it. Any affine plane deduced from $PG(V)$ is a desarguesian affine plane.

We will see that translation planes are examples of *non-desarguesian* planes.

Exercise 1.1. The *order* of a finite affine plane $\mathbf{A} = \mathbf{P}^{\ell_\infty}$ is by definition the order of the corresponding projective plane $\mathbf{P}$. For a finite affine plane of order n, prove that

(i) the number of points is n^2;
(ii) the number of lines is $n^2 + n$;
(iii) any line contains n points;
(iv) the size of a class of parallel lines is n;
(v) through any point there pass $n + 1$ lines.

Definition 1.4. A *collineation* of a projective plane $\mathbf{P}$ is an incidence preserving permutation which maps points onto points and lines onto lines. The set of all collineations is a group, denoted by $\mathrm{Aut}(\mathbf{P})$, and called *the full collineation group* of $\mathbf{P}$. A *collineation group* of $\mathbf{P}$ is any subgroup of the full collineation group.

The full collineation group of an affine plane $\mathbf{A} = \mathbf{P}^\ell$ is $\mathrm{Aut}(\mathbf{P})_\ell$, the stabilizer of ℓ in $\mathrm{Aut}(\mathbf{P})$.

A collineation g is called *central* if there is a point C, called *the centre*, such that $g(\ell) = \ell$ for all the lines incident with C. It can be proven that a collineation g has a centre if and only if it has an *axis*, that is, a line a such that $g(P) = P$ for all the points P on a. Moreover, if g is not the identity, then its centre and axis are uniquely determined.

Central collineations partition into two distinct classes:

homologies: central collineations with a non-incident centre-axis pair;

elations: central collineations with an incident centre-axis pair.

The set of all collineations having the same centre and axis is a subgroup (eventually identical) of the full collineation group. It can be proven that if g is a collineation having centre-axis pair (C, a), then for every collineation h, the collineation $h^{-1}gh$ is a central collineation with $(h(C), h(a))$ as its centre-axis pair.

A fundamental result states that any non-identical central collineation is uniquely determined by its centre-axis pair and the image of any one of its non-fixed points.

Theorem 1.1. *Let (C, a) be a point-line pair in a projective plane $\mathbf{P}$, and X, Y be two points such that $X \neq C$, $Y \neq C$, $X \notin a$, $Y \notin a$ and X, Y, C are collinear. Then there is at most one collineation g having as centre C and as axis a such that $g(X) = Y$.*

The proof can be found for example in [11].

Because of this theorem, the following definition is meaningful.

Definition 1.5. Let $\mathbf{P}$ be a projective plane.

(1) $\mathbf{P}$ is said to be $(C, a)-$*transitive* if $\mathrm{Aut}(\mathbf{P})$ is transitive on the non-fixed points of any line on C.

(2) $\mathbf{P}$ is said to be $(m, l)-$*transitive*, where m and ℓ are lines, if $\mathbf{P}$ is $(C, l)-$transitive for every point $C \in m$. The set of all collineations having as axis ℓ and as centre any point of m is a group.

(3) Finally, $\mathbf{P}$ is said to be $(C, D)-$*transitive*, where C and D are points, if $\mathbf{P}$ is $(C, \ell)-$transitive for every line ℓ on D. The set of all collineations having as centre C and as axis any line on D is a group.

We can now give the definition of translation plane.

Definition 1.6. An affine plane $\mathbf{A} = \mathbf{P}^{\ell_\infty}$ is said to be a *translation plane* (with respect to the line ℓ_∞) if $\mathbf{P}$ is $(\ell_\infty, \ell_\infty)-$transitive. In other words, the group of all elations with axis ℓ_∞ is transitive on the points of $\mathbf{A}$. Any elation with axis ℓ_∞ is called a *translation* of $\mathbf{A}$. The set of all translations is a group, called the *translation group* of $\mathbf{A}$ and denoted by T.

Note that the translation group of a translation plane is indeed *sharply* transitive (or regular) on the set of points.

Translation planes have received, and receive, particular attention because of their close connection with linear algebra and group theory. This link has been shown for the first time by J. André [1].

1.3. **André's construction.** Let $\mathbf{A} = \mathbf{P}^{\ell_\infty}$ be a translation plane with translation group T. For U in ℓ_∞, let $T(U)$ be the group of all translations with centre U. Then the family $\Sigma = \{T(U) \mid U \in \ell_\infty\}$ has the following properties:

(1) Σ contains at least three distinct elements;
(2) $T(U)$ is a normal subgroup of T for each $U \in \ell_\infty$;
(3) $T(U) \cap T(V) = \{1\}$ for all $U, V \in \ell_\infty$ with $U \neq V$;
(4) $T = T(U)T(V)$ for every pair of distinct points on ℓ_∞.

Proof. 1. The line ℓ_∞ has at least three points.

2. For any collineation h of $\mathbf{P}$ it is $h^{-1}T(U)h = T(h(U))$. So $h^{-1}T(U)h = T(h(U)) = T(U)$ for all $h \in T$.

3. Any non-identical collineation has at most one centre.

4. Let $t \in T$. If P is a point of $\mathbf{A}$ and U, V are points of ℓ_∞, let $X = UP \cap Vt(P)$ (we denote by AB the line through the two points A and B). Then there is $s \in T(U)$ and $u \in T(V)$ such that $X = s(P)$ and $u(X) = t(P)$. Then $us(P) = t(P)$. Since T acts regularly on the point-set of $\mathbf{A}$, then $t = us$.

From the above properties one can deduce that T is an abelian group. Note also that T is a normal subgroup of the full collineation group of $\mathbf{A}$.

Definition 1.7. Let $(G, +)$ be an additive abelian group. A family Σ of proper subgroups of G such that

(1) Σ contains at least two distinct elements;
(2) Σ is a partition of $G \setminus \{\mathbf{0}\}$; and
(3) $G = A + B$, for all $A, B \in \Sigma$ with $A \neq B$

is called a *spread* of G. The elements of Σ are called the *components* of the spread.

Exercise 1.2. Let Σ be a spread of the additive group G. Then the incidence structure $A(\Sigma)$, whose *points* are the elements of G, whose *lines* are the cosets $a+S$, with $a \in G$ and $S \in \Sigma$, and incidence is set-theoretic inclusion, is a translation plane. The translations of $A(\Sigma)$, defined for each $a \in G$, are the maps

$$t_a : x \mapsto x + a\,,\ x \in G.$$

Moreover, the translation group T is isomorphic to the group G, and Σ contains at least three components.

Conversely, let $\mathbf{A}$ be a translation plane with translation group T and point-set G. Then the set G can be given the structure of an additive abelian group (using the regularity of T), in such a way that there is a spread Σ of G such that $\mathbf{A} = A(\Sigma)$.

Because of this equivalence, every translation plane is represented as $A(\Sigma)$, where Σ is a suitable spread of an abelian group.

Definition 1.8. Let $A(\Sigma)$ be a translation plane with point-set G. The *kernel* of $A(\Sigma)$, or of the spread Σ, denoted by $K(\Sigma)$, is the set of all the endomorphisms k of the additive group G such that

$$k(S) \subseteq S \quad \text{for all} \quad S \in \Sigma.$$

Theorem 1.2. *Let $K = K(\Sigma)$ be the kernel of $A(\Sigma)$. Then K is a skew-field, and the set of points of $A(\Sigma)$ is a $K-$vector space. Furthermore, every component of the spread is a $K-$subspace and any two components of Σ are isomorphic as $K-$subspaces.*

Proof. Only the proof that K is a skew-field requires some care (see [17, Theorems 1.6]). Begin by observing that K is a ring, since the point-set G of $A(\Sigma)$ is an abelian group; then prove that any nonzero element of K is a bijective map. The other statements are more or less straightforward. The product of the element $k \in K$ with the element $g \in G$ is defined as $kg := k(g)$ (the image of g under k). Then G becomes a $K-$vector space and each component of Σ is a $K-$subspace. Finally, if S, T and U are three distinct components of Σ, then, as a $K-$vector space,

$$G = S \oplus T = S \oplus U;$$

hence $T \cong U$.

As a consequence of the above theorem, if G if *finitely generated* over the kernel K, then $\dim_K(G) = 2n$, where n is the common dimension of the components of the spread. In particular, every *finite* translation plane has as kernel a *finite field*

(because of Wedderburn's theorem), and if $\dim_K(G) = 2n$, then $A(\Sigma)$ has order $|K|^n$.

Exercise 1.3. Let $A(\Sigma)$ be a translation plane with kernel K and point-set V. If $\dim_K(V) = 2$, then $A(\Sigma)$ is a desarguesian plane.

1.4. **The full collineation group of a translation plane.** The following theorem gives a complete description of the full collineation group of a translation plane.

Theorem 1.3. *Let Σ_i, $i = 1, 2$, be a spread of the abelian group V_i with kernel K_i. If f is an isomorphism of $A(\Sigma_1)$ onto $A(\Sigma_2)$ such that $f(\mathbf{0}) = \mathbf{0}$, then f is a semilinear isomorphism of the K_1-vector space V_1 onto the K_2-vector space V_2.*

Proof. See [17, Theorem 1.10]. Note that we denote the zero element of V_i by the same symbol $\mathbf{0}$.

In particular the full collineation group of $A(\Sigma)$ with kernel K can be factored as a product TG_0, where T is the translation group of $A(\Sigma)$ and G_0 is the stabilizer in $\Gamma L(V, K)$ of the spread Σ. The group G_0 is called *the translation complement* of $\mathrm{Aut}(A(\Sigma))$. Note that G_0 contains K^*, the set of nonzero elements of K.

If P is a point of an affine plane $\mathbf{A} = \mathbf{P}^{\ell_\infty}$, we denote by $\Delta(P)$ the group of all homologies with centre P and axis ℓ_∞.

Theorem 1.4. *Let $(V, +)$ be an additive group. If Σ is a spread of V and K its kernel, then $\Delta(\mathbf{0})$ is the multiplicative group of K.*

Proof. $\Delta(\mathbf{0})$ is a subgroup of the group of all invertible endomorphisms of V as an additive group. Since each element of $\Delta(\mathbf{0})$ fixes individually each line on $\mathbf{0}$, then $\Delta(\mathbf{0}) \subseteq K$. Conversely, every element of K^* induces a collineation of the plane that fixes individually each line on the point $\mathbf{0}$; hence $K^* \subseteq \Delta(\mathbf{0})$.

The elements of $\Delta(\mathbf{0})$ are also called *kernel homologies*.

1.5. **Matrix spreadsets.** Let $A(\Sigma)$ be a translation plane with point-set V. We know that V is a $K-$vector space and that each component of Σ is a $K-$vector subspace. From now on we limit our considerations to the case when K is commutative, that is, we assume that K is a field. We assume also that $\dim_K(V)$ is finite. For example this is always the case when $A(\Sigma)$ is finite. If F is any field contained in $K = K(\Sigma)$, then V is also an $F-$vector space (by restriction of scalars) and each component of Σ is an $F-$vector subspace of V. Of course, Σ is again a partition of the set of nonzero vectors of V, regarded now as an $F-$vector space. Henceforth we will consider only finite-dimensional vector spaces over fields.

Definition 1.9. Let V be a vector space over a field F. A *spread* of V is a family Σ of proper subspaces of V such that each nonzero vector belongs to only one component of Σ, and V is the sum of any two distinct components of Σ.

Exercise 1.4. Let V an $F-$vector space and Σ a spread of V. Then the incidence structure whose points are the elements of V and whose lines are the cosets $S + \mathbf{v}$, where $S \in \Sigma$ and $\mathbf{v} \in V$, is a translation plane whose kernel contains a field isomorphic to F. Therefore $V = S \oplus T$ for all $S, T \in \Sigma$, with $S \neq T$ and $\dim_F(V) = 2\dim_F(S)$, where $S \in \Sigma$.

Passing from V to $PG(V)$ (the projective geometry defined by V) any spread of V gives rise to a spread of $PG(V)$. For, by definition, a *spread of* $PG(V)$ is a family of mutually skew subspaces of the same dimension partitioning the set of points of $PG(V)$.

Most of the known translation planes (especially the finite ones) are usually constructed starting from a vector space V of *even* dimension $2n$ over a *field* F and picking a spread Σ, whose components are $n-$subspaces of V. So we expand on this construction of translation planes, and to simplify matter we will use coordinates.

Let $V = V(2n, F)$ be a $2n-$dimensional vector space over the (commutative) field F. Let Σ be a spread of V. As remarked above, the kernel of the corresponding translation plane $A(\Sigma)$ contains a field isomorphic to F. Fix two components of Σ, say S_0 and S_∞. Then $V = S_0 \oplus S_\infty$. Since $S_0 \cong S_\infty$ as $F-$vector spaces, V can be identified with $S_0 \times S_0$. So S_0 is identified with $\{(\mathbf{v}, 0) \mid \mathbf{v} \in S_0\}$ and S_∞ with $\{(0, \mathbf{v}) \mid \mathbf{v} \in S_0\}$. Let $U = \{(\mathbf{v}, \mathbf{v}) \mid \mathbf{v} \in S_0\}$. By [17, Lemma 2.1], it is not restrictive to assume that U is a component of Σ. Let $B_0 = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ and $B_\infty = (\mathbf{w}_1, \ldots, \mathbf{w}_n)$ be bases of S_0 and S_∞, respectively, so that $B = (B_0, B_\infty)$ is a basis of V. With respect to this basis, S_0 and S_∞ identify with F^n and the whole space V with $F^n \times F^n$. Elements of F^n (which are $n-$tuples) will be considered as $n \times 1$ matrices. Thus if $\mathbf{v}$ is a vector of V, its coordinates are $(x_1, \ldots, x_n, y_1, \ldots, y_n) = (X^t, Y^t)$, where $X = (x_1, \ldots, x_n)^t$ and $Y = (y_1, \ldots, y_n)^t$ are in F^n. Using this notation, S_0 has "the equation" $Y = O$ and S_∞ has "the equation" $X = O$, where O denotes the $n \times 1$ zero matrix. Let S be a $n-$subspace of V such that $S \cap S_\infty = \{\mathbf{0}\}$. Then, in the fixed basis B, S can be represented by a linear system like

$$\text{(1)} \qquad \begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ y_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ y_n = a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{cases}$$

for a unique $n \times n$ matrix

$$M_S = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}.$$

It is easy to see that the map $S \mapsto M_S$ is a bijection between the family of all $n-$subspaces of V intersecting S_∞ only in the zero vector and the space of all $n \times n$ matrices with entries in F. Linear system (1) can then be written in matrix form as $Y = M_S X$, where $M_S X$ denotes the ordinary matrix product. We say that $Y = M_S X$ is "the equation" of S. It is a succinct way to denote the subset

$$\{(X, M_S X) \mid X \in F^n\} \subset F^n \times F^n.$$

Let now Σ be a spread of V containing S_0, S_∞ and U. Then to the set $\Sigma \setminus \{S_\infty\}$ there corresponds bijectively a set $\mathcal{M}$ of $n \times n$ matrices over F such that

(1) The zero matrix O and the identity matrix I are in $\mathcal{M}$;
(2) if A and B are in $\mathcal{M}$ and $A \neq B$, then $A - B$ is non-singular; and
(3) the set $\mathcal{M}^* = \mathcal{M} \setminus \{O\}$ acts regularly on the nonzero vectors of F^n.

Proof. (1) Every component S of $\Sigma \setminus \{S_\infty\}$ is represented in matrix form as $Y = M_S X$. So the two matrices O and I belong to $\mathcal{M}$, since S_0 and U are in Σ.

(2) Any two distinct components of Σ, say S and T, intersect only in the zero vector. Therefore the linear system

$$(M_S - M_T)X = O$$

has only the trivial solution; hence the matrix $M_S - M_T$ is non-singular.

(3) Let X and Y be nonzero elements of F^n. Then $(X^t, Y^t)^t$ is an element of $F^n \times F^n$; hence it belongs to only one component S of Σ; that is to say there is a unique $M_S \in \mathcal{M}$ such that $Y = M_S X$.

$\mathcal{M}$ is usually called a *matrix spreadset* (or, more simply, a spreadset) for Σ. Once $\mathcal{M}$ has been determined, then the components of Σ have the equations

$$X = O \ \text{ or } \ Y = MX, \ M \in \mathcal{M}.$$

In this way the lines of $A(\Sigma)$ are represented by the "familiar" form

$$X = H\,,\ H \in F^n\,,\ Y = MX + H\,,\ M \in \mathcal{M}\,,\ H \in F^n.$$

In the case $n = 1$ we find the usual representation of desarguesian affine planes based on coordinates.

We determine now the kernel $K = K(\Sigma)$, using $\mathcal{M}$. As remarked earlier, K contains a field isomorphic to F. So, using Theorem 1.4, each element of K can be represented by a $2n \times 2n$ matrix with entries in F, and any such matrix can be written as a block-matrix, such as $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, where A, B, C, D are $n \times n$ matrices over F. The condition that the above matrix is in K leads to

$$B = C = O\,,\ D = A \ \text{ and } \ AM = MA \ \text{ for all } \ M \in \mathcal{M}.$$

Then

$$K(\Sigma) = \left\{ \begin{pmatrix} A & O \\ O & A \end{pmatrix} \mid A \in GL(n, F) \cup \{O\} \ \text{ and } \ AM = MA \ \text{ for all } \ M \in \mathcal{M} \right\}.$$

Hence $K(\Sigma) \cong C_{End_F(F^n)}(\mathcal{M})$ (the centralizer of $\mathcal{M}$ within $\mathrm{End}_F(F^n)$). The subfield isomorphic to F consists of the matrices

$$\begin{pmatrix} aI & O \\ O & aI \end{pmatrix}\,,\ a \in F.$$

In particular

Theorem 1.5. *If $\mathcal{M}$ is commutative (with respect to multiplication), then $A(\Sigma)$ is desarguesian. Moreover, in this case $K(\Sigma)$ is a field, and so the plane is pappian.*

Proof. As $\mathcal{M}$ is commutative, so

$$\mathcal{M} \subseteq C_{End_F(F^n)}(\mathcal{M}) \cong K.$$

We prove that K^* acts regularly on the set of nonzero vectors of each component of Σ. Let $S : Y = MX$. If $\begin{pmatrix} X \\ MX \end{pmatrix}$ and $\begin{pmatrix} \overline{X} \\ M\overline{X} \end{pmatrix}$ are nonzero vectors of S, then there is $A \in \mathcal{M}^*$ such that $\overline{X} = AX$ (because of property (3) of spreadsets). Hence

$$\begin{pmatrix} A & O \\ O & A \end{pmatrix} \begin{pmatrix} X \\ MX \end{pmatrix} = \begin{pmatrix} AX \\ AMX \end{pmatrix} = \begin{pmatrix} AX \\ M(AX) \end{pmatrix} \in S.$$

Therefore each component of Σ is a $1-$dimensional subspace of V, regarded as a $K-$vector space. So $\dim_K(V) = 2$, and $\mathcal{M} \cong K$. From this all statements follow.

Exercise 1.5. Let $F = GF(q)$. Then the set of 2×2 matrices

$$\mathcal{F} = \left\{ \begin{pmatrix} a & h(a-b) \\ h(a-b) & b \end{pmatrix} \mid a, b \in F \right\},$$

where h is a suitable nonzero element of F such that the polynomial

$$x^2 - \left(\frac{2h^2+1}{h^2} \right) x + 1$$

is irreducible over F, is a field of order q^2.

Example 1.2. Let $V = V(4, q)$ be a $4-$dimensional vector space over $F = GF(q)$. In $PG(V)$ a *regulus* is a set $\mathcal{R}$ of $q+1$ mutually skew lines pointwise covered by another set $\mathcal{R}^o$ of $q+1$ mutually skew lines. The set $\mathcal{R}^o$ is itself a regulus (pointwise covered by $\mathcal{R}$) and is called the *opposite regulus* of $\mathcal{R}$. Assume that Σ is a spread of $PG(V)$ containing a regulus $\mathcal{R}$. Then $(\Sigma \setminus \mathcal{R}) \cup \mathcal{R}^o$ is another spread of $PG(V)$, which defines a translation plane called the *derived plane* of $A(\Sigma)$. In particular, if $A(\Sigma) = AG(2, q^2)$ is the desarguesian plane of order q^2, then its derived plane is called the *Hall plane* of order q^2, denoted by $H(q)$.

If we construct $AG(2, q^2)$ using a field $\mathcal{F}$ of 2×2 matrices as in the exercise, then a spread for $AG(2, q^2)$ is

$$\Sigma = \{X = O\} \cup \{Y = MX \mid M \in \mathcal{F}\}, \ X = (x_0, x_1)^t, Y = (x_2, x_3)^t \in F^2.$$

Assume that $(x_0, x_1, x_2, x_3) = (X^t, Y^t)$ are homogeneous coordinates of $PG(3, q)$. Each component of Σ is a line of $PG(3, q)$, and Σ contains the regulus

$$\mathcal{R} = \{X = O\} \cup \{Y = aI \mid a \in F\},$$

whose opposite regulus is

$$\mathcal{R}^o = \{x_0 = x_2 = 0\} \cup \{bx_0 + x_1 = bx_2 + x_3 = 0, \ b \in F\}.$$

Then $H(q)$ is represented by the spread

$$(\Sigma \setminus \mathcal{R}) \cup \mathcal{R}^o.$$

There is a collineation group of $PG(3, q)$ isomorphic to $SL(2, q)$ that fixes $\mathcal{R}$ linewise and $\mathcal{R}^o$ setwise, and acts transitively on $\Sigma \setminus \mathcal{R}$. Therefore $H(q)$ admits a collineation group isomorphic to $SL(q)$.

Example 1.3. Let $F = GF(q)$, q odd. Then

$$\mathcal{M} = \left\{ \begin{pmatrix} u & at^\sigma \\ t & u \end{pmatrix} \mid u, t \in F \right\},$$

where $a \in F$ is a nonsquare and $\sigma \in \mathrm{Aut}(F)$, is a spreadset which defines a *Knuth's translation plane*. The spread determined by $\mathcal{M}$ contains a regulus (the same as that in the previous example). Therefore also this plane admits a derived plane.

2. Symplectic translation planes

In this section we investigate translation planes defined by *symplectic spread*.

2.1. **Symplectic spreads.** Let $V = V(2n, F)$ be a $2n-$dimensional vector space defined over the *field* F. As V has an even dimension, so it is always possible to define a non-degenerate alternating bilinear form β on V, that we call *symplectic*. The orthogonality relation defined by β is, as usual, denoted by $\perp$ (read "perp") (see Appendix).

Definition 2.1. Let (V, β) be a symplectic space. A spread Σ of V is called *symplectic* if Σ consists of totally isotropic subspaces, that is, $\beta(\mathbf{v}, \mathbf{w}) = 0$ for all $\mathbf{v}, \mathbf{w} \in S$, where $S \in \Sigma$. The corresponding translation plane is called *symplectic*.

Note that the components of a symplectic spread are *maximal* totally isotropic subspaces, as the Witt index of (V, β) is n.

Exercise 2.1. Prove that $AG(2, F)$ is a symplectic plane.

Let Σ be a symplectic spread. We can write

$$V = S_0 \oplus S_\infty\,, \quad \text{with} \quad S_0, S_\infty \in \Sigma.$$

Chose a basis $B_0 = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ of S_0 and let $B_\infty = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ be the basis of S_∞ such that

$$\beta(\mathbf{e}_i, \mathbf{f}_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ \mathbf{0} & \text{if } i \neq j \end{cases}$$

Such bases are called *dual*. Then $B = (B_0, B_\infty)$ is a basis of V. Let

$$(x_1, \ldots, x_n, y_1, \ldots, y_n) = (X^t, Y^t)$$

be vector coordinates, where $X = (x_1, \ldots, x_n)^t$ and $Y = (y_1, \ldots, y_n)^t$ are elements of F^n. With respect to this basis β is represented by the matrix

$$\begin{pmatrix} O & I \\ -I & O \end{pmatrix},$$

where O and I are the zero and the identity $n \times n$ matrices. Repeating the same arguments as those in Section 1.4, we obtain a spreadset $\mathcal{M}$ for Σ. Then S_∞ has the equation $X = O$, while any other component of Σ has the equation $Y = MX$, where $M \in \mathcal{M}$. We assume that $\mathcal{M}$ contains the identity matrix.

Proposition 2.1. *In the above setting, $\mathcal{M}$ consists of symmetric matrices.*

Proof. Each component of Σ is totally isotropic. So from $S \in \Sigma$ we get $S \subseteq S^\perp$. Let S have the equation $Y = MX$, for $M \in \mathcal{M}$. Every vector of S has coordinates of the form $(X^t, (MX)^t)$, $X \in F^n$. Therefore

$$(X^t, (MX)^t) \begin{pmatrix} O & I \\ -I & O \end{pmatrix} \begin{pmatrix} X' \\ MX' \end{pmatrix} = 0 \quad \text{for all} \quad X, X' \in F^n.$$

The above identity gives

$$-(MX)^t X' + X^t M X' = 0 \quad \text{for all} \quad X, X' \in F^n;$$

hence $M = M^t$.

Let $Sp(V)$ be the symplectic group of (V, β). Then $Sp(V)$ is transitive on the ordered pairs of maximal totally isotropic subspaces having in common only the zero vector (that is, $Sp(V)$ is transitive on the ordered symplectic bases; see Appendix). So from the point of view of this symplectic geometry, the pair S_0, S_∞ we started with is indistinguishable from any other such pair.

Writing matrices in the fixed basis B and referring to Section A.3.1, we have

Proposition 2.2. *(i) The elements of $Sp(n,F)$ that fix S_∞ are just those linear automorphisms whose matrices are*

$$\begin{pmatrix} I & O \\ A & I \end{pmatrix}$$

where A ranges through the space of all symmetric $n \times n$ matrices with entries in F.

(ii) These automorphisms form a group isomorphic to the additive group of the vector space of all symmetric $n \times n$ matrices. Moreover, this group acts regularly on the set of maximal totally isotropic subspaces having in common only the zero vector with S_∞.

Of particular interest are symplectic spreads of finite vector spaces. If $V = V(2n,q)$, then any symplectic spread of V produces a symplectic translation plane of order q^n. Finite symplectic translation planes of *even order* are particularly investigated because of their link with non-linear codes, such as Kerdock codes (see below). Of course, they are also interesting in themselves, because they provide wide classes of translation planes.

One of the most general results on finite symplectic translation planes is due to Kantor, see [14]. Let $F = GF(q)$.

Theorem 2.1 (Isomorphism Theorem)**.** *Let Σ_1 and Σ_2 be symplectic spreads in a finite $F-$vector space V equipped with a symplectic form β. Let K_2 be the kernel of Σ_2. Assume that either $|F|$ is even or $[K_2 : F]$ is odd. If $g \in \Gamma L(V)$ sends Σ_1 to Σ_2, then $g = hs$ with $h \in K_2^*$ and $s \in \Gamma L(V)$ satisfying $\beta(s(\mathbf{v}), s(\mathbf{w})) = a\beta(\mathbf{v},\mathbf{w})^\sigma$ for some $a \in F^*$, $\sigma \in \mathrm{Aut}(F)$ and all $\mathbf{v},\mathbf{w} \in V$, that is to say $s \in \Gamma Sp(V)$.*

Proof. Let θ be the symplectic polarity induced by β on $PG(V)$. Then θ is the identity on both Σ_1 and Σ_2. Moreover, θ and $g\theta g^{-1} = \theta^{g^{-1}}$ are symplectic polarities, each of which is the identity on Σ_2. By the fundamental theorem of projective geometry, the collineation $\theta^{g^{-1}}\theta$ of $PG(V)$ is induced by an element of $\Gamma L(V)$ which is the identity on Σ_2; hence it belongs to K_2. Since $(|K_2|-1)/(|F|-1)$ is odd by hypothesis, then $\theta^{g^{-1}}\theta$ has odd order as a collineation of $PG(V)$. Then θ and $\theta^{g^{-1}}$ are conjugate in the dihedral group they generate, and hence $\theta^h = \theta^{g^{-1}}$ for some $h \in \langle \theta, \theta^{g^{-1}} \rangle$. Then the collineation $s = h^{-1}\overline{g}$ commutes with θ, where $\overline{g}$ is the element of $P\Gamma L(V)$ induced by g. Therefore $s \in P\Gamma Sp(V)$. On the other hand, since h is the identity on Σ_2, then it is induced by an element of K_2^*. Replacing s and h by their preimages in $\Gamma L(V)$, one obtains that $g = a(hs)$ for some $a \in F^*$, so that $ah \in hF \subseteq K_2$.

In particular by letting $\Sigma_1 = \Sigma_2 = \Sigma$ in the above theorem, we get the following result.

Corollary 2.1. *Let $A(\Sigma)$ be a finite symplectic translation plane. Then the translation complement of $\mathrm{Aut}(A(\Sigma))$ can be factored as the product of its homologies with centre $\mathbf{0}$ and its intersection with the full symplectic group $\Gamma Sp(V)$.*

2.2. **Construction of symplectic planes of even order.** In this section we report on Kantor's construction (see [13]) of symplectic planes. We fix the field $F = GF(q)$, where q is *even*.

First, we show the link between the orthogonal geometry of the hyperbolic type and Kerdock sets.

Let $V = V(2n, q)$ be a $2n-$dimensional vector space over F, with $n \geq 2$. Assume that V is equipped with a quadratic form Q of Witt index n, and whose polar form is β (see Appendix, Orthogonal polar spaces). Pick a basis

$$B = (\mathbf{e}_1, \ldots, \mathbf{e}_n, \mathbf{f}_1, \ldots, \mathbf{f}_n)$$

such that

$$Q(\mathbf{e}_i) = Q(\mathbf{f}_i) = \beta(\mathbf{e}_i, \mathbf{e}_j) = \beta(\mathbf{f}_i, \mathbf{f}_j) = 0\,, i, j = 1, \ldots, n$$

and

$$\beta(\mathbf{e}_i, \mathbf{f}_j) = \delta_{ij}\,, 1 \leq i, j \leq 2n.$$

Let (X^t, Y^t) be vector coordinates, where $X = (x_1, \ldots, x_n)^t$ and $(Y = (y_1, \ldots, y_n)^t$ are in F^n. Denote by M the matrix of Q. Then for all $\mathbf{v} \in V$

$$Q(\mathbf{v}) = Q((x_1, \ldots, x_n, y_1, \ldots, x_n)) = X^t M X = \sum_{i=1}^{n} x_i y_i.$$

The matrix J of β is

$$J = M + M^t = \begin{pmatrix} O & I \\ I & O \end{pmatrix}.$$

(We can dispense with the minus sign, since the characteristic of the field is two.)

The two $n-$subspaces $H = \langle \mathbf{e}_1, \ldots, \mathbf{e}_n \rangle$ and $K = \langle \mathbf{f}_1, \ldots, \mathbf{f}_n \rangle$ are totally singular and have the equations $Y = O$ and $X = O$, respectively. Any other totally singular $n-$subspace S having only $\mathbf{0}$ in common with H is represented by an equation like $Y = A_S X$, where A_S is a skew-symmetric $n \times n$ matrix, uniquely determined by S (note that skew-symmetric matrices are always assumed to have zero diagonal). Conversely, every skew-symmetric matrix uniquely determines a totally singular $n-$subspace having only $\mathbf{0}$ in common with H. Now, two totally singular $n-$subspaces $S : Y = A_S X$ and $T : Y = A_T X$ have only $\mathbf{0}$ in common if and only if $A_S + A_T$ is non-singular, and this happens if and only if n is *even* (for, the rank of a skew-symmetric matrix is even).

Assume that $n = 2m$. A *Kerdock set* $\mathcal{K}$ is a family of q^{2m-1} skew-symmetric $2m \times 2m$ matrices the difference of any two of which is non-singular. When $F = GF(2)$, $\mathcal{K}$ produces a *generalized Kerdock code* consisting of the zeros of the following functions $F^{2m} \to F$:

$$Z \mapsto Z^t \overline{M} Z + \varphi(Z) + c\,,\ Z \in F^{2m},$$

where $\overline{M}$ is the unique $2m \times 2m$ matrix for which there is $M \in \mathcal{K}$ such that $M = \overline{M} + \overline{M}^t$, φ ranges through all linear functionals on F^{2m}, and $c \in F$. Further information on Kerdock sets and related combinatorial structures can be found in [6]; see also [5].

The set of singular $1-$subspaces of (V, Q) has size $(q^{2m-1} + 1)(q^{2m} - 1)/(q - 1)$ (from the projective point of view that set is the set of all projective points of the quadric defined by Q; see Appendix). So, *an orthogonal spread* of (V, Q) is a family Σ of $q^{2m-1} + 1$ totally singular $2m-$subspaces such that every singular vector of V belongs to a unique component of Σ. From the projective point of view this is the usual definition of a *spread of an orthogonal polar space*. So henceforth we will shift freely from vector spaces to their corresponding projective spaces, and conversely. From what precedes, once a basis like B has been fixed, then there is a bijective

map between the family of all orthogonal spreads containing H and K and the family of all Kerdock sets. For, a Kerdock set $\mathcal{K}$ of $2m \times 2m$ matrices produces the orthogonal spread

$$\Sigma(\mathcal{K}) = \{H\} \cup \{Y = AX \mid A \in \mathcal{K}\}.$$

Now we illustrate how an orthogonal spread of (V, Q), where $V = V(4m, q)$ and q is even, produces a symplectic translation plane of order q^{2m-1}.

Let $\mathbf{y} \neq \mathbf{0}$ be a non-singular vector of V. Then $(\mathbf{y}^\perp, Q_{|y^\perp})$ is a parabolic orthogonal space, and $\mathbf{y} \in \mathbf{y}^\perp$, since the characteristic of the field is two. The $(4m-2)-$dimensional vector space $\mathbf{y}^\perp/\langle \mathbf{y} \rangle$ becomes a symplectic space, since it inherits from β a symplectic form β_y defined by

$$\beta_y(\mathbf{v} + \langle \mathbf{y} \rangle, \mathbf{w} + \langle \mathbf{y} \rangle) := \beta(\mathbf{v}, \mathbf{w}), \quad \text{for all} \quad \mathbf{v}, \mathbf{w} \in \mathbf{y}^\perp.$$

Moreover, the natural projection $\mathbf{y}^\perp \to \mathbf{y}^\perp/\langle \mathbf{y} \rangle$ induces a bijection between the family of totally singular subspaces of $\mathbf{y}^\perp$ containing $\langle \mathbf{y} \rangle$ and the family of totally isotropic subspaces of $\mathbf{y}^\perp/\langle \mathbf{y} \rangle$.

Let Σ be an orthogonal spread of (V, Q). If $S \in \Sigma$, then $\dim(\mathbf{y}^\perp \cap S) = 2m - 1$. The family

$$\Sigma^* = \{\mathbf{y}^\perp \cap S \mid S \in \Sigma\}$$

partitions the set of all singular vectors of $\mathbf{y}^\perp$. Let

$$\Sigma_y := \{\langle S \cap \mathbf{y}^\perp, \mathbf{y} \rangle / \langle \mathbf{y} \rangle \mid S \in \Sigma\}$$

be *the projection* of Σ^* from $\langle \mathbf{y} \rangle$ onto $\mathbf{y}^\perp/\langle \mathbf{y} \rangle$. Then Σ_y is a symplectic spread of $(\mathbf{y}^\perp/\langle \mathbf{y} \rangle, \beta_y)$, which Kantor calls a *slice* of Σ.

Each non-singular vector $\mathbf{y}$ produces a slice Σ_y and hence a symplectic translation plane of order q^{2m-1}. This construction can be reversed, in the sense that every symplectic spread of a $(4m-2)-$dimensional symplectic space is the slice of an orthogonal spread of a $4m-$dimensional orthogonal (Extension theorem) (see also [8]).

Theorem 2.2 (Extension Theorem)**.** *Let Σ' be a symplectic spread of a $(4m-2)-$dimensional symplectic space (V', β') over $F = GF(q)$, with q even. Then there is a unique orthogonal spread Σ (up to an orthogonal isometry) in a $4m-$dimensional orthogonal space (V, Q) such that Σ' is a slice of Σ (up to a symplectic isometry).*

Proof. Up to isometries, there is a unique symplectic form on V'. So we can assume that $V' = \mathbf{y}^\perp/\langle \mathbf{y} \rangle$, where $\mathbf{y}$ is a non-singular vector of a $4m-$dimensional orthogonal space (V, Q). Therefore Σ' is a spread of $\mathbf{y}^\perp/\langle \mathbf{y} \rangle$, and is the projection of a family Σ^* of totally singular $(2m-1)-$subspaces of $(\mathbf{y}^\perp, Q_{|y^\perp})$, partitioning the set of nonzero vectors of $\mathbf{y}^\perp$. Now, there are two classes of totally singular $2m-$subspaces of (V, Q), and any two of them belong to the same class if and only if the dimension of their intersection is even (see Appendix). Let $\mathcal{S}$ be one of these classes. Each element W^* of Σ^* is contained in a unique member W of $\mathcal{S}$. Moreover, if $W_1^*, W_2^* \in \Sigma^*$ then, letting W_i, $i = 1, 2$, be the element of $\mathcal{S}$ containing W_i^*, we have that $\dim(W_1 \cap W_2)$ is even and at most 1. Therefore

$$\Sigma = \{W \in \mathcal{S} \mid W^* \in \Sigma^*\}$$

is a family of $q^{2m-1} + 1$ totally singular $2m-$subspaces, any two of which intersect only in the zero vector. Then Σ is an orthogonal spread and Σ' is the slice Σ_y.

Uniqueness follows since the orthogonal transvection (reflection) with axis $\mathbf{y}^\perp$ interchanges the two classes of totally singular $2m-$subspaces and induces the identity on $\mathbf{y}^\perp$.

From the Isomorphism Theorem (Theorem 2.1) and the above theorem the following useful result follows.

Let $G = G(\Sigma) = \Gamma O^+(4m, q)_\Sigma$ denote the stabilizer of Σ within the full orthogonal group of (V, Q).

Corollary 2.2. *Let Σ_y and Σ_z be slices of an orthogonal spread Σ of (V, Q). Then $A(\Sigma_y)$ is isomorphic to $A(\Sigma_z)$ if and only if the two non-singular vectors $\mathbf{y}$ and $\mathbf{z}$ are in the same orbit of G.*

Remark 2.1. Two non-singular vectors $\mathbf{y}$ and $a\mathbf{y}$, where $a \in F^*$, give rise to the same slice, and scalar maps preserve the quadric defined by Q and are in G. So to apply the above corollary we have to look at the non-singular vectors that are in different $1-$dimensional subspaces. In other words, we must consider distinct projective points.

From this corollary and Corollary 2.1 we deduce that the translation complement of $A(\Sigma_y)$ can be achieved in three stages:

(1) determine the group $G = G(\Sigma)$;
(2) determine $G_{\langle y\rangle}$, the stabilizer of $\langle \mathbf{y}\rangle$, which is also the group induced by $\mathrm{Aut}(A(\Sigma_y))$ on the line at infinity; and
(3) determine the group of homologies of $A(\Sigma_y)$ having as axis the line at infinity and as centre $\mathbf{0}$.

The process of passing from a symplectic spread Σ' to its corresponding orthogonal spread Σ is called *extension*. Given a symplectic spread, we can extend it and then slice the result, obtaining in this way a new symplectic spread. By the above corollary, any symplectic isometry sending one spread to another spread induces an orthogonal isometry between their extensions, and non-isometric orthogonal spreads never produce isomorphic symplectic planes.

2.3. **Examples of symplectic planes of even order.** We begin with the following remark. Let (V', β') be a symplectic space over $K = GF(q^m)$. If $F = GF(q)$ is a subfield of K, then, by restriction of scalars, V' is also a vector space over F. Let $T : GF(q^m) \to GF(q)$ be the *trace map*. Equip the $F-$vector space V' with the symplectic form $\gamma' = T \circ \beta'$. Then (V', γ') becomes a symplectic space over F. In particular, a symplectic spread Σ of (V', β') produces a symplectic spread Σ' of (V', γ'). Of course, the translation planes defined by Σ and Σ' are the same.

The starting point for constructing examples is the desarguesian plane of order q^{2n-1}, denoted by $AG(2, q^{2n-1})$. Then $K = GF(q^{2n-1})$, $n \geq 1$, and $\dim_K(V') = 2$. We assume that $F = GF(q)$ is contained in K. Then $AG(2, q^{2n-1})$ is constructed from the symplectic spread consisting of all $1-$dimensional subspaces of (V', β'), for a suitable symplectic form β'. By the above remark, the family of $1-$dimensional subspaces of (V', β') becomes a family of totally isotropic $(2n-1)-$subspaces of (V', γ'), which is a symplectic spread Σ' of (V', γ'). This spread is called *desarguesian*, since it gives rise to the desarguesian plane $AG(2, q^{2n-1})$. Note that $\dim_F(V') = 2(2n-1)$. Henceforth we assume q is even. Extend the spread Σ' to

an orthogonal spread Σ (called *desarguesian* by Kantor) of a $4n-$dimensional orthogonal space (V,Q), so that $\Sigma' = \Sigma_y$ for some non-singular vector $\mathbf{y} \in (V,Q)$. If we choose another non-singular vector, say $\mathbf{z}$, then we can construct the symplectic spread Σ_z of $\mathbf{z}^\perp/\langle \mathbf{z}\rangle$. By the isomorphism theorem $\Sigma_y = \Sigma'$ is equivalent to Σ_z (i.e. $A(\Sigma_y) \cong A(\Sigma_z)$) if and only if $\langle \mathbf{y}\rangle$ and $\langle \mathbf{z}\rangle$ are in the same orbit under the action of $\Gamma O^+(4n,q)_\Sigma$ (see Remark 2.1). Hence, in order to obtain non-isomorphic symplectic translation planes, one must find inequivalent slices. This leads naturally to the consideration of the orbits of non-singular $1-$subspaces under the action of $G = G(\Sigma) = \Gamma O^+(4n,q)_\Sigma$. When Σ' is desarguesian, G has been determined (see [8] and [7]). In our setting, we have

$$G = \Gamma O^+(4n,q)_\Sigma \cong \Gamma Sp(4n-2,q)_{\Sigma'} \cong \Gamma L(2,q^{2n-1}).$$

Moreover, if $n \geq 3$, then $G = G_{\langle y\rangle}$. Assume $n \geq 3$.

Since

$$\Gamma L(2,q^{2n-1}) \cong (SL(2,q^{2n-1}) \times GF(q)^*) \cdot \mathrm{Aut}(GF(q^{2n-1})),$$

then

$$|G| = q^{2n-1}(q^{4n-2}-1)(q-1)(2n-1)d\,, \quad \text{where} \quad q = 2^d.$$

The $G-$orbits of non-singular points are then:

(1) $\{\langle \mathbf{y}\rangle\}$.

(2) $O(\langle \mathbf{z}\rangle)$, where $\langle \mathbf{z}\rangle$ belongs to the set of non-singular points of $\mathbf{y}^\perp \setminus \{\langle \mathbf{y}\rangle\}$. There is just one orbit of length $q^{4n-2}-1$. Then, using Burnside's formula

$$|G|/|G_{\langle z\rangle}| = |O(\langle \mathbf{z}\rangle)|,$$

the group $G_{\langle z\rangle}$ has order $q^{2n-1}(q-1)(2n-1)d$. It induces on the symplectic plane $A(\Sigma_z)$ an automorphism group of order q^{2n-1} that fixes one component of Σ_z (it corresponds to the unique component of Σ containing $\mathbf{z}$) and acts regularly on the other. Such a plane is a *semifield plane*, because it can be coordinatized by a semifield (see [3] or [17]).

(3) $O(\langle \mathbf{z}\rangle)$ such that $\langle \mathbf{y},\mathbf{z}\rangle$ is a hyperbolic line. There are at least $[(q/2-1)/d]$ such orbits each of size $q^{2n-1}(q^{2n-1}+1)$. The stabilizer $G_{\langle z\rangle}$ of $\langle \mathbf{z}\rangle$ induces on $A(\Sigma_z)$ a collineation group of order $q^{2n-1}-1$ fixing two components of Σ_z, which are the components of Σ containing the two singular points of the hyperbolic line.

(4) $O(\langle \mathbf{z}\rangle)$ such that $\langle \mathbf{y},\mathbf{z}\rangle$ is an anisotropic line. There are at least $[(q/2)/d]$ such orbits each of size $q^{2n-1}(q^{2n-1}-1)$. The stabilizer $G_{\langle z\rangle}$ induces on $A(\Sigma_z)$ a collineation group of order $q^{2n-1}+1$ acting regularly on Σ_z. So the symplectic plane is *flag-transitive* (transitive on the set of ordered pairs (P,ℓ) with P on ℓ).

Details of the proof can be found in [8, Theorem 15]. For concrete examples see [14] and [15]. Here we illustrate one example.

Example 2.1. Let $K = GF(q^{2n-1}) \supset F = GF(q)$, where q is even and $n \geq 3$. Consider the $F-$vector space

$$V = K \times F \times K \times F = \{(x,a,y,b) \mid x,y \in K,\ a,b \in F\}.$$

Then $\dim_F(V) = 4n$. Let Q be the quadratic form

$$Q(x,a,y,b) = T(xy) + ab$$

where $T : K \to F$ is the trace map. Its polar form is

$$\beta((x,a,y,b),(x',a',y',b')) = T(xy' + x'y) + ab' + a'b.$$

The family Σ consisting of the following totally singular $2n-$subspaces

$$\{(0,0,y,b) \mid y \in K,\ b \in F\}$$

and

$$\{(x,a,s^2x + sT(sx) + sa, T(sx)) \mid x \in K,\ a \in F\}, \quad \text{for each} \quad s \in K$$

is an orthogonal spread of (V,Q).

Let $\mathbf{y} = (0,1,0,1)$ be a non-singular vector. Then the slice

$$\Sigma_y = \{\langle S \cap \mathbf{y}^\perp, \mathbf{y}\rangle / \langle \mathbf{y}\rangle \mid S \in \Sigma\}$$

consists of the following subspaces of $\mathbf{y}^\perp/\langle \mathbf{y}\rangle$:

$$\{(0,0,y,0) + \langle \mathbf{y}\rangle \mid y \in K\}$$

and

$$\{(x,0,s^2x,0) + \langle \mathbf{y}\rangle \mid x \in K\}, \quad \text{for each} \quad s \in K.$$

It is a symplectic spread with respect to the symplectic form

$$\beta_y((x,0,y,0) + \langle \mathbf{y}\rangle, (x',0,y',0) + \langle \mathbf{y}\rangle) = T(xy' + x'y).$$

Moreover, Σ_y is a desarguesian spread, since it defines

$$A(\Sigma_y) = AG(2, q^{2n-1}).$$

Fix now $k \in F \setminus \{0,1\}$ and consider the non-singular point

$$\langle \mathbf{y}_k\rangle = \langle (0,k+1,0,1)\rangle.$$

The symplectic spread Σ_{y_k} consists of the following subspaces:

$$\{(0,0,y,0) + \langle \mathbf{y}_k\rangle \mid y \in K\}$$

and

$$\{(x,0,s^2x + ksT(sx),0) + \langle \mathbf{y}_k\rangle \mid x \in K\}, \quad \text{for each} \quad s \in K.$$

The non-singular point $\langle \mathbf{y}_k\rangle$ belongs to an orbit of type 3. (see above), since $\langle \mathbf{y}, \mathbf{y}_k\rangle$ is a hyperbolic line.

Remark 2.2. Kantor's construction produces only symplectic translation planes of even order q^{2n-1}, where the exponent is *odd*. So it would be very interesting to find constructions of symplectic planes of order q^{2n}, with $n \geq 1$. In the next section we will treat the case q^2, but from a different point of view.

2.4. **A characterization of symplectic planes of even order.** We begin by briefly recalling some elementary facts on *ovals* in a finite projective plane. An excellent survey is [16]; for a complete account of ovals in desarguesian planes, see [9].

Let $\mathbf{P}$ be a finite projective plane of order q. An *oval* is a set of $q+1$ points, no three of which are collinear. Dually, a *line oval* is a set of $q+1$ lines no three of which have a common point. Let $\mathcal{O}$ be an oval. Any line of the plane can intersect $\mathcal{O}$ in either 0, 1 or 2 points and is accordingly called *exterior, tangent or secant*. Classical examples of ovals are the non-singular conics in desarguesian projective planes. By a famous theorem of B. Segre (see [21]) the converse is true in the case of *odd* order.

Theorem 2.3 (Segre)**.** *In a desarguesian plane of odd order the ovals are exactly the non-singular conics.*

In the *even* case there is no such a simple characterization, and the classification of ovals, even in desarguesian planes, is an open problem, that seems to be very difficult.

In the even case a "strange" phenomenon occurs: all the tangent lines to an oval $\mathcal{O}$ meet in the same point N, called the *nucleus* (or the knot) of $\mathcal{O}$. The set $\mathcal{O} \cup \{N\}$ becomes a *hyperoval*, that is, a set of $q+2$ points, no three of which are collinear. A *regular hyperoval* is a conic plus its nucleus in a desarguesian plane. By duality, if $\mathcal{O}$ is a line oval, then there is exactly one line n such that on each of its points there is only one line of $\mathcal{O}$. This line n is called the (dual) *nucleus* of $\mathcal{O}$. The $(q+2)-$set $\mathcal{O} \cup \{n\}$ is called a *line hyperoval* or *dual hyperoval*.

Let $\mathcal{O}$ be a line oval in an even order projective plane $\mathbf{P}$, and let ℓ_∞ be its nucleus. If $\mathbf{A} = \mathbf{P}^{\ell_\infty}$, then we put

$$B(\mathcal{O}) := \{P \in \mathbf{A} \mid P \text{ is on a line of } \mathcal{O}\}.$$

Denote by $\mathcal{F}_P$ the pencil of lines on P, where P is a point of $\mathbf{P}$.

Definition 2.2. Let P be a point on ℓ_∞. We say that $\mathcal{O}$ is $P-$*regular* if for any pair of distinct affine lines $x, y \in \mathcal{F}_P \setminus (\mathcal{F}_P \cap \mathcal{O})$ there is a third affine line $z \in \mathcal{F}_P \setminus (\mathcal{F}_P \cap \mathcal{O})$ such that for every affine line ℓ not on P at least one of the points $\ell \cap x$, $\ell \cap y$ or $\ell \cap z$ belongs to $B(\mathcal{O})$. Each non ordered triple of lines sharing the above property is called $P-$regular. Finally, $\mathcal{O}$ is said to be *completely regular* with respect to its nucleus ℓ_∞ if $\mathcal{O}$ is $P-$regular for every point P of ℓ_∞.

Theorem 2.4. *Let* $\mathbf{A}$ *be a translation plane of even order. Then* $\mathbf{A}$ *admits a completely regular line oval with respect to the line at infinity if and only if* $\mathbf{A}$ *is a symplectic translation plane.*

For the proof and other properties of completely regular line ovals see [19]. Here we give an explicit description of such line ovals.

Let $V = V(2n, q)$ be a finite symplectic space with symplectic form β, and assume that q is even, $q = 2^h$. Put $F = GF(q)$. Let Σ be a symplectic spread and let S_0 and S_∞ be two components of Σ. Choose dual bases $B_0 = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ and $B_\infty = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ in S_0 and S_∞ respectively, so that the matrix of β is $\begin{pmatrix} O & I \\ I & O \end{pmatrix}$. Let $\mathcal{M}$ be a spreadset for Σ. Then $\mathcal{M}$ consists of symmetric matrices. If $M \in \mathcal{M}$, let $d(M)$ be the vector of F^n whose elements are the square root those of the diagonal of M in their natural order. Then the set of $q^n + 1$ lines of $A(\Sigma)$

$$\mathcal{O} = \{X = O\} \cup \{Y = MX + d(M) \mid M \in \mathcal{M}\}$$

is a completely regular line oval (see [19]).

We have the following result.

Theorem 2.5. *The map* $d : \mathcal{M} \to F^n$ *is bijective.*

Proof. If $d(M) = d(N)$ and $M \neq N$, then the three lines $X = O$, $Y = MX + d(M)$ and $Y = NX + d(N)$ would have in common the point $(O^t, d(M)^t)$; this is absurd.

The proof is elementary. However there are interesting consequences. For example

Corollary 2.3. *Every matrix $M \in \mathcal{M}$ is* uniquely determined *by its diagonal.*

In the next section we will exploit this fact in the particular case $n = 2$.

3. Ovoidal translation planes

In this section we investigate symplectic translation plane of even order q^2, with q a power of 2. These planes are strictly related to ovoids in $PG(3, q)$, and therefore Thas called them *ovoidal* (see [24]).

3.1. **Ovoids in $PG(3, q)$.** We limit our exposition to the finite case and so we fix the field $F = GF(q)$.

Definition 3.1. A set Ω of distinct points of $PG(d, q)$ is said to be an *ovoid* if

(1) $|\ell \cap \Omega| \leq 2$, for every line ℓ; and
(2) for every point $P \in \Omega$ the union of all tangent lines (i.e. lines meeting Ω in one point) to Ω at P is a hyperplane, called the *tangent hyperplane* to Ω at P and denoted by $T_P(\Omega)$ (or more simply by T_P).

Examples of ovoids are ovals in $PG(2, q)$ and elliptic quadrics in $PG(3, q)$.

It is easily seen that in $PG(d, q)$ any ovoid contains $q^{d-1} + 1$ points. For, $T_P(\Omega)$ contains $(q^{d-1} - 1)/(q - 1)$ lines through P which have only P in common with Ω. As the number of lines of $PG(d, q)$ on P is $(q^d - 1)/(q - 1)$, there are exactly q^{d-1} lines on P, which are not in $T_P(\Omega)$, and each of them meets Ω in a further point distinct from P. Therefore $|\Omega| = q^{d-1} + 1$.

Remark 3.1. Let $d \geq 3$. If H is a hyperplane of $PG(d, q)$ such that $|H \cap \Omega| > 1$, then $H \cap \Omega$ is an ovoid in the subgeometry H. Such a hyperplane is called a *secant hyperplane to* Ω. Therefore, if Ω is an ovoid in $PG(d, q)$ and H is a secant hyperplane, then $|H \cap \Omega| = q^{d-2} + 1$.

Theorem 3.1. *Let Ω be an ovoid in $PG(d, q)$. Then $d \leq 3$.*

Proof. By the above remark it is enough to prove that $PG(4, q)$ does not contain ovoids. Assume the contrary. If Ω is an ovoid in $PG(4, q)$, then we can form the incidence structure, whose points are the points of Ω and whose blocks are the sections of Ω with all the secant hyperplanes to Ω. Then each block contains the same number $k = q^2 + 1$ of points and through every point there pass the same number $r = q^3 + q^2 + q$ of blocks, which is the number of hyperplanes on a point minus the tangent hyperplane. If $v = q^3 + 1$ is the number of points and b the number of blocks, then counting in two different ways the number of (point, block) pairs which are incident gives $vr = bk$; hence k must divide vr. That is to say $q^2 + 1$ must divide $(q^3 + 1)q(q^2 + q + 1)$; this is absurd, as $q \geq 2$.

In the case $d = 2$, ovoids and ovals are the same objects. So we consider the case $d = 3$.

Theorem 3.2. *Let Ω be an ovoid in $PG(3, q)$. If H is a plane of $PG(3, q)$, then H is either a tangent plane to Ω or H is a secant plane intersecting Ω in $q + 1$ points, which are the points of an oval contained in H.*

Proof. The number of secant planes is $q(q^2 + 1)$ and each of them intersects Ω in $q + 1$ points. Clearly these points constitute an oval contained in the plane section.

The number of tangent planes to Ω is q^2+1. As $PG(3,q)$ has q^3+q^2+q+1 planes, the result follows.

We already noted that elliptic quadrics are ovoids. If q is *odd* also the converse is true. This result was found independently by Barlotti and Panella in 1955, see [2] and [20].

Theorem 3.3. *Let Ω be an ovoid in $PG(3,q)$. If q is* odd*, then Ω is an elliptic quadric.*

The proof uses Theorem 3.2 and relies on Segre's theorem that any oval of $PG(2,q)$, with q odd, is a conic. So every secant plane to the ovoid intersects the ovoid in a conic. Then by selecting nine suitable points on the ovoid, one can construct an elliptic quadric, whose point-set coincides with the ovoid.

It is interesting to note that the proof requires only that every secant plane section is a conic. This was pointed out later by Barlotti.

Theorem 3.4. *Let Ω be an ovoid in $PG(3,q)$. If every secant plane section of Ω is a conic, then Ω is an elliptic quadric.*

Corollary 3.1. *Any ovoid in $PG(3,4)$ is an elliptic quadric.*

For the proof, note that in $PG(2,4)$ every oval is a conic.

Theorem 3.4 was improved by B. Segre, who showed that if at least $(q^3-q^2+2q)/2$ plane sections of an ovoid are conics, then the ovoid is an elliptic quadric. Recently M. R. Brown, see [4], proved the following, stronger result.

Theorem 3.5. *Let Ω be an ovoid in $PG(3,q)$, with q even. If any one of the plane sections of Ω is a conic, then Ω is an elliptic quadric.*

From the above theorems, ovoids containing a conic section and elliptic quadrics are the same objects. It remains to investigate the general case when q is even and greater than 4. The case $q=8$ was treated by Segre, who gave an example of an ovoid that is not an elliptic quadric. Later, with the aid of a computer, it was proven that Segre's example and the elliptic quadrics are the only ovoids in $PG(3,8)$. At the same time Tits discovered a family of ovoids in $PG(3,q)$, where $q=2^{2h+1}$ with $h\geq 1$, which are not elliptic quadrics (see [26]). These are called *Tits ovoids*. When $q=8$ Tits ovoid coincides with Segre's example. Note that Tits ovoids exist only if q is an odd power of 2. Furthermore, they are the only known examples of ovoids other than the elliptic quadrics.

There are many papers on the classification problem of ovoids, each of which tries to prove the following conjecture.

Conjecture: The only ovoids in $PG(3,q)$, q even, are the elliptic quadrics or the Tits ovoids.

An excellent survey on ovoids in $PG(3,q)$ is [18], where the reader can find an almost complete list of references until 1993.

We conclude this section with a fundamental theorem on ovoids in $PG(3,q)$ with q even, due to B. Segre ([22]).

Theorem 3.6. *Let Ω be an ovoid in $PG(3,q)$, where q is even. Let ρ be the map from the set of planes of $PG(3,q)$ to the set of points of $PG(3,q)$, defined as*

follows: if H is the tangent plane to Ω at P, then $\rho(H) = P$; if H is not a tangent plane, then $\rho(H)$ is the nucleus of the oval $H \cap \Omega$. Then ρ is bijective and (ρ^{-1}, ρ) defines a symplectic polarity θ of $PG(3,q)$. Moreover, each collineation that fixes Ω centralizes θ and the absolute (totally isotropic) lines of θ are all the tangent lines to Ω.

Proof. The number of secant planes is $q(q^2+1)$, each of which uniquely determines an oval contained in Ω. The number of tangent planes is q^2+1. As the number q^3+q^2+q+1 of points of $PG(3,q)$ equals the number of the planes, so ρ is bijective. Therefore define $\theta(P) := \rho^{-1}(P)$ for each point P of $PG(3,q)$ and $\theta(H) := \rho(H)$ for each plane H. As for the lines, note that the number of secant lines to Ω is $q^2(q^2+1)/2$ and equals the number of exterior lines to Ω. Then θ fixes each tangent line to Ω and sends the secant line AB to the exterior line $T_A \cap T_B$. The rest of the proof follows from definitions of projective symplectic groups.

3.2. **Symmetric spreadsets and ovoids.** Let $V = V(4,q)$ be a $4-$dimensional vector space over $F = GF(q)$, where $q = 2^d$, equipped with a symplectic form β. Let Σ be a symplectic spread and $A(\Sigma)$ be the corresponding translation plane of (even) order q^2. We choose a suitable basis B of V, as we did in Section 2.1, so that β is represented by the matrix $\begin{pmatrix} O & I \\ I & O \end{pmatrix}$, where O and I are the zero and identity 2×2 matrices. Vector coordinates are now denoted by (x_0, x_1, x_2, x_3) and X and Y will represent the vectors $(x_0, x_1)^t$ and $(x_2, x_3)^t$ of $F \times F = F^2$. Also, as explained in Section 1.4, we can assume that the spread Σ contains $S_0 : Y = O$, $S_\infty : X = O$ and $U : Y = X$. By definition, any two distinct components $S, T \in \Sigma$ intersect only in $\mathbf{0}$. As $2-$subspaces of V are lines of $PG(3,q)$, for which (x_0, x_1, x_2, x_3) represents homogeneous coordinates, we will say, for brevity, that S and T are *skew*. From Section 1.4 we have:

Proposition 3.1. *There is a bijection between the family of totally isotropic $2-$subspaces of V skew with S_∞ and the space of all symmetric 2×2 matrices.*

Let $\mathcal{M}$ be the spreadset for Σ in the fixed basis B; so $\mathcal{M}$ consists of symmetric 2×2 matrices. We call $\mathcal{M}$ a *symmetric spreadset*. In the fixed basis, the components of Σ have equations

$$X = O \quad \text{or} \quad Y = MX\,, \ M \in \mathcal{M}.$$

Moreover, in the corresponding translation plane $A(\Sigma)$ the set of q^2+1 lines

$$\mathcal{O} = \{X = O\} \cup \{Y = MX + d(M)\,, \ M \in \mathcal{M}\}$$

is a line oval and the map $d : \mathcal{M} \to F^2$ is bijective. Because of this and the fact that the set of nonzero elements of $\mathcal{M}$ acts regularly on the nonzero vectors of F^2, every element of the spreadset $\mathcal{M}$ can be uniquely written as

$$\begin{pmatrix} u & \varphi(u,v) \\ \varphi(u,v) & v \end{pmatrix}$$

where $u, v \in F$, and φ is a suitable function $\varphi : F^2 \to F$ such that

(i) $\varphi(0,0) = \varphi(1,1) = 0$; and
(ii) $(u+v)(u'+v') + \varphi(u,v)^2 + \varphi(u',v')^2 \neq 0$ for all $(u,v)^t$, $(u',v')^t$ in F^2 such that $(u,v) \neq (u',v')$.

Properties (i) and (ii) are equivalent to the respective properties (1) and (2) of spreadsets. Conversely, every function φ verifying properties (i) and (ii) uniquely determines a symmetric spreadset.

Now we use the Klein correspondence (see Appendix) to associate symplectic spreads with ovoids in $PG(3,q)$.

Let ℓ be a line of $PG(3,q)$. If ℓ is represented by equations like

$$\begin{cases} a_0x_0 + a_1x_1 + a_2x_2 + a_3x_3 = 0 \\ b_0x_0 + b_1x_1 + b_2x_2 + b_3x_3 = 0 \end{cases}$$

then put

$$z_{ij} = a_ib_j - a_jb_i\,,\ 0 \le i < j \le 3.$$

(As remarked earlier we can dispense with the minus sign, as the characteristic of the field F is 2). The 6−tuple (z_{ij}), $0 \le i < j \le 3$, defines the *dual Plücker coordinates* of ℓ, which for brevity we call *line-coordinates*. These line-coordinates (z_{ij}) can be assumed as homogeneous coordinates of $PG(5,q)$. Then it is straightforward to verify that

$$z_{01}z_{23} + z_{02}z_{13} + z_{03}z_{12} = 0.$$

The above quadratic equation defines a hyperbolic quadric $Q^+(5,q)$ of $PG(5,q)$, which is the *Klein quadric*. Note that this definition is different from that given in the Appendix; but they can be easily proven to be equivalent.

Let Σ be a symplectic spread and $\mathcal{M}$ be a spreadset for Σ determined by a function φ. Let $S \in \Sigma$ be defined by the equations

$$\begin{cases} x_2 = ux_0 + \varphi(u,v)x_1 \\ x_3 = \varphi(u,v)x_0 + vx_1 \end{cases}.$$

As S is a line of $PG(3,q)$, so S corresponds with

$$(uv + \varphi(u,v)^2, \varphi(u,v), u, v, \varphi(u,v), 1)$$

on the Klein quadric $Q^+(5,q)$. S_∞ corresponds with $(1,0,0,0,0,0)$. Then we have obtained a set of q^2+1 points which lie on a parabolic quadric $Q(4,q)$, defined by the equations

$$\begin{cases} z_{02} = z_{13} \\ z_{02}^2 = z_{01}z_{23} + z_{03}z_{12} \end{cases}$$

and contained in $Q^+(5,q)$. Moreover, these q^2+1 points are two by two non-orthogonal with respect to the polarity defined by the Klein quadric. So they constitute an *ovoid* in $Q(4,q)$. Now, $Q(4,q)$ admits as nucleus $N = (0,1,0,0,0,1)$. By projecting $Q(4,q)$ from its nucleus onto $H : z_{02} = z_{13} = 0$ (it is a 3−subspace), identifying H with $PG(3,q)$ and applying the linear collineation h

$$x_0' = x_0,\ x_1' = x_1,\ x_2' = x_3,\ x_3' = x_2$$

we get the set of points

$$\Omega(\mathcal{M}) = \{(uv + \varphi(u,v)^2, u, 1, v) \mid u, v \in F\} \cup \{(1,0,0,0)\}$$

which is an ovoid in $PG(3,q)$. In this representation, the set of points

$$\{(uv + \varphi(u,v)^2, u, 1, v)\,,\ u, v \in F\}$$

is the *set of affine points* of $\Omega(\mathcal{M})$ (points of $PG(3,q) \setminus \{x_2 = 0\}$), while $(1,0,0,0)$ is the unique point at infinity. This construction can be reversed as follows.

Let Ω be an ovoid in $PG(3,q)$. Then Ω determines a symplectic polarity θ which interchanges each tangent plane to Ω with its point of tangency, and each secant plane H to Ω with the nucleus of the oval $H \cap \Omega$. Let β be a symplectic form on V that defines θ. Choose homogeneous coordinates (x_0, x_1, x_2, x_3) in $PG(3,q)$ in such a way that

(1) $U_0 = (1,0,0,0)$, $U_2 = (0,0,1,0)$ and $U = (1,1,1,1)$ are points of Ω;
(2) $x_2 = 0$ and $x_0 = 0$ are tangent planes to Ω at U_0 and U_2 respectively; and
(3) β is represented by the matrix $\begin{pmatrix} O & I \\ I & O \end{pmatrix}$.

As $x_2 = 0$ has only U_0 in common with Ω, so we define as *affine points* of Ω the points of Ω contained in $PG(3,q) \setminus \{x_2 = 0\}$. These points are uniquely determined by coordinates of type $(a,b,1,c)$. The projection of $\Omega \setminus \{U_0\}$ from U_0 onto $x_0 = 0$ is bijective. So if $(a,b,1,c)$ is an affine point of the ovoid, we can assume that a is a function of b and c. In this way we have found a function $G : F \times F \to F$ such that $(a,b,1,c) = (G(b,c),b,1,c)$ for every affine point of Ω. In conclusion, as a set of points,

$$\Omega = \{(G(b,c),b,1,c) \mid b,c \in F\} \cup \{(1,0,0,0)\}.$$

By applying now the linear collineation h (see above) to $(G(b,c),b,1,c)$ and then the inverse of the projection of $Q(4,q)$ from its nucleus N to

$$h((G(b,c),b,1,c)) = (G(b,c),b,c,1),$$

we obtain the point of coordinates

$$(G(b,c), \sqrt{bc + G(b,c)}, b, c, \sqrt{bc + G(b,c)}, 1)$$

on the Klein quadric. Define

$$\varphi(b,c) = \sqrt{bc + G(b,c)} \quad \text{for all} \quad b,c \in F. \tag{2}$$

Then $(G(b,c),\varphi(b,c),b,c,\varphi(b,c),1)$ is the image, under the Klein correspondence, of the line of $PG(3,q)$ represented by the equations

$$\begin{cases} x_2 = bx_0 + \varphi(b,c)x_1 \\ x_3 = \varphi(b,c)x_0 + cx_1 \end{cases}.$$

The function φ, as defined in (2), has then the following two properties:

(i) $\varphi(0,0) = \varphi(1,1) = 0$ (since $(0,0,1,0)$ and $(1,1,1,1)$ are points of Ω); and
(ii) $\varphi(u,v)^2 + \varphi(u',v')^2 + (u+u')(v+v') \neq 0$, for all $(u,v) \neq (u',v')$ (since $(uv + \varphi(u,v)^2, u, 1, v)$ and $(u'v' + \varphi(u',v')^2, u', 1, v')$ correspond with non-orthogonal points on $Q(4,q)$).

Therefore the set of 2×2 matrices

$$\mathcal{M} = \left\{ \begin{pmatrix} u & \varphi(u,v) \\ \varphi(u,v) & v \end{pmatrix} \mid u,v \in F \right\}$$

is a symmetric spreadset.

Theorem 3.7. *The determination of ovoids in $PG(3,q)$ containing $(1,0,0,0)$, $(0,0,1,0)$ and $(1,1,1,1)$, and whose tangent planes at $(1,0,0,0)$ and $(0,0,1,0)$ are $x_2 = 0$ and $x_0 = 0$, respectively, is equivalent to the determination of symmetric spreadsets.*

Remark 3.2. The above theorem is a coordinate-version of a theorem due to Thas (see [24]). Note that this construction produces ovoids of $W(3,q)$, and that ovoids of $W(3,q)$ are also ovoids of $PG(3,q)$.

In the above setting, the only two known examples of ovoids of $PG(3,q)$ are the following.

(E) *Elliptic quadrics*: each of them can be represented as

$$\mathcal{E} = \{(m^2(u^2+v^2)+uv, u, 1, v) \mid u, v \in F\} \cup \{(1,0,0,0)\},$$

where $m \in F$ has nonzero *absolute trace* (the absolute trace of the element $a \in F$ is $\sum_{i=0}^{d-1} a^{2^i}$; it is an element of $GF(2)$). The spreadset

$$\mathcal{M} = \left\{ \begin{pmatrix} u & m\,(u+v) \\ m\,(u+v) & v \end{pmatrix} \mid u, v \in F \right\}$$

is a field isomorphic to $GF(q^2)$ and the corresponding ovoidal translation plane is the desarguesian plane of order q^2. Conversely, to the desarguesian plane of order q^2 there corresponds an elliptic quadric of $PG(3,q)$.

(T) *Tits ovoids*: a canonical form is

$$\mathcal{T} = \{(u^\sigma + v^{\sigma+2} + uv, u, 1, v) \mid u, v \in \mathbf{F}_q\} \cup \{(1,0,0,0)\},$$

where σ is a generator of $\mathrm{Aut}(GF(q))$ such that $\sigma^2 = 2$. Therefore $q = 2^{2r}$ where $r > 1$ is odd. The map φ is given by $\varphi(u,v) = u^{\sigma^{-1}} + v^{1+\sigma^{-1}}$. Tits ovoids correspond with Lüneburg translation planes (see [17]).

The constructioin of Tits ovoids is reported in the Appendix.

3.3. **A research problem.** Let $F = GF(q)$, where $q = 2^d$ and $d \geq 2$. In Section 3.1 we reported Brown's theorem, which states that an ovoid Ω in $PG(3,q)$ is an elliptic quadric if and only if Ω contains a conic plane section.

Exercise 3.1. An ovoid Ω in $PG(3,q)$ contains a conic plane section if and only if Ω can be represented by a symmetric spreadset $\mathcal{M}$ containing the set of scalar matrices

$$\mathcal{S} = \left\{ \begin{pmatrix} a & 0\,\mathbf{0} \\ \mathbf{0} & a \end{pmatrix} \mid a \in F \right\}.$$

From the above exercise Brown's theorem is equivalent to the following one.

Theorem 3.8. *A symmetric spreadset $\mathcal{M}$ contains the set of scalar matrices $\mathcal{S}$ if and only if $\mathcal{M}$ is a field of order q^2.*

Problem 3.1. Give an algebraic proof of Theorem 3.8.

4. Appendix. Geometry of vector spaces

In this Appendix we give a self-contained account of symplectic and orthogonal geometries that one can defines on a vector space. A *geometry* is a triple $\mathcal{G} = (X, \mathcal{F}, G)$, where X is a non-empty set (the *points* of $\mathcal{G}$), $\mathcal{F}$ a family of subsets of X (the *subspaces* of $\mathcal{G}$), and G is a group of permutations of X sending subspaces onto subspaces and preserving incidence. Different groups acting on X give rise to different geometries.

As a general reference, we refer to [23].

4.1. **Linear and semilinear groups.** In this section we study maps between vector spaces defined over the same field K.

Definition 4.1. Let V and W be $K-$vector spaces. A *semilinear map* between V and W is a pair (f,σ), where $f : V \to W$ is a map and σ is an automorphism of the field K, such that for all $a, b \in K$ and $\mathbf{v}, \mathbf{w} \in V$

$$f(a\mathbf{v} + b\mathbf{w}) = a^\sigma f(\mathbf{v}) + b^\sigma f(\mathbf{w}).$$

If σ is the identity, f is called *linear*. If f is bijective, then (f,σ) is said to be a *semilinear isomorphism*. In the case where $V = W$ and f is bijective, then (f,σ) is called a *semilinear automorphism*.

Often we omit reference to σ and simply refer to the semilinear map f, since σ, called the *companion automorphism* of f, is uniquely determined by f.

Let V be a $K-$vector space. The set of all semilinear automorphisms of V, denoted by $\Gamma L(V)$, is a group with respect to the usual operation of composition. $GL(V)$ is the subgroup of $\Gamma L(V)$ consisting of all linear automorphisms of V. It is called *the general linear group* of V. A standard result in linear algebra states that any linear map of V is completely determined by its action on the vectors of a basis. Also, if a basis is fixed, then to any linear map f there is uniquely associated an $n \times n$ matrix A. Changing basis, A changes to $C^{-1}AC$, where C is the matrix of the basis change. Therefore it is well defined the *determinant* of f, to be denoted by $\det(f)$. In particular, $\det(f) \neq 0$ if and only if f is a linear automorphism. If $\det(f) = 1$, then f is called *unimodular*. The set of all unimodular automorphisms of V is a subgroup of $GL(V)$. It is denoted by $SL(V)$ and called the *special linear group* of V.

Proposition 4.1. *(i) The map*

$$j : \Gamma L(V) \to \mathrm{Aut}(K)$$

such that $j(f,\sigma) = \sigma$, where $(f,\sigma) \in \Gamma L(V)$ and $\sigma \in \mathrm{Aut}(K)$, is an epimorphism whose kernel is $GL(V)$. Therefore $GL(V)$ is a normal subgroup of $\Gamma L(V)$ and

$$\Gamma L(V)/GL(V) \cong \mathrm{Aut}(K).$$

(ii) Let K^* be the multiplicative group of the field K. The map

$$\det : GL(V) \to K^*$$

sending each element of $GL(V)$ to its determinant is an epimorphism whose kernel is $SL(V)$. Therefore $SL(V)$ is a normal subgroup of $GL(V)$ and

$$GL(V)/SL(V) \cong K^*.$$

Proof. Exercise.

Notation. The group of all invertible matrices of order n with entries in the field K is denoted by $GL(n,K)$. A similar meaning has the notation $SL(n,K)$. If $K = \mathbf{F}_q$ is the finite field with q elements, then $GL(n,K)$ and $SL(n,K)$ are denoted by $GL(n,q)$ and $SL(n,q)$, respectively.

If $K = \mathbf{F}_q$, where $q = p^r$ is a power of the prime p, the orders of linear and semilinear groups are easily calculated.

Proposition 4.2. *Let $K = \mathbf{F}_q$, where $q = p^r$. For any vector space V of dimension $n \geq 1$ over K the following order formulae hold.*

(1) $|GL(V)| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)$

(2) $|SL(V)| = q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1)$

(3) $|\Gamma L(V)| = r|GL(V)|$

Proof. First observe that $GL(V)$ acts regularly on the set of ordered bases of V, which are

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$$

in number. Therefore

$$|GL(V)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

Then the other order formulae follow from Proposition 4.1, recalling that $|\mathbf{F}_q^*| = q - 1$ and that $|\mathrm{Aut}(K)| = r$.

We assume now that V is a finite dimensional vector space over K and that $\dim_K(V) \geq 2$.

Definition 4.2. A linear automorphism $T \in GL(V)$ is a *transvection* if there is a hyperplane H such that

(i) $T(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in H$, and

(ii) $T(\mathbf{v}) - \mathbf{v} \in H$, for all $\mathbf{v} \notin H$.

The hyperplane H is the *axis* of the transvection.

Note that the definition includes also the identity. In this case, however, the axis is not determined.

There is a very simple formula that describes completely the transvection it represents. Let V^o denote the *dual vector space* of V. The elements of V^o are called *linear functionals* (or also *linear forms*).

Proposition 4.3. *Let T be a tranvection with axis H. If $H = \mathrm{Ker}(f)$ for a suitable linear functional $f \in V^0$, then there is a vector $\mathbf{a} \in H$ such that $f(\mathbf{a}) = 0$ and*

$$T(\mathbf{x}) = \mathbf{x} + f(\mathbf{x})\mathbf{a} \quad \textit{for all} \quad \mathbf{x} \in V.$$

The subspace generated by $\mathbf{a}$ is called the centre *of the transvection T.*

Proof. Let $\mathbf{b} \notin H$. Set

$$\mathbf{c} = f(\mathbf{b})^{-1}\mathbf{b} \quad \text{and} \quad \mathbf{a} = T(\mathbf{c}) - \mathbf{c}.$$

For all $\mathbf{x} \in V$

$$f(\mathbf{x} - f(\mathbf{x})f(\mathbf{b})^{-1}\mathbf{b}) = f(\mathbf{x}) - f(\mathbf{x})f(\mathbf{b})^{-1}f(\mathbf{b}) = 0.$$

Therefore

$$\mathbf{x} - f(\mathbf{x})f(\mathbf{b})^{-1}\mathbf{b} = \mathbf{x} - f(\mathbf{x})\mathbf{c} \in H.$$

Since T is the identity on H, then T fixes the vector $\mathbf{x} - f(\mathbf{x})\mathbf{c}$. So

$$T(\mathbf{x} - f(\mathbf{x})\mathbf{c}) = T(\mathbf{x}) - f(\mathbf{x})T(\mathbf{c}) = \mathbf{x} - f(\mathbf{x})\mathbf{c};$$

whence

$$T(\mathbf{x}) = \mathbf{x} - f(\mathbf{x})[\mathbf{c} - T(\mathbf{c})] = \mathbf{x} + f(\mathbf{x})\mathbf{a}.$$

We will write $T_{f,a}$ to denote the transvection given by the formula

$$\mathbf{x} \mapsto \mathbf{x} + f(\mathbf{x})\mathbf{a}\,, \quad \text{with} \quad f(\mathbf{a}) = 0.$$

Note that the same transvection $T_{f,a}$ can be represented by different pairs $(f, \mathbf{a})$. However, if $T_{f,a}$ is not the identity, then its axis $\mathrm{Ker}(f)$ and its centre $\langle \mathbf{a} \rangle$ are uniquely determined. If we want to consider also the identity as a transvection, we assume for it a formula where $f = 0$ or $\mathbf{a} = \mathbf{0}$.

Proposition 4.4. *For all $f, f_1, f_2 \in V^0$ and $\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2 \in V$ the following identities hold.*

(1) $T_{f,a_1+a_2} = T_{f,a_1} \circ T_{f,a_2}$
(2) $T_{f_1+f_2,a} = T_{f_1,a} \circ T_{f,a_2}$
(3) $s \circ T_{f,a} \circ s^{-1} = T_{f(s^{-1}),f(a)}$, *for all $s \in GL(V)$, where $f(s^{-1})$ is the linear functional*

$$f(s^{-1})(\mathbf{v}) = f(s^{-1}(\mathbf{v})).$$

Proof. Use the formula

$$T_{f,a}(\mathbf{x}) = \mathbf{x} + f(\mathbf{x})\mathbf{a}.$$

From identity 1, we have $T_{f,a}^{-1} = T_{f,-a}$. Hence

Corollary 4.1. *The set of all transvections having the same axis H is a group isomorphic to the additive group of the subspace H.*

Transvections having the same axis H can be represented by nice matrices. Let $E = (\mathbf{e}_1, \ldots, \mathbf{e}_{n-1}, \mathbf{e}_n)$ be a basis of V such that $H = \langle \mathbf{e}_1, \ldots, \mathbf{e}_{n-1} \rangle$. If T is a transvection with axis H, then

$$T(\mathbf{e}_i) = \mathbf{e}_i\,,\ i = 1, \ldots, n-1$$

$$T(\mathbf{e}_n) - \mathbf{e}_n = \sum_{i=1}^{n-1} a_i e_i.$$

So the matrix of T with respect E is

$$A = \begin{pmatrix} 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & a_{n-1} \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

Note that $\det(A) = 1$. Therefore transvections are elements of $SL(V)$. Indeed

Theorem 4.1. *The linear group $SL(V)$ is generated by its transvections.*

For the proof, see [23, Theorem 4.3].

The geometrical ambient where linear groups are studied is that of projective spaces. If V is a vector space over K, then the *projective space* based on V and denoted by $PG(V)$, has as *set of points* the family of $1-$dimensional subspaces of V and as *subspaces* the subspaces of V. It is then defined a map P between the family of subspaces of V and the family of subspaces of $PG(V)$, whose set of points will be denoted by $P(V)$. So if X is a subspace of V the corresponding projective subspace is $P(X)$ and its set of points coincides with the set of all $1-$dimensional subspaces

contained in X. In particular, points of $PG(V)$ are represented as $P(\langle \mathbf{v} \rangle)$, where $\mathbf{v}$ is a non-zero vector. For simplicity, we will write $P(\mathbf{v})$, or, simply, $\langle \mathbf{v} \rangle$.

If $P(X)$ is a (projective) subspace of $PG(V)$, then the (projective) *dimension* of $P(X)$ is $\dim(X) - 1$. In particular, if $\dim(V) = n$, then $PG(V)$ has dimension $n - 1$.

If $K = \mathbf{F}_q$ and $V = V(n+1, q)$ it is customary to write $PG(n, q)$ to denote $PG(V)$.

Definition 4.3. An *isomorphism* between projective spaces $PG(V_1)$ and $PG(V_2)$, defined on the same field, is a bijection of $P(V_1)$ onto $P(V_2)$, sending subspaces onto subspaces and preserving incidence. When $V_1 = V_2$, isomorphisms are called *automorphisms*.

Note that an isomorphism takes collinear points to collinear points, that is to say isomorphisms are *collineations*.

The set of all automorphisms of $PG(V)$ is a group, called *the automorphism group* of $PG(V)$.

Example 4.1. Let $f : V_1 \to V_2$ be a semilinear isomorphism. Then

$$P(f) : PG(V_1) \to PG(V_2)$$

defined by

$$P(f)(\langle \mathbf{v} \rangle) = P(f(\mathbf{v}))$$

is an isomorphism.

Theorem 4.2. (The fundamental theorem of projective geometry) *Let $PG(V_1)$ and $PG(V_2)$ be projective spaces defined on the same field K and of dimension at least 2. If $\varphi : PG(V_1) \to PG(V_2)$ is a collineation, then there is a semilinear isomorphism f of V_1 onto V_2 such that $\varphi = P(f)$. Moreover, if $\varphi = P(f')$, then there exists $a \in K$, with $a \neq 0$, such that*

$$f'(\mathbf{v}) = af(\mathbf{v}), \quad \textit{for all} \quad \mathbf{v} \in V_1.$$

The proof can be found in [23, Theorem 3.1]. From the above theorem we deduce in particular that the map

$$P : \Gamma L(V) \to \mathrm{Aut}(PG(V))$$

(see the above example) is a homomorphism *onto*. So

$$\mathrm{Aut}(PG(V)) \cong \Gamma L(V)/Z$$

where Z is the kernel of the homomorphism. The group Z is the *centre* of $\Gamma L(V)$ and consists of the *scalar maps*, defined for each $a \in K$ by

$$\mathbf{v} \mapsto a\mathbf{v}, \ \mathbf{v} \in V.$$

The group $\mathrm{Aut}(PG(V))$ is then denoted by $P\Gamma L(V)$, and is called *the full collineation group of* $PG(V)$. It contains the two subgroups

$$PGL(V) \cong GL(V)/Z$$

and

$$PSL(V) \cong SL(V)/(Z \cap SL(V)).$$

These groups are called projective groups. The elements of $PG(V)$ are also called *linear collineations*. When $PG(V) = PG(n-1, q)$ the corresponding projective

groups are denoted by $P\Gamma L(n,q)$, $PGL(n,q)$ and $PSL(n,q)$ (note the shift of the dimension).

The following result is one motivation, at least from the point of view of group theory, for the introduction of projective spaces.

Recall that a group is said to be *simple* if it has no proper normal subgroup.

Theorem 4.3. *$PSL(n,q)$ is simple if $n \geq 3$ or $n = 2$ and $q > 3$.*

For the proof, see [23, Theorem 4.5].

For the two exceptions, note that $PS(2,2)$ has order 6 and is isomorphic to a subgroup of S_3. Therefore $PSL(2,2) \cong S_3$, which is not simple, since it admits the normal subgroup A_3.

$PSL(2,3)$ is isomorphic to a subgroup of order 12 of S_4. Therefore $PSL(2,3) \cong A_4$ is not simple.

4.2. **Polar geometry.** Linear groups are the most classical groups. Other interesting groups arise as subgroups of $GL(V)$, generally as groups preserving a sesquilinear form. We limit our introduction to vector spaces of finite dimension over a field F.

Let $V = V(n,F)$ be a $n-$dimensional vector space over a field F.

Definition 4.4. A *$\sigma-$sesquilinear form* on V is a function $\beta : V \times V \to F$ such that, for each $\mathbf{v} \in V$, $\mathbf{u} \mapsto \beta(\mathbf{u},\mathbf{v})$ is a linear map from V to F, and $\mathbf{u} \mapsto \beta(\mathbf{v},\mathbf{u})$ is a $\sigma-$semilinear map from V to F.

A $\sigma-$sesquilinear form β is called *non-degenerate* if $\beta(\mathbf{u},\mathbf{v}) = \mathbf{0}$ for all $\mathbf{u} \in V$ implies $\mathbf{v} = \mathbf{0}$.

If β is a sesquilinear form on V, then we say that the pair of vectors $(\mathbf{u},\mathbf{v})$ is *orthogonal* if $\beta(\mathbf{u},\mathbf{v}) = 0$; we write $\mathbf{u} \perp \mathbf{v}$ (read "$\mathbf{u}$ *perp* $\mathbf{v}$"). If W is a subspace of V, *the orthogonal complement* of W is

$$W^{\perp} = \{\mathbf{v} \in V \mid \beta(\mathbf{v},\mathbf{w}) = 0\,, \quad \text{for all} \quad \mathbf{w} \in W\}.$$

It is easy to prove that $W^{\perp}$ is a subspace of V (even if W is a subset).

Non-degenerate sesquilinear forms are interesting because they define correlations on $PG(V)$.

Definition 4.5. A *correlation* of $PG(V)$ is a bijective map ρ acting on the subspaces of $PG(V)$ which inverts inclusion, that is, for subspaces U, W,

$$U \subseteq W \quad \text{implies} \quad \rho(W) \subseteq U.$$

Theorem 4.4. *Any non-degenerate $\sigma-$sesquilinear form on V induces a correlation of $PG(V)$, and conversely.*

Proof. Let β be a non-degenerate sesquilinear form on V. Then the map $U \mapsto U^{\perp}$ sends subspaces to subspaces and if $U \subseteq W$ then $W^{\perp} \subseteq U^{\perp}$. If we pass from V to $PG(V)$, then $\perp$ induces a correlation of $PG(V)$.

To prove the converse, we appeal to the fundamental theorem of projective geometry. If ρ is a correlation of $PG(V)$, then ρ can be regarded as an isomorphism between $PG(V)$ and its *dual projective space*, which is the projective geometry defined by V^o, the *dual vector space* of V. Then if g is a semilinear map between V and V^o inducing ρ, define

$$\beta(\mathbf{v},\mathbf{w}) = g(\mathbf{w})(\mathbf{v}) \quad \text{for all} \quad \mathbf{v},\mathbf{w} \in V.$$

So β is the required sesquilinear form.

Let β be a sesquilinear form on V and $\perp$ the orthogonality relation it defines. A subspace U of V is called *totally isotropic* if $U \subseteq U^\perp$. Also, a totally isotropic subspace is called *maximal* if it is not properly contained in any other totally isotropic subspace.

Note that a totally isotropic subspace has dimension at most $n/2$ (from $U \subseteq U^\perp$ it follows $\dim(U) \leq \dim(U^\perp) = \dim(V) - \dim(U)$; whence $2\dim(U) \leq \dim(V)$).

The same terminology applies passing from V to $PG(V)$. Note that a point P of $PG(V)$ is either totally isotropic or non-isotropic. In the former case P is also called *absolute*.

The most interesting correlations are polarities: a *polarity* of $PG(V)$ is a correlation of order 2. Then ρ is a polarity if and only if $\rho(\rho(U)) = U$ for every subspace U of $PG(V)$. An easy characterisation of sesquilinear forms inducing polarities is the following. First, we say that a sesquilinear form β is *reflexive* if $\beta(\mathbf{v}, \mathbf{w}) = 0$ implies $\beta(\mathbf{w}, \mathbf{v}) = 0$, for all $\mathbf{v}, \mathbf{w} \in V$. It is easily shown that β is reflexive if and only if

$$\mathbf{w} \in \mathbf{v}^\perp \text{ implies } \mathbf{v} \in \mathbf{w}^\perp.$$

Theorem 4.5. *A correlation is a polarity if and only if the sesquilinear form defining it is reflexive.*

Proof. Let β be a sesquilinear form. Hence, if β is reflexive, then $U \subseteq (U^\perp)^\perp$ for all subspace U of V. By non-degeneracy, $U = (U^\perp)^\perp$. Therefore the map $\perp$ induces a polarity of $PG(V)$.

Conversely, given a polarity ρ, let β be the corresponding non-degenerate sesquilinear form, so that $\rho(U) = U^\perp$. So, if $\mathbf{v} \in \mathbf{w}^\perp$, then $\mathbf{w} \in (\mathbf{w}^\perp)^\perp \subseteq \mathbf{v}^\perp$; hence β is reflexive.

There is a complete classification of non-degenerate, reflexive sesquilinear forms, and so also a classification of polarities.

Definition 4.6. Let β be a $\sigma-$sesquilinear form.

(1) β is said to be $\sigma-$ *Hermitian* if $\beta(\mathbf{v}, \mathbf{w}) = \beta(\mathbf{w}, \mathbf{v})^\sigma$, for all $\mathbf{v}, \mathbf{w} \in V$. If $\sigma = 1$, then β is called *symmetric*.

(2) β is said to be alternating *if $\beta(\mathbf{v}, \mathbf{v}) = 0$ for all $\mathbf{v} \in V$.*

Remark 4.1. Let β be a non-degenerate $\sigma-$Hermitian form. Then

(1) for all $\mathbf{v} \in V$, $\beta(\mathbf{v}, \mathbf{v}) \in Fix(\sigma) = \{a \in F \mid a^\sigma = a\}$.
(2) $\sigma^2 = 1$. Proof: if $c \in F$, then there are $\mathbf{v}, \mathbf{w} \in V$ such that $c = \beta(\mathbf{v}, \mathbf{w})$. Therefore
$$c^{\sigma^2} = \beta(v, w)^{\sigma^2} = (\beta(v, w)^\sigma)^\sigma = \beta(w, v)^\sigma = \beta(v, w) = c.$$
Then $\sigma^2 = 1$.
(3) Let β be alternating. Since $\beta(\mathbf{v}, \mathbf{v}) = 0$ for all $\mathbf{v} \in V$, then $\beta(\mathbf{v}, \mathbf{w}) = -\beta(\mathbf{w}, \mathbf{v})$ for all $\mathbf{v}, \mathbf{w} \in V$, but not conversely, as F may have characteristic 2. Moreover, if F has characteristic 2, then $\beta(\mathbf{v}, \mathbf{w}) = -\beta(\mathbf{w}, \mathbf{v}) = \beta(\mathbf{w}, \mathbf{v})$, that is to say β is also symmetric.

Clearly alternating or $\sigma-$Hermitian forms are reflexive. Also the converse holds.

Theorem 4.6. *Let β be a non-degenerate $\sigma-$sesquilinear form on V. Assume that β is relexive. Then there are exactly the following possibilities.*

(1) $\sigma = 1$, $\beta(\mathbf{v},\mathbf{w}) = \beta(\mathbf{w},\mathbf{v})$, *for all* $\mathbf{v},\mathbf{w} \in V$ *and if* $char(F) = 2$, *then* $\beta(\mathbf{v},\mathbf{v}) \neq 0$ *for some* $\mathbf{v} \in V$. *The form β is called* symmetric.
(2) $\sigma = 1$ *and* $\beta(\mathbf{v},\mathbf{v}) = 0$ *for all* $\mathbf{v} \in V$. *The form β is called* symplectic.
(3) $\sigma^2 = 1 \neq \sigma$ *and* $\beta(\mathbf{v},\mathbf{w}) = \beta(\mathbf{w},\mathbf{v})^\sigma$ *for all* $\mathbf{v},\mathbf{w} \in V$. *The form β is called* unitary.

The corresponding polarities are called orthogonal, symplectic, unitary, *respectively.*

The proof can be found in [23, Theorem 7.1].

Remark 4.2. The terms used in the above theorem have been chosen because the groups connected with these polarities are well known under these names. The more customary terminology for symplectic polarity is *null polarity*.

4.2.1. *Symplectic polar spaces.* We begin our investigation with a $F-$vector space V equipped with a symplectic form β. The pair (V,β) is called a *symplectic space*.

Definition 4.7. The *symplectic group* of (V,β) is the group, denoted by $Sp(V)$, consisting of all linear automorphisms of V which preserve β:

$$Sp(V) = \{g \in GL(V) \mid \beta(g(\mathbf{v}),g(\mathbf{w})) = \beta(\mathbf{v},\mathbf{w})\,, \quad \text{for all} \quad \mathbf{v},\mathbf{w} \in V\}.$$

More generally, the *full symplectic group* is the group of all $f \in \Gamma L(V)$ such that

$$\beta(f(\mathbf{v}),f(\mathbf{w})) = a\beta(\mathbf{v},\mathbf{w})^\sigma$$

for some $a \in F^*$, $\sigma \in \mathrm{Aut}(F)$ and all $\mathbf{v},\mathbf{w} \in V$.

The elements of $\Gamma Sp(V)$ are called *semilinear isometries*, while those of $Sp(V)$ are called *linear isometries*.

Let $B = (\mathbf{v}_1,\ldots,\mathbf{v}_n)$ be a basis of V. Then if J denotes the $n \times n$ matrix whose $(i,j)-$entry is $\beta(\mathbf{v}_i,\mathbf{v}_j) = a_{ij} \in F, i,j = 1,\ldots,n$, we see that

$$\beta(\mathbf{v},\mathbf{w}) = X^tJY.$$

where $X^t = (x_1,\ldots,x_n)$ and $Y^t = (y_1,\ldots,x_n)$ are the coordinates of $\mathbf{v}$ and $\mathbf{w}$ and symbol t means transposition. J is called *the matrix of β* with respect to the basis B. It is a skew-symmetric matrix, that is, $a_{ii} = 0$ and $a_{ij} = -a_{ji}$ for all i,j. Moreover, if $g \in Sp(V)$ and M is the matrix of g with respect to the basis B, then

$$\beta(g(\mathbf{v}),g(\mathbf{w})) = (MX)^tJ(MY) = \beta(\mathbf{v},\mathbf{w}) = X^tJY\,, \quad \text{for all} \quad X,Y \in F^n.$$

Therefore $M^tJM = J$. As a consequence, the elements of $Sp(V)$ have determinant ± 1.

It is always possible to choose suitable bases of V in which the matrix of β has a nice form.

Let $\mathbf{e}_1 \in V$, $\mathbf{e}_1 \neq 0$. We can choose $\mathbf{f}_1$ such that $\beta(\mathbf{e}_1,\mathbf{f}_1) = 1$ (as β is non-degenerate, there is a vector $\mathbf{v}$ such that $\beta(\mathbf{e}_1,\mathbf{v}) \neq 0$; let $\mathbf{f}_1 = \beta(\mathbf{e}_1,\mathbf{v})^{-1}\mathbf{v}$). Then $\mathbf{e}_1,\mathbf{f}_1$ are linearly independent and span a $2-$dimensional subspace $U_1 = \langle \mathbf{e}_1,\mathbf{f}_1\rangle$, which is non-isotropic and is called a *hyperbolic plane*. The pair $(\mathbf{e}_1,\mathbf{f}_1)$ is called a *hyperbolic pair*. As $U_1 \cap U_1^\perp = \{\mathbf{0}\}$, so $V = U_1 \oplus U_1^\perp$ and the restriction of β to $U_1^\perp$ is a symplectic form. Therefore the procedure can be applied to $U_1^\perp$, and note that $\dim(U_1^\perp) = \dim(V) - 2$. Proceeding inductively, we build a basis (called *symplectic*)

$$(\mathbf{e}_1,\mathbf{f}_1,\mathbf{e}_2,\mathbf{f}_2,\ldots,\mathbf{e}_r,\mathbf{f}_r)$$

such that

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_r,$$

where each $U_i = \langle \mathbf{e}_i, \mathbf{f}_i \rangle$, $i = 1, \ldots, n$, is a hyperbolic plane. Also, these hyperbolic planes are mutually orthogonal. Therefore (V, β) has even dimension $2r$. The integer r is the *Witt index* of (V, β). It is an invariant and is the common dimension of maximal totally isotropic subspaces.

In the symplectic basis $(\mathbf{e}_1, \mathbf{f}_1, \mathbf{e}_2, \mathbf{f}_2, \ldots, \mathbf{e}_r, \mathbf{f}_r)$, β has matrix $diag(A, \ldots, A)$, where

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

If the above basis is given a new ordering, we can get the new basis

$$(\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r, \mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_r).$$

With respect to this new basis, β is represented by the matrix

$$J = \begin{pmatrix} O & I \\ -I & O \end{pmatrix}$$

where O and I are the $r \times r$ zero and identity matrices. This matrix is that usually used in the applications. We give an example. Let $M \in Sp(n, F)$. Then M can be represented as a block-matrix, each block being an $r \times r$ matrix:

$$M = \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}.$$

Since the matrix M verifies $M^t J M = J$, then

$$\begin{pmatrix} M_1^t & M_3^t \\ M_2^t & M_4^t \end{pmatrix} \begin{pmatrix} O & I \\ -I & O \end{pmatrix} \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix} = \begin{pmatrix} O & I \\ -I & O \end{pmatrix}.$$

Hence

$$\begin{cases} -M_3^t M_1 + M_1^t M_3 = O \\ -M_3^t M_2 + M_1^t M_4 = I \\ -M_4^t M_2 + M_2^t M_4 = O \end{cases}$$

The matrices $M_1^t M_3$ and $M_2^t M_4$ are symmetric and

$$M_1^t M_4 - M_3^t M_2 = I.$$

In particular, when $n = 2$, then $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $Sp(2, F)$ if and only if $ad - bc = 1$, that is to say $Sp(2, F) = SL(2, F)$.

Let Z be the centre of $\Gamma L(V)$. From what precedes, $Sp(V) \cap Z = \{\pm 1\}$. If we define *the projective symplectic group*, denoted by $PSp(V)$, as the group induced by $Sp(V)$ on $PG(V)$, we have

$$PSp(V) \cong Sp(V)/(Sp(V) \cap Z) = Sp(V)/\{\pm 1\}.$$

The *full projective symplectic group* is $P\Gamma Sp(V) = \Gamma Sp(V)/(\Gamma Sp(V) \cap Z)$.

The *polar symplectic space*, denoted by $\mathcal{S}(V)$, is the family of all totally isotropic subspaces of $PG(V)$. The *polar rank* of $\mathcal{S}(V)$ is the Witt index of V. Note that the set of points of $\mathcal{S}(V)$ coincides with that of $PG(V)$. The group of the symplectic polar space is $PSp(V)$. For, it can be proven that:

(1) $PSp(V)$ acts transitively on the set of points;
(2) $PSp(V)$ sends totally isotropic subspaces to totally isotropic subspaces; and

(3) $PSp(V)$ acts transitively on the family of maximal totally isotropic subspaces.

All the above statements are consequence of Witt's theorem which states that every linear isometry between subspaces of (V, β) extends to a linear isometry of (V, β) (see [23, Theorem 7.4]).

In the finite case the polar symplectic space of polar rank n is denoted by $W(2n-1, q)$, where q is a prime power. It contains

$$\frac{q^{2n}-1}{q-1}$$

points.

Polar spaces have good inductive properties. For example, if $P = \langle \mathbf{v} \rangle$ is a point of $PG(V)$, then the quotient space $\mathbf{v}^{\perp}/\langle \mathbf{v} \rangle$ naturally inherits from β a symplectic form. This new symplectic space has Witt index $n-1$. Moreover, there is a bijection between the family of maximal totally isotropic subspaces of V containing $\mathbf{v}$ and the family of maximal totally isotropic subspaces of the quotient space. We give an application.

Proposition 4.5. *Let $H(n)$ be the number of maximal totally isotropic subspaces of $W(2n-1, q)$. Then*

$$H(n) = \prod_{i=1}^{n} (q^i + 1).$$

Proof. Count in two different ways the ordered pairs $(\mathbf{v}, U)$ where $\mathbf{v}$ is a nonzero vector and U is a maximal totally isotropic subspace containing $\mathbf{v}$. Then

$$\frac{q^n-1}{q-1} H(n) = \frac{(q^n-1)(q^n+1)}{q-1} H(n-1);$$

whence

$$H(n) = (q^n+1)H(n-1)\,, \quad \text{for} \quad n \geq 2$$

and $H(1) = q+1$.

Exercise 4.1. Let (V, β) be a finite symplectic space of Witt index n. Then the number of hyperbolic pairs is

$$(q^{2n}-1)q^{2n-1}.$$

Deduce that

$$|Sp(2n, q)| = \prod_{i=1}^{n} (q^{2i}-1)q^{2i-1} = q^{n^2} \prod_{i=1}^{n} (q^{2i}-1).$$

4.2.2. *Orthogonal polar spaces.* Let $V = V(n, F)$ be a vector space equipped with a symmetric form β. Then there are vectors $\mathbf{v}$ such that $\beta(\mathbf{v}, \mathbf{v}) \neq 0$. Assume that F is a field of characteristic different from 2, and define the map $Q : V \to F$ such that $Q(\mathbf{v}) = \beta(\mathbf{v}, \mathbf{v})$ for all $\mathbf{v} \in V$. Then Q has the following properties:

(i) $Q(a\mathbf{v}) = a^2 Q(\mathbf{v})$, for all $\mathbf{v} \in V$ and all $a \in F$; and
(ii) $2\beta(\mathbf{v}, \mathbf{w}) = Q(\mathbf{v}+\mathbf{w}) - Q(\mathbf{v}) - Q(\mathbf{w})$, for all $\mathbf{v}, \mathbf{w} \in V$.

If a basis is fixed, then Q is represented by a quadratic homogeneous polynomial in n variables, and so it is called a quadratic form. Conversely, any such polynomial uniquely determines a symmetric form, because of (ii) above.

To treat at the same time the case of the characteristic different from two and that of characteristic two, it is convenient to give an intrinsic definition of quadratic form and then to start with such a form.

Definition 4.8. A *quadratic form* on V is a map $Q : V \to F$ such that for all $a \in F$ and $\mathbf{v}, \mathbf{w} \in V$

(1) $Q(a\mathbf{v}) = a^2 Q(\mathbf{v})$; and
(2) the map $\beta : V \times V \to F$ defined by

$$\beta(\mathbf{v}, \mathbf{w}) = Q(\mathbf{v} + \mathbf{w}) - Q(\mathbf{v}) - Q(\mathbf{w}) \quad \text{for all} \quad \mathbf{v}, \mathbf{w} \in V$$

is a bilinear form, called the *polar form* of Q.

We say that a quadratic form Q is *non-degenerate* (or also *non-singular*) if Q is nonzero on every nonzero vector of $V^\perp$, where, as usual, $\perp$ denotes the orthogonality relation defined by the polar form of Q.

Remark 4.3. Let Q be a quadratic form and β its polar form. If $char(F) \neq 2$, then Q is non-degenerate if and only if β is non-degenerate. Also, in this case, letting $\mathbf{v} = \mathbf{w}$ in property (2) above gives $\beta(\mathbf{v}, \mathbf{v}) = 2Q(\mathbf{v})$ for all $\mathbf{v} \in V$. Therefore in characteristic different from two Q is uniquely determined by β, and conversely. Note also that β is symmetric. On the other hand, if the field has characteristic two, then letting $\mathbf{v} = \mathbf{w}$ as above gives $\beta(\mathbf{v}, \mathbf{v}) = 0$ for all $\mathbf{v} \in V$, so that β is alternating. In other words, V becomes a symplectic space. Furthermore, if the field is *perfect* (i.e. the map $x \mapsto x^2$, $x \in F$, is an automorphism) and Q is non-degenerate, then $\dim(V^\perp) \leq 1$. For, the restriction of Q to $V^\perp$ satisfies

$$Q(\mathbf{v} + \mathbf{w}) = Q(\mathbf{v}) + Q(\mathbf{w}) \quad \text{and} \quad Q(a\mathbf{v}) = a^2 Q(\mathbf{v}), \ \mathbf{v}, \mathbf{w} \in V, \ a \in F$$

that is to say $Q_{|V^\perp}$ is a semilinear map from $V^\perp$ to F. As Q is non-degenerate, then the the kernel of its restriction to $V^\perp$ contains only the zero vector. So if $V^\perp$ contains some nonzero vector, then $V^\perp \cong F$.

An *orthogonal space* is a pair (V, Q), where Q is a non-degenerate quadratic form on V. The *orthogonal group* or the *isometry group* of (V, Q) is

$$O(V, Q) := \{f \in GL(V) \mid Q(f(\mathbf{v})) = Q(\mathbf{v}) \quad \text{for all} \quad \mathbf{v} \in V\}.$$

The *full orthogonal group* is

$$\Gamma O(V, Q) := \{f \in \Gamma L(V) \mid Q(f(\mathbf{v})) = aQ(\mathbf{v})^\sigma \quad \text{for all} \quad \mathbf{v} \in V \quad \text{and some} \quad a \in F\}.$$

Finally, the *general orthogonal group* is

$$GO(V, Q) := \Gamma O(V, Q) \cap GL(V).$$

A nonzero vector $\mathbf{v} \in V$ is called *singular* if $Q(\mathbf{v}) = 0$. A subspace U of V is said to be *totally singular* if $Q(\mathbf{u}) = 0$ for all $\mathbf{u} \in U$. Let U be a totally singular subspace. Then for all $\mathbf{u}, \mathbf{v} \in U$,

$$\beta(\mathbf{u}, \mathbf{v}) = Q(\mathbf{u} + \mathbf{v}) - Q(\mathbf{u}) - Q(\mathbf{v}) = 0.$$

Therefore U is totally isotropic (with respect to β). When $char(F) \neq 2$ also the converse holds, but it is false in characteristic two (every $1-$dimensional subspace is totally isotropic, as β is alternating, but there are non-singular vectors for Q, because of non-degeneracy).

A totally singular subspace is called *maximal* if it is not properly contained in any other totally singular subspace.

Finally, a subspace U of V is called *anisotropic* if $Q(\mathbf{u}) \neq 0$ for all nonzero vector $\mathbf{u} \in U$ (i.e., U does not contain singular vectors).

Let (V, Q) be an orthogonal space and let β be the polar form of Q. Assume $\dim(V) = n$ and let $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V. If $\mathbf{v} = \sum_{i=1}^{n} x_i \mathbf{v}_i$ then

$$Q(\mathbf{v}) = Q\left(\sum_{i=1}^{n} x_i \mathbf{v}_i\right) = \sum_{i=1}^{n} x_i^2 Q(\mathbf{v}_i) + \sum_{i<j} x_i x_j \beta(\mathbf{v}_i, \mathbf{v}_j).$$

Put $b_{ii} = Q(\mathbf{v}_i)$, $i = 1, \ldots, n$, and

$$b_{ij} = \begin{cases} \beta(\mathbf{v}_i, \mathbf{v}_j) & \text{for } 1 \leq i < j \leq n \\ 0 & \text{for } i > j \end{cases}.$$

Then we obtain an upper triangular matrix B, that we call *the matrix of* Q in the fixed basis. If $X^t = (x_1, \ldots, x_n)$ are vector coordinates, then

$$Q(\mathbf{v}) = X^t B\, X.$$

If $x_1, \ldots, x_n$ are regarded as indeterminates over F, then $X^t BY$ is a homogeneous quadratic polynomial. Therefore it is meaningful to define a *quadric* of $PG(V)$ as the set of points $P = \langle \mathbf{v} \rangle$ such that $Q(\mathbf{v}) = 0$. If Q is non-degenerate the corresponding quadric is called *non-degenerate* (or also *non-singular*).

Note that the matrix of β can be recovered from the matrix of Q, letting $A = B + B^t$. If $char(F) \neq 2$, then A is symmetric, while if $char(F) = 2$, A is skew-symmetric.

A pair of vectors $(\mathbf{v}, \mathbf{w})$ is a *hyperbolic pair* if $Q(\mathbf{v}) = Q(\mathbf{w}) = 0$ and $\beta(\mathbf{v}, \mathbf{w}) = 1$. If Q is non-degenerate, then every hyperbolic pair spans a hyperbolic plane. Following a similar pattern as that used for symplectic spaces, we can decompose V as the direct sum of r hyperbolic planes $U_i = \langle \mathbf{e}_i, \mathbf{f}_i \rangle$, where $(\mathbf{e}_i, \mathbf{f}_i)$ is a hyperbolic pair, for $i = 1, \ldots, r$, and one anisotropic space U:

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_r \oplus U. \tag{3}$$

The integer r is an invariant, called *the Witt index* of Q. Also the isomorphism class of the anisotropic space appearing in the above decomposition is an invariant. So a complete classification for orthogonal spaces requires a complete classification for all anisotropic spaces. In many cases this is not a simple problem. When $F = GF(q)$, a classification of anisotropic subspaces is available.

Lemma 4.1. *Let (V, Q) be an orthogonal space of dimension at least three. Then there are singular vectors.*

Proof. A consequence of Chevalley's theorem (see [12]) states that any homogeneous polynomial of degree two in at least three variables admits at least one non-trivial zero.

Corollary 4.2. *If the orthogonal space (V, Q) is anisotropic then $\dim(V) \leq 2$.*

Exercise 4.2. Let $F(x, y, z)$ be a homogeneous polynomial of degree two over $GF(q)$. Then the number of zeros of $F(x, y, z)$ is $q + 1$.

In the finite case the complete classification of orthogonal spaces is as follows. We refer to decomposition (3).

I. $\dim(U) = 0$. Then $U = \{\mathbf{0}\}$, $\dim(V) = 2r$ and for each positive integer r there is just one orthogonal space, up to isometries. In the basis $(\mathbf{e}_1, \ldots, \mathbf{e}_r, \mathbf{f}_1, \ldots, \mathbf{f}_r)$, which, in a different ordering, is that determined for decomposition (3), a canonical form of Q is

$$Q(x_1, \ldots, x_r, y_1, \ldots, y_r) = \sum_{i=1}^{r} x_i y_i,$$

where $(x_1, \ldots, x_r, y_1, \ldots, y_r)$ represents vector coordinates. The two subspaces

$$\langle \mathbf{e}_1, \ldots, \mathbf{e}_r \rangle \quad \text{and} \quad \langle \mathbf{f}_1, \ldots, \mathbf{f}_r \rangle$$

are maximal totally singular subspaces.

In this case the orthogonal group is denoted by $O^+(2r, q)$, and the quadratic form is called *hyperbolic*.

II. $\dim(U) = 1$. Then $U = \langle \mathbf{u} \rangle$, $Q(\mathbf{u}) \neq 0$ and $\dim(V) = 2r+1$. The geometry is different, according as $Q(\mathbf{u})$ is either a square or a nonsquare in the field. A canonical form for Q with respect to the basis

$$(\mathbf{e}_1, \ldots, \mathbf{e}_r, \mathbf{f}_1, \ldots, \mathbf{f}_r, \mathbf{u})$$

is

$$Q(x_1, \ldots, x_r, y_1, \ldots, y_r, z) = \sum_{i=1}^{r} x_i y_i + Q(\mathbf{u}) z^2.$$

In the case of characteristic two, every element of the field is a square. In the odd characteristic case the field has squares and nonsquares. However the orthogonal group is in any case the same, since one can pass from one quadratic form to the other by multiplying with a nonsquare. Therefore the orthogonal group is denoted by $O(2r+1, q)$ and the quadratic form is called *parabolic*.

III. $\dim(U) = 2$. Then $\dim(V) = 2r + 2$. Furthermore there are vectors $\mathbf{e}, \mathbf{f}$ such that

$$U = \langle \mathbf{e}, \mathbf{f} \rangle, \; Q(\mathbf{e}) = 1 \quad \text{and} \quad \beta(\mathbf{e}, \mathbf{f}) = 1.$$

Then

$$Q(x\mathbf{e} + y\mathbf{f}) = x^2 + xy + ay^2, \quad \text{where} \quad a = Q(\mathbf{f}).$$

The polynomial $x^2 + x + a$ is irreducible over F (otherwise U would have singular vectors). A canonical form for Q with respect to the basis

$$(\mathbf{e}_1, \ldots, \mathbf{e}_r, \mathbf{f}_1, \ldots, \mathbf{f}_r, \mathbf{e}, \mathbf{f})$$

is

$$Q(x_1, \ldots, x_r, y_1, \ldots, y_r, x, y) = \sum_{i=1}^{r} x_i y_i + x^2 + xy + ay^2.$$

The orthogonal group is denoted by $O^-(2r+2, q)$ and the quadratic form is called *elliptic*.

The integer r appearing in each of the above canonical forms is called the *Witt index* (or simply the *index*) of Q, and will be denoted by $m = m(Q)$. It is an invariant for Q and the number $g(Q) = m(Q) - 1$ represents the projective dimension of maximal totally singular subspaces contained on the quadric defined by Q. Also

$\dim(U)$ is an invariant for Q, that we call the *type* of Q. We denote it by $\delta = \delta(Q)$. Note that in each of the above cases $\dim(V) = n = 2r + \delta$.

In $PG(V)$ we defined a non-singular quadric as the set of points

$$\mathcal{Q} = \{\langle \mathbf{v} \rangle \in PG(V) \mid Q(\mathbf{v}) = 0\},$$

where Q is a non-degenerate quadratic form on V. In other words, $\mathcal{Q}$ is the set of all the projective points represented by the singular vectors for Q. Also, we say that two quadrics of $PG(V)$ are *equivalent* if there is a collineation of $PG(V)$ sending one to the other. The *index* and the *type* of a non-singular quadric are the Witt index and the type of the quadratic form defining it, respectively. The above classification of finite orthogonal spaces translates in $PG(d, q)$ to the following theorem.

Theorem 4.7. *Let $PG(d, q)$ be the $d-$dimensional projective geometry over $F = GF(q)$.*

(1) *If d is* even*, then all the non-singular quadrics of $PG(d, q)$ are equivalent, have index $m = d/2$, type $\delta = 1$ and the group preserving each of them is $PGO(d + 1, q)$. Such quadrics are called* parabolic*.*
(2) *If d is* odd*, then there are two equivalence classes of non-singular quadrics of respective indexes $m = (d + \varepsilon)/2$, where $\varepsilon = \pm 1$. In the case $\varepsilon = 1$, the quadric is called* hyperbolic*, has type $\delta = 0$ and its group is $PGO^+(d+1, q)$. In the case $\varepsilon = -1$, the quadric is called* elliptic*, has type $\delta = 2$ and its group is $PGO^-(d + 1, q)$.*

Each of the above quadrics gives rise to an *orthogonal polar space*. Here is the list.

(1) $\mathcal{P}(2m, q)$ is the *parabolic polar space*. Its subspaces are the totally singular subspaces contained in the parabolic quadric of $PG(2m, q)$. The *polar rank* is m, its type is $\delta = 1$ and the group is $PGO(2r + 1, q)$.
(2) $\mathcal{H}(2m + 1, q)$ is the *hyperbolic polar space*. Its subspaces are the totally singular subspaces contained in the hyperbolic quadric of $PG(2m + 1, q)$. The *polar rank* is m, its type is $\delta = 0$ and the group is $PGO^+(2m + 1, q)$.
(3) $\mathcal{E}(2m + 1)$ is the *elliptic polar space*. Its subspaces are the totally singular subspaces contained in the elliptic quadric of $PG(2m + 1, q)$. The *polar rank* is m, its type is $\delta = 2$ and the group is $PGO^-(2m + 1, q)$.

We calculate now the number of points of each polar space. Let $\mathcal{Q}_d$ be a non-singular quadric in $PG(d, q)$ defined by a quadratic form Q. Let β be the polar form of Q. We say that a line ℓ is tangent to $\mathcal{Q}_d$ if ℓ meets the quadric in exactly one point.

Proposition 4.6. *Let $A = \langle \mathbf{a} \rangle \in \mathcal{Q}_d$. For every point $B = \langle \mathbf{b} \rangle \neq A$, let ℓ be the line through A and B.*

(i) *If $\langle \mathbf{b} \rangle \notin \mathcal{Q}_d$, then $\beta(\mathbf{a}, \mathbf{b}) = 0$ if and only if the line ℓ is tangent to $\mathcal{Q}_d$.*
(ii) *If $\langle \mathbf{b} \rangle \in \mathcal{Q}_d$, then $\beta(\mathbf{a}, \mathbf{b}) = 0$ if and only if ℓ is completely contained in $\mathcal{Q}_d$.*
(iii) *$\beta(\mathbf{a}, \mathbf{b}) \neq 0$ if and only if $|\ell \cap \mathcal{Q}_d| = 2$.*

Proof. All points of ℓ except $\langle \mathbf{a} \rangle$ are represented as $\langle t\mathbf{a} + \mathbf{b} \rangle$, where $t \in F$. Therefore $\langle t\mathbf{a} + \mathbf{b} \rangle$ belongs to $\mathcal{Q}_d$ if and only if

$$Q(t\mathbf{a} + \mathbf{b}) = t^2 Q(\mathbf{a}) + Q(\mathbf{b}) + t\beta(\mathbf{a}, \mathbf{b}) = Q(\mathbf{b}) + t\beta(\mathbf{a}, \mathbf{b}) = 0.$$

The value $t = 0$ corresponds with B. A simple discussion of the above equation proves all statements.

Let $P = \langle \mathbf{a} \rangle$ be a point on $\mathcal{Q}_d$. The map $\beta(\mathbf{a}, -) : V \to F$ is a linear functional from V onto F. Its kernel defines a hyperplane in $PG(V)$, called *the tangent hyperplane* to the quadric at P and denoted by $T_P = T_P(\mathcal{Q}_d)$.

Theorem 4.8. *Let T_P be the tangent hyperplane to $\mathcal{Q}_d$ at P. Then*

(i) *T_P consists of all points on the tangent lines to $\mathcal{Q}_d$ at P and on the lines through P contained in $\mathcal{Q}_d$;*
(ii) *T_P contains every subspace S such that $P \in S \subset \mathcal{Q}_d$;*
(iii) *If $d \geq 3$, then T_P meets $\mathcal{Q}_d$ in a cone which projects from P a non-singular quadric $\mathcal{Q}_{d-2}$ contained in a subspace of dimension $d-2$, which is contained in T_P and does not contain P. Moreover, $\mathcal{Q}_d$ and $\mathcal{Q}_{d-2}$ have the same type and $m(\mathcal{Q}_d) = m(\mathcal{Q}_{d-2}) + 1$.*

Proof. The proof of items (i) and (ii) easily follows from Proposition 4.6. For the proof of (iii) we make use of coordinates. Let $(x_0, x_1, \ldots, x_d)$ be homogeneous coordinates in $PG(d, q)$. Denote by U_0, U_1,..., U_d and U the fundamental points of the reference, and assume:

(1) $P = U_d$;
(2) $U_0, U_1, \ldots, U_{d-2}$ are in T_P; and
(3) U_{d-1} is in $\mathcal{Q}_d$.

Then T_P has equation $x_{d-1} = 0$. As U_{d-1} and $U_d = P$ are both in $\mathcal{Q}_d$, then an equation for $\mathcal{Q}_d$ is

$$\sum_{i=0}^{d-2} a_{ii} x_i^2 + \sum_{0 \leq i < j \leq d-1} a_{ij} x_i x_j + x_{d-1} x_d = 0.$$

The linear substitution $x_i \mapsto x_i,\ i = 0, \ldots, d-1,\ x_d \mapsto -(\sum_{i=0}^{d-2} a_{i,d-1} x_i) + x_d$ transforms the above equation to the equation

$$\sum_{i=0}^{d-2} a_{ii} x_i^2 + \sum_{0 \leq i < j \leq d-2} a_{ij} x_i x_j + x_{d-1} x_d = 0.$$

P and T_P remain fixed under the above transformation. Therefore $T_P \cap \mathcal{Q}_d$ has equations

$$(*) \begin{cases} x_{d-1} = 0 \\ \sum_{i=0}^{d-2} a_{ii} x_i^2 + \sum_{0 \leq i < j \leq d-2} a_{ij} x_i x_j = 0 \end{cases}$$

which represent a non-singular quadric $\mathcal{Q}_{d-2}$ in the subspace $x_{d-1} = x_d = 0$, which is contained in T_P and does not contain P. $\mathcal{Q}_{d-2}$ has the same type as $\mathcal{Q}_d$ and $m(\mathcal{Q}_d) = m(\mathcal{Q}_{d-2}) + 1$, since the quadratic forms which define $\mathcal{Q}_d$ and $\mathcal{Q}_{d-2}$ differ by the term $x_{d-1} x_d$. In $PG(V)$ the variety represented by equations (*) is a cone which projects from P the quadric $\mathcal{Q}_{d-2}$.

A point $\langle \mathbf{v} \rangle$ of $PG(d, q)$ is a *nucleus* of $\mathcal{Q}_d$ if $\beta(\mathbf{v}, \mathbf{w}) = 0$ for all $\langle \mathbf{w} \rangle$ in $PG(d, q)$. From this definition it follows that $\dim(V^{\perp}) = 1$, and so d must be even. Looking at the canonical forms that a non-degenerate quadratic form can have, we see that $\mathcal{Q}_d$ has a nucleus if and only if q and d are both even and, if this is the case, then $\mathcal{Q}_d$ is parabolic, and its nucleus is unique and does not belong to $\mathcal{Q}_d$. Furthermore, all the tangent hyperplanes to $\mathcal{Q}_d$ meet in the nucleus.

Theorem 4.9. *Let $\mathcal{Q}_d$ be a non-singular quadric of $PG(d,q)$ defined by the quadratic form Q with polar form β. Then the following statements hold.*

(i) *If q and d are not both even, then β induces a polarity on $PG(d,q)$. For q odd the polarity is orthogonal and the set of absolute points is $\mathcal{Q}_d$. If q is even the polarity is symplectic (null polarity) and every point of $PG(d,q)$ is absolute.*

(ii) *If q and d are both even, then $\mathcal{Q}_d$ is parabolic and all the tangent hyperplanes to $\mathcal{Q}_d$ meet in the nucleus.*

(iii) *Let δ and r be the type and the index of $\mathcal{Q}_d$. Then $d = 2r - 1 + \delta$ and*

$$|\mathcal{Q}_d| = (q^{r-1+\delta} + 1)(q^r - 1)/(q - 1).$$

Proof. We need to prove only item (iii). We proceed by induction on d. By Exercise 4.2 the formula holds for $d = 2$. So assume $d \geq 3$. Let P be a point of $\mathcal{Q}_d$. The number of lines of $PG(d,q)$ on P is

$$q^{d-1} + q^{d-2} + \cdots + q + 1 = (q^d - 1)/(q - 1),$$

while the number of lines of T_P on P is

$$q^{d-2} + q^{d-1} + \cdots + q + 1 = (q^{d-1} - 1)/(q - 1).$$

Then in $PG(d,q)$ there are q^{d-1} lines on P which are not in T_P and each of them meets $\mathcal{Q}_d$ in exactly one point distinct from P. The lines of T_P which meet the quadric out of the set of the previous points are the generatrices of the cone $P\mathcal{Q}_{d-2}$ (see the above theorem), its number equals the number of points of $\mathcal{Q}_{d-2}$ and each of them contains q points of $\mathcal{Q}_{d-2}$ distinct from P (every line of $PG(d,q)$ has $q+1$ points). Let $a_{d-2} = |\mathcal{Q}_{d-2}|$. Then

$$(*) \quad |\mathcal{Q}_{d-2}| = q^{d-1} + 1 + qa_{d-2}.$$

As $\mathcal{Q}_d$ and $\mathcal{Q}_{d-2}$ have the same type, $m(\mathcal{Q}_d) = m(\mathcal{Q}_{d-2}) + 1$ and $d = 2r - 1 + \delta$, so by the inductive hypothesis

$$a_{d-2} = (q^{r-2+\delta} + 1)(q^{r-1} - 1)/(q - 1).$$

Substituting for a_{d-2} its value in (*), the result follows.

Let $\mathcal{S}$ be an orthogonal polar space. If $\mathcal{S}$ has polar rank m then the subspaces of dimension $g = m - 1$ contained in $\mathcal{S}$ are called *the generators* of $\mathcal{S}$. Let $\mathcal{G}(\mathcal{S})$ be the family of all generators of $\mathcal{S}$.

Theorem 4.10. *The numbers of generators of the finite orthogonal polar spaces are as follows:*

(i) $|\mathcal{G}(\mathcal{P}(2m,q))| = \prod_{i=1}^{m}(q^i + 1)$

(ii) $|\mathcal{G}(\mathcal{H}(2m+1,q))| = 2\prod_{i=1}^{m}(q^i + 1)$

(iii) $|\mathcal{G}(\mathcal{E}(2m+1,q))| = \prod_{i=1}^{m}(q^{i+1} + 1)$

For the proof, and further properties of quadrics, see [10].

The polar space $\mathcal{H}(2m+1,q)$ deserves particular attention. Given two generators M_1 and M_2, define M_1 to be equivalent to M_2 if $\dim(M_1 \cap M_2) \equiv m \pmod 2$. It

can be proven (see [10, Theorem 22.4.12]) that the relation on the generators is an equivalence relation with two equivalence classes.

4.3. **The Klein correspondence.** Let $V = V(4, F)$ be a 4−dimensional vector space over a field F. The Klein correspondence is, in its basic aspect, a map from the family of 2−dimensional subspaces of V onto a certain set of 1−dimensional subspaces of $\Lambda_2 V$, the *second exterior algebra* of V, which has dimension 6 over F. More precisely, it determines a well defined correspondence between the projective geometry $PG(V)$ and the geometry of a non-singular quadric of $PG(\Lambda_2 V)$, called the *Klein quadric*. We will give only an introductory account based upon the use of coordinates.

Let $B = (\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ be a basis of V. For $\mathbf{u} \in V$ the notation $\mathbf{u} = (x_i)$ means that the vector $\mathbf{u}$ has coordinates (x_0, x_1, x_2, x_3).

We define $\Lambda_2 V$ to be the 6−dimensional vector space over F having as a basis *the symbols* $\mathbf{e}_i \wedge \mathbf{e}_j$, $0 \le i < j \le 3$, and such that the "wedge map"

$$\wedge : V \to \Lambda_2 V$$

sending $(\mathbf{u}, \mathbf{v})$ to

$$\mathbf{u} \wedge \mathbf{v} = \sum_{0 \le i < j \le 3} (x_i y_j - x_j y_i)\, \mathbf{e}_i \wedge \mathbf{e}_j,$$

for all $\mathbf{u} = (x_i)$ and $\mathbf{v} = (y_i)$ in V, is bilinear and alternating. The elements of $\Lambda_2 V$ are called *bivectors*.

Now let ℓ be a line of $PG(V)$. Then $\ell = \langle \mathbf{u}, \mathbf{v} \rangle$ for some pair of linearly independent vectors $\mathbf{u}, \mathbf{v} \in V$. The *Plücker coordinates* of ℓ are the coordinates of the bivector $\mathbf{u} \wedge \mathbf{v}$, that is, if $\mathbf{u} = (x_i)$ and $\mathbf{v} = (y_i)$, then the Plücker coordinates of ℓ are

$$p_{ij} = x_i y_j - x_j y_i\,,\ 0 \le i < j \le 3.$$

Up to a nonzero factor of proportion, Plücker coordinates are well defined. For if $\ell = \langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{u}', \mathbf{v}' \rangle$, then $\mathbf{u}' = a\mathbf{u} + b\mathbf{v}$, $\mathbf{v}' = c\mathbf{u} + d\mathbf{v}$, where $ad - bc \neq 0$. Hence

$$\mathbf{u}' \wedge \mathbf{v}' = (a\mathbf{u} + b\mathbf{v}) \wedge (c\mathbf{u} + d\mathbf{v}) = (ad - bc)(\mathbf{u} \wedge \mathbf{v}),$$

that is $p'_{ij} = (ad - bc)p_{ij}$, $0 \le i < j \le 3$. We have therefore a well defined map, denoted by κ, from the set of lines of $PG(V)$ into the set of points of $PG(\Lambda_2 V)$. We want to determine the image of κ.

Remark 4.4. A line ℓ of $PG(V)$ is also determined by any two distinct planes containing ℓ. So if $\sum_{i=0}^{3} u_i x_i = 0$ and $\sum_{i=0}^{3} v_i x_i = 0$ are two planes on ℓ, we define the *dual Plücker coordinates* of ℓ as

$$p^*_{ij} = u_i v_j - u_j v_i\,,\ 0 \le i < j \le 3.$$

It is easily verified that

$$p^*_{01} p^*_{23} - p^*_{02} p^*_{13} + p^*_{03} p^*_{12} = 0$$

and that

$$(p^*_{01}, p^*_{02}, p^*_{03}, p^*_{12}, p^*_{13}, p^*_{23}) = a(p_{23}, -p_{13}, p_{12}, p_{03}, -p_{02}, p_{01}),$$

where $a \in F^*$.

Notation. If ℓ is a line of $PG(V)$ and (p_{ij}), $0 \leq i < j \leq 3$, are its Plücker coordinates, we write simply

$$\ell = (p_{ij}).$$

If $P = \langle \mathbf{v} \rangle$ is a point of $PG(V)$ and $\mathbf{v} = (x_i)$, then we write $P = (x_i)$, and say that (x_i) are the coordinates of P.

Finally, if $P = (x_i)$ is a point and A is a 4×4 matrix, then we write AP to mean the product of A with the 4×1 matrix whose column is given by the coordinates of P.

Lemma 4.2. *Let $\ell = (p_{ij})$ be a line of $PG(V)$. Then*

$$p_{01}p_{23} - p_{02}p_{13} + p_{03}p_{12} = 0.$$

The proof is a straightforward calculation.

We denote by $(z_{01}, z_{02}, z_{03}, z_{12}, z_{13}, z_{23})$ vector coordinates on $\Lambda_2 V$. Coherently, if $\mathbf{z} \in \Lambda_2 V$, then $\mathbf{z} = (z_{ij})$ means that the bivector $\mathbf{z}$ has coordinates (z_{ij}), $0 \leq i < j \leq 3$.

For $\mathbf{z} = (z_{ij})$ in $\Lambda_2 V$, define

$$Q_\kappa(z) = z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12}.$$

Then Q_κ is a quadratic form and its polar form β_κ is given by

$$\beta_\kappa(\mathbf{z}, \mathbf{z}') = z_{01}z'_{23} + z_{23}z'_{01} - (z_{02}z'_{13} + z_{13}z'_{02}) + z_{03}z'_{12} + z_{12}z'_{03}.$$

The form β_κ is non-degenerate, and so Q_κ is a non-degenerate quadratic form. Furthermore, the subspaces

$$H_1 = \langle \mathbf{e}_0 \wedge \mathbf{e}_1, \mathbf{e}_2 \wedge \mathbf{e}_3 \rangle\,,\ H_2 = \langle \mathbf{e}_0 \wedge \mathbf{e}_2, \mathbf{e}_1 \wedge \mathbf{e}_3 \rangle\,,\ H_3 = \langle \mathbf{e}_0 \wedge \mathbf{e}_3, \mathbf{e}_1 \wedge \mathbf{e}_2 \rangle$$

are hyperbolic planes of $\Lambda_2 V$ and

$$\Lambda_2 V = H_1 \oplus H_2 \oplus H_3.$$

We have proven the following proposition.

Proposition 4.7. *Q_κ is a non-degenerate quadratic form of Witt index 3.*

We denote by $\mathcal{K}$ the quadric of $PG(\Lambda_2 V)$ defined by Q_κ. It is known as the *Klein quadric*.

Theorem 4.11. *The map κ that associates to every line of $PG(V)$ its Plücker coordinates is a bijection between the lines of PGV) and the points of the Klein quadric.*

Proof. By Lemma 4.2 the image of κ is contained in $\mathcal{K}$. The rest of the proof relies on the following construction. Let $\mathbf{z} = (z_{ij}) \in \Lambda_2 V$. Associate to $\mathbf{z}$ the 4×4 skew-symmetric matrix

$$A(\mathbf{z}) = \begin{pmatrix} 0 & z_{01} & z_{02} & z_{03} \\ -z_{01} & 0 & z_{12} & z_{13} \\ -z_{02} & -z_{12} & 0 & z_{23} \\ -z_{03} & -z_{13} & -z_{23} & 0 \end{pmatrix}.$$

By direct calculation,

$$\det(A(\mathbf{z})) = (z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12})^2 = (Q_\kappa(\mathbf{z}))^2.$$

It is easy to verify that the map $\mathbf{z} \mapsto A(\mathbf{z})$ is bijective and that the set of singular bivectors (bivectors $\mathbf{z}$ such that $Q_\kappa(\mathbf{z}) = 0$) corresponds bijectively with the set of

all 4×4 singular, skew-symmetric matrices. Since a 4×4 skew-symmetric matrix A determines an alternating form on V, then the rank of A is even, and so it can be either 0 or 2 or 4. Therefore the set of nonzero singular bivectors corresponds bijectively with the set of 4×4 rank 2 skew-symmetric matrices.

Now a rank 2 skew-symmetric matrix

$$A(\mathbf{z}) = \begin{pmatrix} 0 & z_{01} & z_{02} & z_{03} \\ -z_{01} & 0 & z_{12} & z_{13} \\ -z_{02} & -z_{12} & 0 & z_{23} \\ -z_{03} & -z_{13} & -z_{23} & 0 \end{pmatrix}$$

determines a 2−dimensional subspace of V, which is the subspace spanned by two linearly independent vectors corresponding with two linearly independent rows of $A(\mathbf{z})$. Assume that two linearly independent rows are the first two. Since $z_{01}z_{12} - z_{02}z_{13} + z_{03}z_{12} = 0$, then $z_{01} \neq 0$. The 2-subspace spanned by $(0, z_{01}, z_{02}, z_{03})$ and $(-z_{01}, 0, z_{12}, z_{13})$ determines a line ℓ whose Plücker coordinates are

$$(p_{ij}) = (z_{01}^2, z_{01}z_{02}, z_{01}z_{03}, z_{01}z_{12}, z_{01}z_{13}, z_{02}z_{13} - z_{12}z_{03}).$$

Since $z_{01}z_{23} = z_{02}z_{13} - z_{12}z_{03}$, then

$$(p_{ij}) = z_{01}(z_{01}, z_{02}, z_{03}, z_{12}, z_{13}, z_{23}),$$

that is to say the line ℓ of $PG(V)$ corresponds with the point $\langle \mathbf{z} \rangle$ on the Klein quadric.

The map κ as above described is known as the *Klein correspondence*, because its geometric properties give a complete correspondence between the projective geometry $PG(V)$ and the geometry of the Klein quadric.

We illustrate some of these properties. For the sake of simplicity, if ℓ is a line of $PG(V)$, we write $Q_\kappa(\ell)$ to denote the value of Q_κ on the bivector whose coordinates are the Plücker coordinates of ℓ. A similar meaning has the notation $\beta_\kappa(\ell, \ell')$.

Proposition 4.8. *Two lines ℓ and ℓ' of $PG(V)$ intersect if and only if $\beta_\kappa(\ell, \ell') = 0$.*

Proof. Let $\ell = \langle \mathbf{u}, \mathbf{v} \rangle$ and $\ell' = \langle \mathbf{u}', \mathbf{v}' \rangle$, where $\mathbf{u} = (x_i)$, $\mathbf{v} = (y_i)$, $\mathbf{u}' = (x_i')$, $\mathbf{v}' = (y_i')$. Then ℓ and ℓ' intersect if and only if

$$\begin{vmatrix} x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ x_0' & x_1' & x_2' & x_3' \\ y_0' & y_1' & y_2' & y_3' \end{vmatrix} = 0.$$

Hence

$$p_{01}p_{23}' - p_{02}p_{13}' + p_{03}p_{12}' + p_{12}p_{03}' - p_{13}p_{02}' + p_{23}p_{01}' = 0,$$

that is, $\beta_\kappa(\ell, \ell') = 0$.

Proposition 4.9. *Let (P, H) be an incident point-plane pair of $PG(V)$. Denote by $\Sigma_{P,H}$ the pencil of lines contained in H, and whose centre is P. Then κ maps $\Sigma_{P,H}$ to the points of a line contained in $\mathcal{K}$. Conversely, every line contained in $\mathcal{K}$ is of type $\Sigma_{P,H}$ for some pair (P, H).*

Proof. Let $P = \langle \mathbf{u} \rangle$ and $H = \langle \mathbf{u}, \mathbf{v}, \mathbf{w} \rangle$, where $\mathbf{u}, \mathbf{v}, \mathbf{w}$ are linearly independent. The two lines $\ell = \langle \mathbf{u}, \mathbf{v} \rangle$ and $m = \langle \mathbf{u}, \mathbf{w} \rangle$ generate the pencil $\Sigma_{P,H}$. Every line of this pencil has the form

$$\ell' = \langle \mathbf{u}, a\mathbf{u} + b\mathbf{v} + c\mathbf{w} \rangle \,, \text{ where } a, b, c \in F.$$

The Plücker coordinates of ℓ' are the coordinates of the bivector

$$\mathbf{u} \wedge (a\mathbf{u} + b\mathbf{v} + c\mathbf{w}) = b(\mathbf{u} \wedge \mathbf{v}) + c(\mathbf{u} \wedge \mathbf{w}).$$

Therefore every line of $\Sigma_{P,H}$ is mapped by κ onto the points of the line spanned by $\mathbf{u} \wedge \mathbf{v}$ and $\mathbf{u} \wedge \mathbf{w}$. Conversely, let $r = \langle \mathbf{u} \wedge \mathbf{v}, \mathbf{u}' \wedge \mathbf{w} \rangle$ be a line contained in $\mathcal{K}$. Then

$$\beta_\kappa(\mathbf{u} \wedge \mathbf{v}, \mathbf{u}' \wedge \mathbf{w}) = 0.$$

By Proposition 4.8 the two lines $\ell = \langle \mathbf{u}, \mathbf{v} \rangle$ and $m = \langle \mathbf{u}', \mathbf{w} \rangle$ intersect and so they span a plane H. We can assume $H = \langle \mathbf{u}, \mathbf{v}, \mathbf{w} \rangle$ and $\ell = \langle \mathbf{u}, \mathbf{v} \rangle$, $m = \langle \mathbf{u}, \mathbf{w} \rangle$. Then every point on the line $r \subset \mathcal{K}$ is the image of a line of $\Sigma_{P,H}$, where $P = \langle \mathbf{u} \rangle$.

We saw that Q_κ has index 3. So $\mathcal{K}$ contains subspaces of two dimensions, that is planes. We determine the family of all such planes.

Let P be a point and H a plane of $PG(V)$. Define

$$\kappa(P) := \{\kappa(\ell) \mid \ell \text{ is a line of } PG(V) \text{ on } P\}$$

$$\kappa(H) := \{\kappa(\ell) \mid \ell \text{ is a line of } PG(V) \text{ and } \ell \subset H\}.$$

Proposition 4.10. *For every point P and every plane H of $PG(V)$, $\kappa(P)$ and $\kappa(H)$ are planes contained in $\mathcal{K}$ and every plane contained in $\mathcal{K}$ has either the form $\kappa(P)$ or the form $\kappa(H)$. Moreover,*

(i) *two distinct planes U_1 and U_2 contained in $\mathcal{K}$ intersect in a point if and only if either $U_1 = \kappa(P_1)$ and $U_2 = \kappa(P_2)$ or $U_1 = \kappa(H_1)$ and $U_2 = \kappa(H_2)$; and*

(ii) *$\kappa(P)$ and $\kappa(H)$ intersect in a line if and only if $P \in H$.*

Proof. The set of lines of $PG(V)$ on the point $P = \langle \mathbf{u} \rangle$ can be represented by three non-complanar lines:

$$\ell_1 = \langle \mathbf{u}, \mathbf{v}_1 \rangle, \ \ell_2 = \langle \mathbf{u}, \mathbf{v}_2 \rangle, \ \ell_3 = \langle \mathbf{u}, \mathbf{v}_3 \rangle$$

where $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are linearly independent. Therefore every line ℓ on P has the form

$$\ell = \langle \mathbf{u}, a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3\mathbf{v}_3 \rangle$$

and so its Plücker coordinates are the coordinates of the bivector

$$\mathbf{u} \wedge (a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3\mathbf{v}_3) = a_1(\mathbf{u} \wedge \mathbf{v}_1) + a_2(\mathbf{u} \wedge \mathbf{v}_2) + a_3(\mathbf{u} \wedge \mathbf{v}_3).$$

As the bivectors $\mathbf{u} \wedge \mathbf{v}_1$, $\mathbf{u} \wedge \mathbf{v}_2$ and $\mathbf{u} \wedge \mathbf{v}_3$ are linearly independent, so the set $\kappa(P)$ is the plane spanned by these bivectors.

To prove that $\kappa(H)$ is a plane, let ℓ_1, ℓ_2, ℓ_3 be three non-concurrent lines of H. We can assume

$$\ell_1 = \langle \mathbf{u}, \mathbf{v}_1 \rangle, \ \ell_2 = \langle \mathbf{u}, \mathbf{v}_2 \rangle, \ \ell_3 = \langle \mathbf{v}_1, \mathbf{v}_2 \rangle$$

and $H = \langle \mathbf{u}, \mathbf{v}_1, \mathbf{v}_2 \rangle$. Let ℓ be a line contained in H. Assume that ℓ_1, ℓ_2 and ℓ are not concurrent. Then

$$\ell = \langle a\mathbf{u} + b\mathbf{v}_1, c\mathbf{u} + d\mathbf{v}_2 \rangle$$

and its Plücker coordinates are the coordinates of the bivector

$$(a\mathbf{u} + b\mathbf{v}_1) \wedge (c\mathbf{u} + d\mathbf{v}_2) = ad(\mathbf{u} \wedge \mathbf{v}_2) + bc(\mathbf{v}_1 \wedge \mathbf{u}) + bd(\mathbf{v}_1 \wedge \mathbf{v}_2).$$

So $\kappa(\ell)$ belongs to the plane spanned by $\mathbf{u} \wedge \mathbf{v}_2$, $\mathbf{v}_1 \wedge \mathbf{u}$ and $\mathbf{v}_1 \wedge \mathbf{v}_2$.

Conversely, let U be a plane contained in $\mathcal{K}$. If $U = \langle \mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3 \rangle$, where $\mathbf{z}_i \in \Lambda_2 V$, then $\beta_\kappa(\mathbf{z}_i, \mathbf{z}_j) = 0$. By Proposition 4.8, the three lines ℓ_1, ℓ_2, ℓ_3 of $PG(V)$ corresponding with $\mathbf{z}_1$, $\mathbf{z}_2$, $\mathbf{z}_3$, respectively, either have a point P in common or span a plane H. In the first case $U = \kappa(P)$; in the second case $U = \kappa(H)$.

For the proof of statement (i) it suffices to note that two distinct pencils of lines have exactly one line in common (the join of the centres), and that two distinct plane intersect in one line.

Proof of (ii). If $\kappa(P) \cap \kappa(H)$ is a line, then $\kappa(P) \cap \kappa(H) = \langle \mathbf{z}_1, \mathbf{z}_2 \rangle$, and $\kappa^{-1}(\langle \mathbf{z}_1 \rangle) = \ell_1$ and $\kappa^{-1}(\langle \mathbf{z}_2 \rangle) = \ell_2$ are two intersecting lines of $PG(V)$. Then

$$P \in \ell_1 \cap \ell_2 \subset H.$$

Conversely, if $P \in H$, then the set of lines contained in H and passing through P corresponds, via κ, with the point-set of a line contained in $\mathcal{K}$; hence $\kappa(P) \cap \kappa(H)$ is a line.

We denote by $\mathcal{M}_1$ (resp., $\mathcal{M}_2$) the family of planes of type $\kappa(P)$ (resp., $\kappa(H)$). Because of the above theorem, κ establishes a correspondence between points, lines and planes of $PG(V)$ and planes of $\mathcal{M}_1$, points of $\mathcal{K}$ and planes of $\mathcal{M}_2$. Moreover, the triple $(\mathcal{M}_1, \mathcal{K}, \mathcal{M}_2)$ becomes an incidence structure with the following relation of incidence:

- $\kappa(P) \in \mathcal{M}_1$ is incident with $Z \in \mathcal{K}$ if the point Z is in $\kappa(P)$;
- $k(P)$ is incident with $\kappa(H)$ if $\kappa(P) \cap \kappa(H)$ is a line; and
- a point Z of $\mathcal{K}$ is incident with $\kappa(H)$ if Z is in $\kappa(H)$.

Therefore κ is an isomorphism of the projective geometry $PG(V)$ of points, lines and planes with the incidence structure $(\mathcal{M}_1, \mathcal{K}, \mathcal{M}_2)$.

We end this section noting (but omitting any development and detail) that the Klein correspondence gives rise to a homomorphism between the semilinear group $\Gamma L(V)$ and the semilinear group $\Gamma L(\Lambda_2 V)$. If $(g, \alpha) \in \Gamma L(V)$, define $\overline{g} \in \Gamma L(\Lambda_2 V)$ letting

$$\overline{g}(\mathbf{v} \wedge \mathbf{w}) = g(\mathbf{v}) \wedge g(\mathbf{w}).$$

4.4. **Tits ovoids.** We retain the notation introduced in the previous section and assume that F is a *perfect field* of characteristic 2 (this means that the map $x \mapsto x^2$, $x \in F$, is an automorphism, called *the Frobenius automorphism*).

Let π be a symplectic polarity of $PG(V) = PG(3, F)$ and $\mathcal{A}$ be the set of all totally isotropic lines. $\mathcal{A}$ is commonly called a *linear complex* (of lines). Recall that, up to equivalence, $PG(V)$ admits only one symplectic polarity. Therefore we fix a system of homogeneous coordinates (x_0, x_1, x_2, x_3) in $PG(3, F)$ in such a way that the symplectic polarity is induced by the symplectic form β represented by the matrix

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

Note that we can dispense with the minus sign, since the characteristic of the field is two. In this setting the polar plane of the point $P = (a_0, a_1, a_2, a_3)$ is the plane $P^\perp : a_2 x_0 + a_3 x_1 + a_0 x_2 + a_1 x_3 = 0$.

Proposition 4.11. *Let $\ell = (p_{ij})$ be a line of $PG(3, F)$. Then ℓ belongs to $\mathcal{A}$ if and only if $p_{02} + p_{13} = 0$.*

Proof. Let $\ell = \langle \mathbf{u}, \mathbf{v} \rangle$ with $\mathbf{u} = (x_i)$ and $\mathbf{v} = (y_i)$. Then ℓ is totally isotropic if and only if $\beta(\mathbf{u}, \mathbf{v}) = x_0y_2 + x_2y_0 + x_1y_3 + x_3y_1 = 0$, that is to say $p_{02} + p_{13} = 0$.

As a consequence, the linear complex $\mathcal{A}$ is mapped by κ onto the section of $\mathcal{K}$ with the hyperplane $H_4 : z_{02} + z_{13} = 0$. So in H_4 it is determined the parabolic quadric $\mathcal{P}_4$ of equations

$$\begin{cases} z_{02} + z_{13} = 0 \\ z_{01}z_{23} + z_{02}z_{13} + z_{03}z_{12} = 0 \end{cases}$$

or equivalently

$$\begin{cases} z_{13} = z_{02} \\ z_{02}^2 = z_{01}z_{23} + z_{03}z_{12}. \end{cases}$$

$\mathcal{P}_4$ has as nucleus the point $N = (0, 1, 0, 0, 1, 0)$, which is $H_4^{\perp}$. Project now the parabolic quadric $\mathcal{P}_4$ from N onto the subspace of three dimensions $S_3 : z_{02} = z_{13} = 0$. Then the point $Z = (z_{01}, z_{02}, z_{03}, z_{12}, z_{02}, z_{23})$ of $\mathcal{P}_4$ is mapped to the point of coordinates $(z_{01}, 0, z_{03}, z_{12}, 0, z_{23})$. Identify S_3 with $PG(V) = PG(3, F)$ and then define a map δ_1 which sends the line $\ell = (p_{ij})$ of $\mathcal{A}$ to the point $\delta_1(\ell) = (p_{01}, p_{03}, p_{23}, p_{12})$ of $PG(V)$.

The map δ_1 is nothing else that the Klein correspondence κ, followed by the projection p from the point N, the identification i of S_3 with $PG(V)$ and the homography h of $PG(V)$ defined by the equations

$$ax'_0 = x_0,\ ax'_1 = x_1,\ ax'_2 = x_3,\ ax'_3 = x_2.$$

Note that h is involutory.

The map δ_1 is clearly bijective. Its inverse is

$$\delta_1^{-1}(a_0, a_1, a_2, a_3) = (a_0, \sqrt{a_0a_2 + a_1a_3}, a_1, a_3, \sqrt{a_0a_2 + a_1a_3}, a_2).$$

For brevity, the composition of maps $h \circ i \circ p$ will be called "the projection from N".

Now we define a bijective map δ_2 between the points of $PG(V)$ and the lines of $\mathcal{A}$. We first describe the map that will be its inverse. Let ℓ be a totally isotropic line. By applying the inverse of the projection from N, the line ℓ corresponds with a line contained in $\mathcal{P}_4$, and thus contained in the Klein quadric. By Proposition 4.9 this line uniquely determines a pencil of lines in $PG(V)$, which has a well defined centre.

Then the map δ_2 is defined as follows. Let P be a point of $PG(V)$. Consider the set of all totally isotropic lines through P. These lines are contained in the plane $P^{\perp}$ and are mapped by κ to a line contained in $\mathcal{P}_4$, which projects to a line of $PG(3, F)$, that will be proved to be totally isotropic. To this end we write equations for δ_2. So, let $P = (a_0, a_1, a_2, a_3)$ and ℓ and m be two distinct, totally isotropic lines meeting in P. They are determined by two points not collinear with P in the plane $P^{\perp}$ which has the equation

$$a_2x_0 + a_3x_1 + a_0x_2 + a_1x_3 = 0.$$

Assume $a_3 \neq 0$ and let

$$\ell = \langle (a_0, a_1, a_2, a_3), (a_3, a_2, 0, 0) \rangle\ ,\ m = \langle (a_0, a_1, a_2, a_3), (0, a_0, a_3, 0) \rangle.$$

Then

$$\ell = (a_0a_2 + a_1a_3, a_2a_3, a_3^2, a_2^2, a_2a_3, 0)$$

and

$$m = (a_0^2, a_0a_3, 0, a_0a_2 + a_1a_3, a_0a_3, a_3^2),$$

respectively. Projecting from N and applying the homography h we obtain the two points of $PG(V)$ of coordinates

$$(a_0a_2 + a_1a_3, a_3^2, 0, a_2^2)$$

and

$$(a_0^2, 0, a_3^2, a_0a_2 + a_1a_3).$$

The line spanned by them has Plücker coordinates

$$a_3^2(a_0^2, a_0a_2 + a_1a_3, a_1^2, a_3^2, a_0a_2 + a_1a_3, a_2^2)$$

which is totally isotropic, as the second and fifth coordinate are equal. Therefore δ_2 is a bijection between the set of points of $PG(V)$ and the set of lines of $\mathcal{A}$. In terms of coordinates, δ_2 maps the point of coordinates (x_0, x_1, x_2, x_3) to the line whose Plücker coordinates are

$$(x_0^2, x_0x_2 + x_1x_3, x_1^2, x_3^2, x_0x_2 + x_1x_3, x_2^2).$$

The two maps δ_1 and δ_2 define a *correlation* δ of the symplectic polar space $W(3, F)$. Following Tits, we ask under which conditions $W(3, F)$ admits a polarity, that is, a correlation of order 2.

Theorem 4.12. *Let F be a perfect field of characteristic two. Then $W(3, F)$ admits a polarity if and only if F has an automorphism σ such that $\sigma^2 = 2$, where $x \mapsto x^2$ is the Frobenius automorphism.*

Proof. First of all note that the correlation δ as above defined is such that

$$\delta^2(x_0, x_1, x_2, x_3) = (x_0^2, x_1^2, x_2^2, x_3^2) = (x_0, x_1, x_2, x_3)^2;$$

hence δ^2 acts as the collineation of $PG(V)$ induced by the Frobenius automorphism.

Assume that there is a field automorphism σ such that $\sigma^2 = 2$. Then by direct calculation, $\rho = \sigma^{-1} \circ \delta$ is a correlation of $W(3, F)$ whose square is the identity, that is, ρ is a polarity. (Here σ^{-1} indicates the collineation induced by the automorphism σ^{-1}).

Conversely, suppose that there is a polarity ρ. A suitable symplectic reference frame can be chosen so that $\rho = \sigma^{-1} \circ \delta$, where σ is a field automorphism. Since $\delta^2 = 2$ and $\rho^2 = 1$, then $\sigma^2 = 2$, as required.

We have now all the ingredients to define Tits ovoids. Let σ be an automorphism of F such that $\sigma^2 = 2$. For all $x \in F$ the following identities are easily verified:

$$(x^{\sigma+1})^{\sigma-1} = x\,, \ (x^{\sigma+2})^{\sigma-1} = x^{\sigma}.$$

(It is sufficient to note that the set of all endomorphisms of the field F is a ring) Therefore the endomorphisms $\sigma + 1$, $\sigma - 1$ and $\sigma + 2$ of the multiplicative group F^* are bijective. A necessary condition for the existence of an automorphism σ such that $\sigma^2 = 2$ is that F does not contain (a subfield isomorphic to) $GF(4)$. If $F = GF(q)$, where $q = 2^h$, then h *odd* is a necessary and sufficient condition for the existence of σ. If $h = 2e + 1$, then the unique automorphism σ such that $\sigma^2 = 2$, is

$$x \mapsto x^{2^{e+1}}.$$

Assume that $W(3,F)$ admits the polarity $\rho = \sigma^{-1} \circ \delta$ (see above). We use standard terminology for the polarity ρ:

- if $\ell = \rho(P)$, then ℓ is the *polar line* of P and P is the *pole* of ℓ
- a point P of $W(F)$ is *absolute* if $P \in \rho(P)$
- a line ℓ of $W(F)$ is *absolute* if $\rho(\ell) \in \ell$
- two points P and Q of $W(F)$ are *conjugate* if $P \in \rho(Q)$ (and $Q \in \rho(P)$)
- two lines ℓ and m of $W(F)$ are *conjugate* if $\rho(\ell) \in m$ (and $\rho(m) \in \ell$)

Let $\mathcal{A}$ be the set of all the absolute lines of ρ and Ω be the set of absolute points of ρ.

Theorem 4.13. *Ω is an ovoid of $PG(V)$.*

The proof uses the following two lemmas.

Lemma 4.3. *Let A be a non-absolute point and $\ell = \rho(A)$. Then the unique point A' on ℓ conjugate to A has as its polar line the line $\ell' = AA'$. In particular, A' and ℓ' are absolute.*

Proof. Let $A = \langle \mathbf{u} \rangle$. Then $\mathbf{u}^\perp$ meets ℓ in a unique point $A' = \langle \mathbf{u}' \rangle$, as $\ell \notin \mathcal{A}$. The line $\ell' = \langle \mathbf{u}, \mathbf{u}' \rangle$ belongs to $\mathcal{A}$. For, $\ell' = \mathbf{u}^\perp \cap \mathbf{u}'^\perp$ and so $\beta(\mathbf{u}, \mathbf{u}') = 0$. Moreover, ℓ' is the polar line of A'.

Lemma 4.4. *Every line ℓ of $\mathcal{A}$ contains exactly one absolute point. Every point P belongs to exactly one absolute line.*

Proof. The two statements are dual. So it is enough to prove only the first.

If $\rho(\ell) \in \ell$, then $\rho(\ell)$ is an absolute point and is the unique absolute point on ℓ. For if B is another absolute point on ℓ, $B \neq \rho(\ell)$, then $B \in \ell$ and $\rho(\ell) \in \rho(B)$; so $\rho(B) = \ell$ and $B = \rho(\ell)$, a contradiction.

Let now $\rho(\ell) \notin \ell$. By the previous lemma, the point $A \in \ell$ conjugate to $\rho(\ell)$ is absolute. Conversely, if $A \in \ell$ is absolute, then $\rho(A)$ contains A and $\rho(\ell)$; so A and $\rho(\ell)$ are conjugate.

Proof. [Theorem 4.13] Because of Lemma 4.4, every line of $\mathcal{A}$ meets Ω in one point. Moreover, the lines of $\mathcal{A}$ on a point $P \in \Omega$ constitute a plane. Thus it remains to prove that every line not in $\mathcal{A}$ meets Ω in either 0 or 2 points. It suffices to show that if $\ell \notin \mathcal{A}$ and $\ell \cap \Omega \neq \emptyset$, then $|\ell \cap \Omega| = 2$.

Let $A \in \ell \cap \Omega$. As $\ell \notin \mathcal{A}$, so the set $\cap_{P \in \ell} P^\perp$ is a line ℓ'. Let $B = \rho(A) \cap \ell'$. The two lines $\rho(B)$ and ℓ' intersect, since they both belong to $A^\perp$. Therefore let $C = \rho(B) \cap \ell'$. Finally, let A' be a point on ℓ distinct from A and

$$C' = \rho(A'B) = \rho(A') \cap \rho(B).$$

Hence $A' = \rho(C') \cap \ell$.

If $A' \in \Omega$, then C' is conjugate to A'. Hence

$$C' = (A')^\perp \cap \rho(B) = (A')^\perp \cap A^\perp \cap \rho(B) = \ell' \cap \rho(B) = C.$$

Conversely, the two lines $\rho(C)$ and ℓ intersect, since they both belong to the plane $B^\perp$ and $\rho(C) \cap \ell$ is the unique point on $\rho(C)$ conjugate to C and so absolute, because of Lemma 4.3.

Now we write equations for Ω which will prove that Ω is not an elliptic quadric.

Let $P = (x_0, x_1, x_2, x_3)$ be a point of Ω. Then

$$\begin{aligned}\rho(P) &= \sigma^{-1} \circ \delta(x_0, x_1, x_2, x_3) = \\ &= (x_0^2, x_0x_2 + x_1x_3, x_1^2, x_3^2, x_0x_2 + x_1x_3, x_2^2)^{\sigma^{-1}} = \\ &= (x_0^\sigma, (x_0x_2 + x_1x_3)^{\sigma^{-1}}, x_1^\sigma, x_3^\sigma, (x_0x_2 + x_1x_3)^{\sigma^{-1}}, x_2^\sigma)\end{aligned}$$

as $2\sigma^{-1} = \sigma$. Since $P \in \Omega$ if and only if $P \in \rho(P)$, then we get

$$\begin{cases} x_2^\sigma x_1 + (x_0x_2 + x_1x_3)^{\sigma^{-1}} x_2 + x_3^{\sigma+1} = 0 \\ x_2^\sigma x_0 + x_1^\sigma x_2 + (x_0x_2 + x_1x_3)^{\sigma^{-1}} x_3 = 0 \\ (x_0x_2 + x_1x_3)^{\sigma^{-1}} x_0 + x_1^{\sigma+1} + x_0^\sigma x_3 = 0 \\ x_3^\sigma x_0 + (x_0x_2 + x_1x_3)^{\sigma^{-1}} x_1 + x_0^\sigma x_2 = 0 \end{cases}$$

The above equations are obtained from the following

Exercise 4.3. Associate to the line $\ell = (p_{ij})$ the skew-symmetric matrix

$$\Lambda_\ell = \begin{pmatrix} 0 & p_{23} & -p_{13} & p_{12} \\ -p_{23} & 0 & p_{03} & -p_{02} \\ p_{13} & -p_{03} & 0 & p_{01} \\ -p_{12} & p_{02} & -p_{01} & 0 \end{pmatrix}.$$

Then the point $P = (x_i)$ belongs to $\ell = (p_{ij})$ if and only if

$$\Lambda_\ell P = O.$$

If $x_2 = 0$, then the above system has the unique solution $(1, 0, 0, 0)$. In other words, the plane $x_2 = 0$ is the tangent plane to Ω at $(1, 0, 0, 0)$. So, let $x_2 \neq 0$ and introduce non-homogeneous coordinates

$$x = x_0/x_2\,,\ y = x_1/x_2\,,\ z = x_3/x_2.$$

The point of coordinates $(x, y, 1, z)$ belongs to Ω if and only if

$$\begin{cases} y + (x + yz)^{\sigma^{-1}} + z^{\sigma+1} = 0 \\ x + y^\sigma + (x + yz)^{\sigma^{-1}} z = 0 \\ (x + yz)^{\sigma^{-1}} x + y^{\sigma+1} + x^\sigma z = 0 \\ z^\sigma x + (x + yz)^{\sigma^{-1}} y + x^\sigma = 0 \end{cases}$$

It is easy to verify that the above system has as set of solutions the set

$$\{(x, y, 1, z) \mid x + yz + y^\sigma + z^{\sigma+2} = 0\}.$$

Proposition 4.12. *Ω is the union of the point $(1, 0, 0, 0)$ and the affine set represented by the equation*

$$x = yz + y^\sigma + z^{\sigma+2}.$$

It follows that if $F \neq GF(2)$ then Ω is not an elliptic quadric. The ovoid Ω is the *Tits ovoid*. The equation

$$x = yz + y^\sigma + z^{\sigma+2}$$

is the affine canonical form of Ω.

References

[1] J. André, *Über nicht-Desarguessche ebenen mit transitiver translationsgruppe*, Math. Z., 60(1954), 156-186.

[2] A. Barlotti, *Un'estensione del teorema di Segre-Kustaanheimo*, Boll. Unione Mat. Ital., 10(1955), 96-98.

[3] M. Biliotti & V. Jha & N. L. Johnson, *Foundation of translation planes*, Monographs and Textbooks in Pure and Applied Mathematics, 243, M. Dekker Inc., New York, 2001.

[4] M. R. Brown, *Ovoids of $PG(3,q)$, q even, with a conic section*, J. London Math. Soc., (2)62(2000), 569-582.

[5] A. R. Calderbank & P. J. Cameron & W. M. Kantor & J. J. Seidel, *$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets*, Proc. London Math. Soc., (3)75(1997), 436-480.

[6] P. J. Cameron & J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge Univ. Press, Cambridge, 1991.

[7] A. M. Cohen & H. A. Wilbrink, *The stabilizer of Dye's spread on a hyperbolic quadric in $PG(4n-1,2)$ within the orthogonal group*, Rend. Acc. Naz. Lincei, 69(1980), 22-25.

[8] R. H. Dye, *Partition and their stabilizers for line complexes and quadrics*, Annali di Matem., (4)114(1977), 173-194.

[9] J. W. P. Hirschfeld, *Projective geometries over finite fields* Clarendon Press, Oxford, 1998, 2nd ed. .

[10] J. W. P. Hirschfeld & J. A. Thas, *General Galois geometries*, Oxford Math. Monographs, Clarendon Press, Oxford, 1991.

[11] D. R. Hughes & F. C. Piper, *Projective planes*, Springer, Berlin, Heidelberg, New York, 1973.

[12] J.-R. Joly, *Équations et variétés algébriques sur un corps fini*, Enseignement Math., (2)19(1973), 1-117.

[13] W. M. Kantor, *Spreads, translation planes and Kerdock sets, I, II*, SIAM J. Algebraic Discrete Methods 3, (1982), 151-165 & 254-278.

[14] W. M. Kantor, *Isomorphisms of symplectic planes*, to appear in European J. Combin. .

[15] W. M. Kantor & M. E. Williams, *Symplectic semifield planes and $\mathbb{Z}_4$-linear codes*, to appear in Trans. Amer. Math. Soc. .

[16] G. Korchmáros, *Old and new results on ovals in finite projective planes*, in *Surveys in combinatorics*, (Guildford, 1991), Cambridge Univ. Press, 1991, 41-72.

[17] H. Lüneburg, *Translation planes*, Springer, Berlin, Heidelberg, New York, 1980.

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

[19] A. Maschietti, *Symplectic translation planes and line ovals*, Adv. Geom., 3(2003), 123-143.

[20] G. Panella, *Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito*, Boll. Un. Mat. Ital., 10(1955), 507-513.

[21] B. Segre, *Ovals in a finite projective plane*, Canad. J. Math., 7(1955), 414-416.

[22] B. Segre, *On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two*, Acta Arithm., 5(1959), 315-332.

[23] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann, Berlin, 1992.

[24] J. A. Thas, *Ovoidal translation planes*, Arch. Math., 23(1972), 110-112.

[25] J. A. Thas, *Construction of maximal arcs and dual ovals in translation planes*, European J. Combin., 1(1980), 189-192.

[26] J. Tits, *Ovoïdes et groupe de Suzuki*, Arch. Math., 13(1962), 187-198.