

Translation Planes of Odd Order via Dembowski-Ostrom Polynomials*

Ulrich Dempwolff, Peter Müller

Abstract

We describe a class of translation planes whose orders are of the form q^n , where n is odd and q is an odd prime power > 3 . These planes have the property that a translation complement fixes a triangle and acts transitively on the set of non-vertices of each side. The planes form an odd order analogue to the planes of Kantor-Williams [17] which have even order. The construction of the planes is based on a certain type of Dembowski-Ostrom polynomials.

1 Introduction

The main results of this note are summarized in the following theorem.

Theorem. *Let $q > 3$ be a power of the odd prime p , n an odd number, $0 < r < n$ a number coprime to n , and $0, \pm 1 \neq \alpha \in \text{GF}(q)$. Then one can associate with the quadruple (q, n, r, α) a translation plane \mathbf{A} of order q^n such that the following holds.*

- (a) *The kernel of \mathbf{A} has order q .*
- (b) *Let G be a translation complement. Then G contains normal subgroups \mathcal{G} , \mathcal{H} and Z , such that $|G : \mathcal{G}| \leq 2$, $\mathcal{G}/\mathcal{H} \simeq \text{Gal}(\text{GF}(q) : \text{GF}(p)[\alpha])$, $\mathcal{H}/Z \simeq C_n$, and $Z \simeq (C_{q^n-1} \times C_{q-1})$. Moreover $|G : \mathcal{G}| = 2$ iff there exists $\sigma \in \text{Aut}(\text{GF}(q))$ with $\alpha^\sigma = -\alpha$.*
- (c) *The group \mathcal{G} fixes a triangle $\{L_\infty, L_0, L_1\}$ (here L_∞ denotes the line at infinity, L_0, L_1 are affine lines). Let L^0 be any side of this triangle. Then \mathcal{G} induces a transitive group on the set of non-vertices of L^0 .*
- (d) *The plane \mathbf{A} is not a generalized André plane, nor a nearfield or a generalized twisted field plane, and not a plane of Suetake [22].*
- (e) *For q and n fixed there exist precisely $\varphi(n)M_q/2$ planes of this type. Here φ denotes the Euler function and M_q the number of orbits of $\text{Aut}(\text{GF}(q))$ on $\text{GF}(q) - \{0, \pm 1\}$.*

*2000 Mathematics Subject Classification: Primary 51E15, Secondary 05E20

Translation planes having a subgroup in the translation complement which fixes a triangle and acts transitively on the non-vertices of each side of the triangle have been studied several times before. In [12] they are called *triangle transitive* and in [17] nearly *flag-transitive*. Chapter 70 of [2] gives a survey of the known planes with this property.

According to (d) of the theorem the planes of this result are not among the planes previously described. With respect to the automorphism group and its action these planes are an analogue of the planes of Kantor-Williams [17]. It is clear that the construction of the Kantor-Williams planes can not be easily transformed into the case of odd characteristic. Indeed our construction is completely different: we use a certain type of Dembowski-Ostrom polynomial (see the next section for the definition) as a basis for the existence of our planes.

In the next section we introduce some notation and recall some basic facts about translation planes and linear groups. In section 3 we construct our planes and verify some elementary properties. Section 4 is concerned with isomorphisms and automorphisms. This includes the computation of the automorphism groups, the solution of the equivalence problem between two planes of our class and we count numbers of such planes. In the last section we exhibit connections of our class of translation planes with generalized twisted fields and with the flag transitive planes of Kantor [14] and Suetake [21].

2 Notation

For the remainder of this note q will be a power of the odd prime p and n will be a positive odd integer. We set

$$K = \text{GF}(q), \quad F = \text{GF}(q^n), \quad \text{with prime field } K_0 = \text{GF}(p),$$

and $no : F \rightarrow K$ will be the norm. By V we denote an n -dimensional K -space.

(2.1) Spreads and translation planes. We assume that the reader is familiar with the basics of finite translation planes (see [2], [5], [19] or [11]). However for convenience we recall the description of translation planes by spreads and quasifields. Let $W = V \times V$. A *spread* \mathcal{S} in W is a set of n -dimensional K -spaces such that

$$W = \bigcup_{X \in \mathcal{S}} X, \quad X \cap Y = 0, \text{ for } X, Y \in \mathcal{S}, X \neq Y.$$

Then $|\mathcal{S}| = q^n + 1$. The corresponding affine plane $\mathbf{A} = \mathbf{A}(\mathcal{S})$ has as points the vectors of W and as lines the cosets of the fibers of \mathcal{S} . Sometimes it is convenient to consider such a plane as a projective plane, i.e. as the *projective extension*. The points of the extension are the elements of W together with symbols (X) , $X \in \mathcal{S}$ and the lines are the *line at infinity*

$$L_\infty = \{(X) \mid X \in \mathcal{S}\}$$

and lines of the form $(X + w) \cup \{(X)\}$, $X \in \mathcal{S}$, $w \in W$ (i.e. $X + w$ is the "affine part" of this line).

Spread sets. Concrete coordinatizations of spreads lead to spread sets. A set $0 \in \Sigma \subseteq \text{GL}(V) \cup 0$ is called a *spread set* iff $\det(T - T') \neq 0$ for $T, T' \in \Sigma$, $T \neq T'$ and $|\Sigma| = q^n$. Then

$$\mathcal{S} = \mathcal{S}(\Sigma) = \{V(\infty)\} \cup \{V(T) \mid T \in \Sigma\}$$

is a spread where

$$V(\infty) = 0 \times V \quad \text{and} \quad V(T) = \{(v, vT) \mid v \in V\}.$$

Vice versa: using a suitable basis of W any spread can be described by a spread set.

Suppose that two spreads defined by Σ and Σ' share the fibers $V(0)$ and $V(\infty)$ and let D be a semilinear transformation mapping the first spread onto the second. If D fixes both $V(0)$ and $V(\infty)$ we write $D = \text{diag}(A, B)$ where $A = D_{V(0)}$, $B = D_{V(\infty)}$, and both fibers are identified in an obvious way with V . A fiber represented by $X \in \Sigma$ is then mapped to the fiber of the second spread represented by $A^{-1}XB$. If D interchanges $V(0)$ and $V(\infty)$ we write

$$D = \begin{pmatrix} \mathbf{0} & B \\ A & \mathbf{0} \end{pmatrix}.$$

Since $(v, vX)D = (w, wA^{-1}X^{-1}B)$, $w = vA$, a fiber represented by X is then mapped to the fiber represented by $A^{-1}X^{-1}B$.

Translation complements. Denote by $\Gamma\text{L}(W)$ the group of invertible semilinear operators on W . Then

$$G = \{T \in \Gamma\text{L}(W) \mid ST = \mathcal{S}\}$$

is called the *translation complement* of \mathbf{A} . It induces in the obvious way a group of collineations and the full automorphism group of \mathbf{A} is the semidirect product of W (identified with the group of translations) with G . In particular the automorphism group is determined completely by the translation complement. We also define the *linear translation complement* as

$$H = \{T \in G \mid T \in \text{GL}_{\mathcal{K}}(W)\}$$

where \mathcal{K} is the kernel of the plane. Clearly, $H \trianglelefteq G$.

Quasifields. A *quasifield* is an abelian group $(Q, +)$ together with a multiplication $Q \times Q \ni (x, y) \mapsto x \cdot y \in Q$ such that $Q - \{0\}$ is a loop and the distributive law $(x + y) \cdot z = x \cdot z + y \cdot z$ holds. If Q does not have a neutral element with respect to the multiplication we speak of a *weak quasifield*. Let Σ be a spread set as before and $\psi : V \rightarrow \Sigma$ a bijection with $\psi(0) = 0$. Define

$$x \cdot y = x\psi(y).$$

Then this multiplication turns V into a weak quasifield. Conversely every weak quasifield multiplication on V can be associated with a spread set.

(2.2) Oyama's description of linear spaces and transformations. It will be convenient to use a description of vector spaces and linear operators due to Oyama [20]. We identify an n -dimensional K -space V with F and denote vectors by (x) , $x \in F$. For $a \in F$ and $0 \leq k < n$ we define a K -linear mapping $T_k(a)$ by

$$(x)T_k(a) = (ax^{q^k}).$$

The basic multiplication rule for such maps is

$$T_k(a)T_\ell(b) = T_{k+\ell}(a^q b)$$

where $k + \ell$ is read modulo n . A K -endomorphism T of V has a unique representation

$$T = \sum_{i=0}^{n-1} T_i(a_i), \quad a_i \in F.$$

Let γ be an automorphism of F and $T \in \text{End}_K(V)$. Denote by $[\gamma, T]$ the operator on V defined by

$$[\gamma, T] : (v) \mapsto (v^\gamma)T.$$

Then $[\gamma, T]$ is a semilinear operator, i.e. semilinear with respect to the automorphism γ_K . There is some ambiguity in this representation: γ and $\gamma\tau$ induce the same automorphism on K for $\tau \in \text{Gal}(F : K)$. In fact the K -linear map $(v) \mapsto (v^q)$ is the same as $T_1(1)$. We remove this ambiguity by requiring $\gamma \in \Gamma$ where

$$\Gamma \text{ is a set of coset representatives of } \text{Gal}(F : K_0)/\text{Gal}(F : K).$$

Note that the latter group is isomorphic to $\text{Gal}(K : K_0)$. Using this convention the description of semilinear operators is now unique.

Singer cycles. Cyclic groups which act regularly on the non-trivial vectors of V are called *Singer cycles*. In the Oyama representation they can be written in a simple form: let $F^* = \langle \omega \rangle$ then

$$\mathcal{C} = \langle T_0(\omega) \rangle$$

is a Singer cycle. The normalizers of \mathcal{C} in $\text{GL}(V)$ and $\Gamma\text{L}(V)$ are well known (for instance [10], (II.7.3)):

$$\mathcal{N}_0 = N_{\text{GL}(V)}(\mathcal{C}) = \mathcal{C}\langle T_1(1) \rangle, \quad \mathcal{N} = N_{\Gamma\text{L}(V)}(\mathcal{C}) = \mathcal{N}_0\{[\gamma, \mathbf{1}] \mid \gamma \in \Gamma\}.$$

Moreover:

- (1) Any Singer cycle in $\text{GL}(V)$ is conjugate to \mathcal{C} .

- (2) If $T \in \text{GL}(V)$ is irreducible then it is contained in a unique Singer cycle which is also the centralizer of T in $\text{GL}(V)$.

(2.3) Dembowski-Ostrom Polynomials. A polynomial $P \in F[X]$ will be called a *Dembowski-Ostrom polynomial* or short *DO polynomial* if it has the form

$$P = \sum_{i,j=0}^{n-1} a_{ij} X^{q^i+q^j}.$$

DO polynomials were introduced in [6] for the construction of planar functions. But see also [3], [4], [1] for other applications. We will be interested only in DO polynomials of the form

$$P = a_0 X^2 + a_1 X^{q+1} + \dots + a_{n-1} X^{q^{n-1}+1}.$$

In this case $P(X) = L(X)X$ where

$$L = a_0 X + a_1 X^q + \dots + a_{n-1} X^{q^{n-1}}$$

is called the *linearized polynomial polynomial* of P .

3 Nearly flag-transitive translation planes and DO polynomials

Examples of nearly flag-transitive translation planes are nearfield planes, some generalized twisted field planes, some generalized André planes, the planes of Suetake in odd characteristic and the planes of Kantor and Williams in even characteristic. By any measure the Kantor-Williams construction produces the majority of such planes. They have an order of the form q^n where q is a 2-power and n is odd. Kantor and Williams show that with $n \rightarrow \infty$ the number of such planes grows rapidly if n is a highly decomposed number.

Let q (in contrast to our general assumption) be for the moment an even prime power. A plane of Kantor and Williams of order q^n has the following properties:

- (KW1) The translation complement contains a group $Z_1 \simeq C_{q^{n-1}}$ which acts fixed point freely on W and which fixes precisely two fibers of \mathcal{S} , say X and Y . The representation of Z_1 on X is contragredient to the representation of Z_1 on Y .
- (KW2) The plane admits a homology group $Z_0 \simeq K^*$ with coaxis X and axis Y . More precisely: let $a \in K^*$ then the map defined by $y \mapsto ay$ for $y \in Y$ and $x \mapsto ax$ for $x \in X$ lies in the translation complement.

Of course the fixed triangle is the line at infinity and the two other lines are represented by the fibers X and Y and $Z = Z_0 \times Z_1$ acts transitively on the set on non-vertices of each side. Our aim is to

construct planes of order q^n satisfying (KW1-2) for *odd* q .

The group $\{T_0(\lambda) \mid \lambda \in F^*\}$ is a Singer cycle on V . Taking $X = V(0)$ and $Y = V(\infty)$ as the fixed fibers we can identify the group Z_1 with

$$Z_1 = \{T(\lambda) = \text{diag}(T_0(\lambda^{-1}), T_0(\lambda)) \mid \lambda \in F^*\}. \quad (1)$$

The homology group is represented as

$$Z_0 = \{D(\varepsilon) = \text{diag}(\varepsilon \mathbf{1}, \mathbf{1}) \mid \varepsilon \in K^*\}. \quad (2)$$

For the remainder of this note ζ will denote a fixed non-square in K .

(3.1) Lemma. *A plane satisfying (KW1-2) is associated with a spread set*

$$\Sigma = \{M(y) \mid y \in F\}$$

where

$$M(y) = \sum_{i=0}^{n-1} T_i(a_i y^{(q^i+1)/2})$$

if y is a square and if y is a non-square one has

$$M(y) = \sum_{i=0}^{n-1} T_i(a_i \zeta^{(1-q^i)/2} y^{(q^i+1)/2}).$$

Conversely, a spread set of the above form defines a plane which satisfies (KW1-2).

Notation. For a sequence $\underline{a} = (a_0, \dots, a_{n-1}) \in F^n$ define a set Σ as in the lemma. We say that Σ is *defined by the sequence* \underline{a} .

Proof. Let Σ be the spread set associated with the plane and $\mathbf{0} \neq T = \sum_{i=0}^{n-1} T_i(a_i)$ be in Σ . Then

$$V(T)D(\zeta) = V(\zeta^{-1}T), \quad V(T)T(\lambda) = V(T_0(\lambda)TT_0(\lambda)).$$

As

$$T_0(\lambda)TT_0(\lambda) = T_0(a_0\lambda^2) + T_1(a_1\lambda^{q+1}) + \dots + T_{n-1}(a_{n-1}\lambda^{q^{n-1}+1})$$

this shows $\Sigma = \{T_0(\lambda)TT_0(\lambda), \zeta T_0(\lambda)TT_0(\lambda) \mid \lambda \in F\}$. Changing the notation somewhat we obtain the spread set in the form as stated in the assertion of the lemma. Of course our argument can be reversed so that the second assertion is

true. □

Question. Are there choices for the sequence \underline{a} which produce spread sets, i.e. guarantee $T - T' \in \text{GL}(V)$ for $T, T' \in \Sigma$, $T' \neq T$?

Define a multiplication on F by $x * y = z$ if $(x)M(y) = (z)$. The multiplication has the form:

$$x * y = \begin{cases} \sum_{i \geq 0} a_i x^{q^i} y^{(q^i+1)/2}, & y \in F^2, \\ \sum_{i \geq 0} a_i \zeta^{(1-q^i)/2} x^{q^i} y^{(q^i+1)/2}, & y \notin F^2. \end{cases} \quad (3)$$

So a reformulation of our question asks as to whether or not this multiplication is the multiplication of a weak quasifield.

(3.2) Lemma. For a sequence $\underline{a} = (a_0, \dots, a_{n-1}) \in F^n$ define a multiplication by (3) and a DO polynomial by $P = a_0 X^2 + a_1 X^{q+1} + \dots + a_{n-1} X^{q^{n-1}+1}$ whose linearized polynomial shall be denoted by L . Then the multiplication is a multiplication of a weak quasifield if:

(1) The K -linear map $F \ni x \mapsto L(x) \in F$ is bijective.

(2) $|P(F^*)| = \frac{q^n - 1}{2}$.

(3) $P(F^*) \cap \zeta P(F^*) = \emptyset$.

Proof. We have to show that for $x \neq 0$ the map $y \mapsto x * y$ is bijective and that for $y \neq 0$ the map $x \mapsto x * y$ is bijective.

First we note: If $y = \zeta s^2$ then $x * y = \zeta(x * s^2)$. Moreover $x(x * s^2) = P(xs)$ and $x(x * y) = \zeta P(xs)$.

Assume first $x * y = x_1 * y$ for some $y \neq 0$. Since the multiplication is left distributive we have $(x - x_1) * y = 0$. Thus it is enough to show $x = 0$ if $x * y = 0$.

Assume $x \neq 0$. If $y = w^2$ is a square we have $0 = \sum_{i=0}^{n-1} a_i x^{q^i} w^{q^i+1}$. Dividing by w we obtain $L(xw) = 0$, a contradiction because of (1). In the case $y = \zeta w^2$ we obtain $\zeta L(xw) = 0$, again a contradiction. Hence $x \mapsto x * y$ is bijective.

Assume now $y \mapsto x * y$ is not bijective for some $x \neq 0$. Hence $x * y = x * y_1$ for two y, y_1 . Clearly, we may assume $y \neq 0 \neq y_1$. Suppose first $y, y_1 \in (F^*)^2$, say $y = s^2, y_1 = s_1^2$. Then $P(xs) = x(x * y) = x(x * y_1) = P(xs_1)$. From (2) we deduce $s_1 = \pm s$ (note $P(z) = P(-z)$). Hence $y = y_1$. If $y = \zeta s^2, y_1 = \zeta s_1^2$ we get similarly $\zeta P(xs) = \zeta P(xs_1)$ and again $y = y_1$. Finally assume $y = s^2, y_1 = \zeta s_1^2$. Then $x(x * y) = x * (x * y_1)$ implies $P(xs) = \zeta P(xs_1)$, which contradicts (3). □

Define for $0 \leq i < j \leq n$ by π_{ij} the projection of the space $\text{End}_K(V)$ in the Oyama representation into $F \times F$ by

$$\text{End}_K(V) \ni T_0(a_0) + T_1(a_1) + \dots + T_{n-1}(a_{n-1}) \mapsto (a_i, a_j) \in F \times F. \quad (4)$$

(3.3) Lemma. Let Σ be defined by the sequence \underline{a} .

(a) Set $W = \langle \pi_{ij}(\Sigma) \rangle_K$ for $i, j \in \{0, \dots, n-1\}$, $i \neq j$. Then $\dim W \leq n$ iff one of the following assertions holds:

- (1) a_i or $a_j = 0$.
- (2) $j = n - i$.

(b) If Σ is additively closed then at most two entries of the sequence \underline{a} are nontrivial.

Proof. (a) Clearly the assertion is true if (1) holds. Moreover $(x^{q^i+1})^{q^{n-i}} = x^{1+q^{n-i}}$ which shows that (2) also implies $\dim W \leq n$.

Assume now $a_i \neq 0 \neq a_j$, $\dim W \leq n$. Then there exists a K -linear map $\ell : F \rightarrow F$ such that $W = \{(x, \ell(x)) \mid x \in F\}$. The general form of such a function is $\ell(x) = \sum_{k=0}^{n-1} b_k x^{q^k}$. Inspecting Σ we obtain for $\lambda \in F$ that

$$a_j \lambda^{1+q^j} = \ell(a_i \lambda^{1+q^i}) = \sum_{k=0}^{n-1} b_k a_i^{q^k} \lambda^{q^k+q^{i+k}}.$$

Define the polynomial Q by

$$Q(X) = \sum_{k=0}^{n-i-1} b_k a_i^{q^k} X^{q^{i+k}+q^k} + \sum_{k=n-i}^{n-1} b_k a_i^{q^k} X^{q^{i+k-n}+q^k} - a_j X^{1+q^j}.$$

Then $\deg Q \leq 2q^{n-1}$. But all λ 's in F are a zero of Q , so $Q = 0$ follows. This implies $j = n - i$ (as $i \neq j$) and assertion (2) follows.

(b) Clearly, $k\Sigma \subseteq \Sigma$ for $k \in K$. So if Σ is additively closed it is already a K -space. We deduce from (a) that at most two entries of the sequence \underline{a} are nontrivial. \square

We also use:

(3.4) Lemma. *Let K be a field not of characteristic 2 and A be a K -linear operator such that $A^n = a\mathbf{1}$, n odd, and $a \neq 0, \pm 1$. Then the following holds:*

- (a) *The operator $\mathbf{1} - A$ is invertible and $(\mathbf{1} - A)^{-1} = \frac{1}{1-a}(\mathbf{1} + A + A^2 + \dots + A^{n-1})$.*
- (b) *Set $L = 2(\mathbf{1} - A)^{-1} - \mathbf{1}$. Then L is invertible and $L^{-1} = 2(\mathbf{1} + A)^{-1} - \mathbf{1}$.*

Proof. The first assertion follows by the usual telescoping argument. As $(-A)^n = -a\mathbf{1}$ we see that $\mathbf{1} + A$ is invertible too with $(\mathbf{1} + A)^{-1} = \frac{1}{1+a}(\mathbf{1} - A + A^2 - A^3 + \dots - A^{n-2} + A^{n-1})$. Now

$$(2(\mathbf{1} - A)^{-1} - \mathbf{1})(2(\mathbf{1} + A)^{-1} - \mathbf{1}) = \mathbf{1} + R$$

with

$$R = 4(\mathbf{1} - A)^{-1}(\mathbf{1} + A)^{-1} - 2((\mathbf{1} - A)^{-1} + (\mathbf{1} + A)^{-1}).$$

Multiplying R with $(\mathbf{1} - A)(\mathbf{1} + A)$ we observe $R = \mathbf{0}$ and therefore $(2(\mathbf{1} - A)^{-1} - \mathbf{1})^{-1} = 2(\mathbf{1} + A)^{-1} - \mathbf{1}$. \square

The next result guarantees the existence of the desired quasifields.

(3.5) Proposition. *Let $0 < r < n$ be a number and a be an element in F^* such that its norm with respect to the subfield of order $q^{(n,r)}$ is not ± 1 . Define the linear polynomials A, B by $A(X) = X - aX^{q^r}$ and B as the unique polynomial of degree $\leq q^{n-1}$ such that $x \mapsto B(x)$ is the inverse of the mapping $F \ni x \mapsto A(x) \in F$. Finally define $L(X) = 2B(X) - X$ and the DO polynomial P by $P(X) = XL(X)$. Then P satisfies the assumptions of Lemma (3.2).*

Proof. It is enough to assume $(n, r) = 1$ (otherwise the subfield of order $q^{(n,r)}$ takes the role of K). The n -th power of the mapping $x \mapsto ax^{q^r}$ is the multiplication $x \mapsto no(a)x$. Therefore the mapping $x \mapsto A(x)$ is invertible by (3.4). Assertion (1) of (3.2) follows now from (3.4.b).

The polynomial $C(X) = X - a^2X^{q^r}$ defines by (3.4) an invertible operator too. Since $P(X) = 2B(X)X - X^2$ we have for $x \in F$ the equation:

$$\begin{aligned} P(A(x)) &= 2B(A(x))A(x) - A(x)^2 = A(x)(2x - A(x)) \\ &= (x - ax^{q^r})(2x - x + ax^{q^r}) \\ &= x^2 - a^2(x^2)^{q^r} = C(x^2) \end{aligned}$$

This implies $|P(F^*)| = (q^n - 1)/2$ and (2) of (3.2) holds.

Assume that (3) of (3.2) does not hold. Then there exist $u, v \in F$, $u \neq v$, such that $\zeta P(u) = P(v)$. Write $u = A(x)$ and $v = A(y)$. Then

$$\zeta(x^2 - a^2(x^2)^{q^r}) = \zeta C(x^2) = C(y^2) = y^2 - a^2(y^2)^{q^r}.$$

This implies $\zeta x^2 - y^2 = a^2(\zeta x^2 - y^2)^{q^r}$ and hence

$$a^2 = (\zeta x^2 - y^2)^{1-q^r}.$$

Therefore $no(a^2) = no(a)^2 = 1$ contradicting our assumptions. \square

Remark. Take $a \in F$ such that $no(a) \neq 0, \pm 1$ and let r be a number coprime to n . Define L as in (3.5). Using (3.4) we see that the linear map $x \mapsto L(x)$ has the form

$$L = \frac{2}{1 - no(a)} \sum_{i=0}^{n-1} T_r(a)^i - \mathbf{1} = \frac{1 + no(a)}{1 - no(a)} \mathbf{1} + \frac{2}{1 - no(a)} \sum_{i=1}^{n-1} T_r(a)^i.$$

Since $T_r(a)^j = T_{jr}(a^{1+q^r+\dots+q^{(j-1)r}})$ we can write L in the form

$$L = \sum_{i=0}^{n-1} T_{ir}(a_{ir})$$

with

$$a_0 = \frac{1 + no(a)}{1 - no(a)} \text{ and } a_{jr} = \frac{2}{1 - no(a)} a^{1+q^r+\dots+q^{(j-1)r}} \text{ for } j > 0. \quad (5)$$

The sequence $\underline{a} = (a_0, \dots, a_{n-1})$ then defines by (3.1), (3.2) and (3.5) a plane which satisfies (KW1-2).

Definition. Let q be an odd prime power, n be an odd number. For $0 < r < n$ a number coprime to n and $a \in F = \text{GF}(q^n)$ an element such that the norm with respect to $K = \text{GF}(q)$ is not $0, \pm 1$ let \underline{a} be the sequence defined as under (5). The multiplication (3) is then a quasifield multiplication. We call this multiplication of *type* (a, r) . Similarly we call the associated spread set (see (3.1)) and the associated plane also of *type* (a, r) . For the spread set we use the symbol

$$\Sigma_{a,r}.$$

Remark. It is not necessary to choose r coprime to n . But if $(n, r) = e > 1$ we set $K' = \text{GF}(q^e)$, $q' = qe$, and $n = n/e$. Considering $V = F$ as a K' -space and replacing in our construction the pair (n, q) by (n', q') we obtain the same spread set. So by assuming $(n, r) = 1$ we do not loose any spread sets.

4 Isomorphisms and automorphisms

In this section $q > 3$ will denote a power of an odd prime p and $1 < n$ will be an odd number. We will determine the translation complement of planes of type (r, a) and study possible isomorphisms between members of this class and show that these planes are not isomorphic to planes of other classes which share similar properties (nearly flag transitive).

(4.1) Lemma. *Let $\Sigma = \Sigma_{a,r}$ be a spread set of type (a, r) . Then the following holds:*

- (a) *Set $\Sigma^{-1} = \{S^{-1} \mid S \in \Sigma - 0\} \cup 0$. Then $\Sigma^{-1} = \Sigma_{-a,r}$.*
- (b) *Let b be an element in F^* such that $a \equiv b \pmod{(F^*)^{q-1}}$. Then $\Sigma_{a,r}$ is equivalent to $\Sigma_{b,r}$.*

Proof. Assertion (a) follows from (3.4.b) and the definition of spread sets of type (a, r) .

Assume now $a = be$ with $e \in (F^*)^{q-1}$. Choose $x \in F$ such that $x^{q^r-1} = e^{-1}$. Then

$$T_0(x) \left(\sum_{i=0}^{n-1} T_i(a_i) \right) T_0(x)^{-1} = \sum_{i=0}^{n-1} T_i(a_i x^{q^i-1})$$

where the sequence $\underline{a} = (a_0, \dots, a_{n-1})$ is associated with the type (a, r) . Let $\underline{b} = (b_0, \dots, b_{n-1})$ be the sequence associated with (b, r) . Clearly $no(a) = no(b)$.

Hence $a_0x^{q^0-1} = a_0 = b_0$. Moreover for $i > 0$ we have

$$\begin{aligned}
a_{ir}x^{q^{ir}-1} &= \frac{2}{1-no(a)}a^{1+q^r+\dots+q^{(i-1)r}}x^{q^{ir}-1} \\
&= \frac{2}{1-no(a)}(ax^{q^r-1}) \cdot (ax^{q^r-1})^{q^r} \dots (ax^{q^r-1})^{q^{(i-1)r}} \\
&= \frac{2}{1-no(b)}b^{1+q^r+\dots+q^{(i-1)r}} \\
&= b_{ir}.
\end{aligned}$$

Since $T_0(x)$ commutes with all $T_0(y)$'s we deduce from the construction of the spread sets that $T_0(x)\Sigma_{a,r}T_0(x)^{-1} = \Sigma_{b,r}$. \square

(4.2) Some automorphisms. We collect some "obvious" automorphisms of a plane of type (a, r) . The group Z (see (1-2)) is already present via the construction of the plane. In particular the plane is nearly flag transitive. Set

$$\mathcal{A}_a = \{\sigma \in \text{Aut}(F) \mid a^\sigma \equiv a \pmod{(F^*)^{q-1}}\}.$$

As the norm map defines a $\text{Aut}(F)$ -epimorphism from $F^*/(F^*)^{q-1}$ onto K^* and as $\text{Gal}(F : K) = \{\sigma \in \text{Aut}(F) \mid \gamma_K = 1_K\}$ one has

$$\mathcal{A}_a/\text{Gal}(F : K) \simeq \text{Gal}(K : K_0[no(a)]).$$

Let $\underline{a} = (a_0, \dots, a_{n-1})$ be the sequence associated with the pair (a, r) . Pick $\sigma \in \mathcal{A}_a$ and write it as $\sigma = \gamma\tau$ with $\gamma \in \Gamma$ and $x^\tau = x^{q^k}$. By the proof of (4.1) there exists some $x \in F$ such that

$$T_0(x)\left(\sum_i T_i(a_i)\right)T_0(x)^{-1} = \sum_i T_i(a_i^\sigma) = [\gamma, T_k(1)]^{-1}\left(\sum_i T_i(a_i)\right)[\gamma, T_k(1)].$$

This shows that $\text{diag}([\gamma, T_k(x)], [\gamma, T_k(x)])$ is an automorphism. Denote such an element by μ_σ and observe that the $|\sigma|$ -th power of μ_σ is a kern homology. We set

$$\mathcal{G} = Z\{\mu_\sigma \mid \sigma \in \mathcal{A}_a\}$$

and denote by \mathcal{H} the intersection of \mathcal{G} with the linear translation complement. Then (as $\text{Gal}(F : K) \subseteq \mathcal{A}_a$)

$$Z \simeq C_{q^n-1} \times C_{q-1}, \quad \mathcal{H}/Z \simeq C_n, \quad \mathcal{G}/\mathcal{H} \simeq \text{Gal}(K : K_0[no(a)]),$$

as the quotient \mathcal{H}/Z is isomorphic to $\text{Gal}(F : K)$. Our aim is to show that \mathcal{G} is essentially a full translation complement.

The following lemma will be used several times. Similar ideas one can find in [17].

(4.3) Lemma. *Let \bar{p} be a p -primitive divisor of $q^n - 1$ and S be a Sylow \bar{p} -subgroup of Z . Let $P = \text{diag}(P_0, P_\infty)$ be a semilinear transformation which maps a spread defined by $\Sigma_{a,r}$ onto the spread defined by $\Sigma_{b,s}$ (in particular $P_0^{-1}\Sigma_{a,r}P_\infty = \Sigma_{b,s}$) and which normalizes S . Then $P_0 = [\gamma, T_k(x)]$ and $P_\infty = [\gamma', T_\ell(y)]$ for some $\gamma \in \Gamma$, $0 \leq k < n$, and $x, y \in F$. If P is linear then $P_0 = T_k(x)$ and $P_\infty = T_k(y)$.*

Proof. By definition of Z a generator of S has the form $\text{diag}(T_0(w)^{-1}, T_0(w))$ with $w \in F^*$ of \bar{p} -power order. Note that by Zsigmondy's theorem [23] such primes always exist. By assumption P_0 and P_∞ lie in the normalizer in $\Gamma\text{L}(V)$ of $\langle T_0(w) \rangle$ which is \mathcal{N} (see (2.2)). Hence there exist $\gamma, \gamma' \in \Gamma$, $0 \leq k, \ell < n$, and nontrivial elements $x, y \in F$ such that $P_0 = [\gamma, T_k(x)]$ and $P_\infty = [\gamma', T_\ell(y)]$. Since P is a semilinear operator with respect to K we deduce $\gamma = \gamma'$.

We claim $k = \ell$:

By (3.3) we have

$$\dim_K \pi_{1,n-1}(\Sigma_{a,r}) = \dim_K \pi_{1,n-1}(\Sigma_{b,s}) = n.$$

Form the equation

$$[\gamma, T_k(x)]^{-1} \left(\sum_i T_i(b_i) \right) [\gamma, T_\ell(y)] = \sum_i T_{i+\ell-k} (x^{-q^{i+\ell-k}} y (b_i^\gamma)^{q^\ell})$$

we deduce that there exist constants $c_1, c_2 \in F$ such that

$$\begin{aligned} n &= \dim_K \pi_{1,n-1}([\gamma, T_k(x)]^{-1} \Sigma_{a,r} [\gamma, T_\ell(y)]) \\ &= \dim_K \{(c_1(u^\gamma)^{q^\ell}, c_2(v^\gamma)^{q^\ell}) \mid (u, v) \in \pi_{k+1-\ell, n-1+k-\ell}(\Sigma_{a,r})\}. \end{aligned}$$

Hence $n = \dim_K \pi_{k+1-\ell, n-1+k-\ell}(\Sigma_{a,r})$ and by (3.3) we have $k+1-\ell \equiv 1-k+\ell \pmod{n}$. As n is odd we get $k = \ell$. \square

(4.4) Lemma. *Let \mathcal{K} be the kernel of a plane of type (a, r) . Then $\mathcal{K} \simeq K$.*

Proof. Clearly, $K\mathbf{1}_W \simeq K$ is a subfield of \mathcal{K} . Therefore $\mathcal{K} \simeq \text{GF}(q^m)$ for some $m \leq n$. The multiplicative group \mathcal{K}^* can be identified with the group of *kern homologies*, i.e. the homologies whose axes are the line at infinity and whose centers are the null vector in W .

Choose S as in (4.3). Then the restriction $S_{V(0)}$ ($S_{V(\infty)}$) of S to $V(0)$ ($V(\infty)$) normalizes $\mathcal{K}_{V(0)}$ ($\mathcal{K}_{V(\infty)}$). By conjugation S induces a group of automorphisms of \mathcal{K} which lie in $\text{Gal}(\mathcal{K} : K)$. Since $\bar{p} \geq n+1 > m$ these automorphisms are trivial, i.e. S centralizes \mathcal{K} .

For $\kappa \in \mathcal{K}^*$ the restrictions $\kappa_{V(0)}$ and $\kappa_{V(\infty)}$ lie in the centralizer of $S_{V(0)}$ and $S_{V(\infty)}$ respectively. By (2.2) these centralizers are \mathcal{C} , i.e. $\kappa = \text{diag}(T_0(x), T_0(y))$ for suitably chosen $x, y \in F$. For $\sum_i T_i(b_i) \in \Sigma_{a,r}$ we must have

$$\sum_i T_i(b_i) = T_0(x)^{-1} \left(\sum_i T_i(b_i) \right) T_0(y) = \sum_i T_i(x^{-q^i} b_i y).$$

Since $b_0 \neq 0$ we obtain $x = y$ and since $b_1 \neq 0$ we also get $x^{q-1} \in K$. Hence $\kappa \in K\mathbf{1}_W$ and we are done. \square

(4.5) Lemma. *Let $T = \text{diag}(T_0, T_\infty)$ be an element in the linear translation complement normalizing Z . Then $T \in \mathcal{H}$.*

Proof. We can apply (4.3) and write $T_0 = T_k(x)$ and $T_\infty = T_k(y)$. However the automorphism $x \mapsto x^{q^k}$ lies in \mathcal{A}_a . So adjusting T with an element from \mathcal{H} we may assume that T fixes the fiber $V(M(1))$ and that $k = 0$. Note that $T_0(x)^{-1}(\sum_i T_i(a_i))T_0(y) = \sum_i T_i(a_i(x^{-1})^{q^i}y)$. This implies (considering the first summand of $M(1)$) that $x = y$ and considering the second summand we see $1 = x^{1-q}$. We conclude that is a kern homology and lies therefore in \mathcal{H} . \square

(4.6) Lemma. *Let G be the translation complement and H the linear translation complement of a plane of type (a, r) . The following holds:*

- (a) *One has $\mathcal{H} = H_{(0)} = H_{(\infty)}$ and $G_{(0)} = G_{(\infty)} = G_{(0),(\infty)}$.*
- (b) *$G = G_{\{(0),(\infty)\}}$.*

Proof. (a) We first claim:

(1) Assume that $T \in G$ fixes the spaces $V(0)$ and $V(\infty)$ and that $T_{V(0)} \in \mathcal{G}_{V(0)}$ and $T_{V(\infty)} \in \mathcal{G}_{V(\infty)}$. Then $T \in \mathcal{G}$.

Adjusting T by an element from \mathcal{G} we may assume $T_{V(0)} = \mathbf{1}$. Then by (4.3) we can write $T_{V(\infty)} = T_0(x)$ with $x \in F^*$. For $\sum_i T_i(a_i) \in \Sigma_{a,r}$ we have $(\sum_i T_i(a_i))T_0(x) = \sum_i T_i(xa_i)$ which implies $x \in K$. But then $T \in Z \leq \mathcal{G}$. Next we claim:

(2) $H_{(0),(\infty)} = \mathcal{H}$:

Set $\overline{H} = H_{(0),(\infty)}$ and assume $\overline{H} > \mathcal{H}$. Then $\overline{H}_{V(0)} > \mathcal{H}_{V(0)}$ or $\overline{H}_{V(\infty)} > \mathcal{H}_{V(\infty)}$ by (1). By symmetry it is enough to assume $\overline{H}_{V(0)} > \mathcal{H}_{V(0)}$. By (4.5) we see that $\overline{H}_{V(0)}$ does not lie in the normalizer in $H_{V(0)}$ of $Z_{V(0)} = (Z_1)_{V(0)}$. The group Z induces a Singer cycle on $V(0)$. By [13] $\overline{H}_{V(0)} \simeq \text{GL}(m, q^k)$ with $n = km$ and $m > 1$. In particular \overline{H} would contain an element of t of order $p = \text{Char } K$ such that $\dim_K C_{V(0)}(t) = (m-1)k$. As t has order p we have $C_{V(\infty)}(t) \neq 0$. Hence t is planar. As a subplane $C_W(t)$ has order $\leq q^{n/2}$. But this is in conflict with $\dim_K C_{V(0)}(t) = (m-1)k$. Now (2) follows.

Assume next $H_{(\infty)} > \mathcal{H}$. Then $L_\infty - \{(\infty)\}$ is an $H_{(\infty)}$ -orbit and by (2) we deduce $|H_{(\infty)} : \mathcal{H}| = q^n$, $H_{(\infty)} = \mathcal{H}P$, and $\mathcal{H} \cap P = 1$ for $P \in \text{Syl}_p(H_{(\infty)})$. Assume that P acts trivially on $V(\infty)$. We claim that then P acts trivially on $V/V(\infty)$ too. P lies in the kernel of the action of $H_{(\infty)}$ on $V(\infty)$ (which is PZ_0). By a Frattini-argument we know that $N_{H_{(\infty)}}(P)$ contains a Sylow \bar{p} -subgroup,

say S . By elementary representation theory $0 \neq U = C_{V/V(\infty)}(P)$ (see [10], V, 5.16 for instance). If P would act nontrivially on $V/V(\infty)$ then U would be a nontrivial, proper S -invariant space, contradicting the irreducible action of S on $V/V(\infty)$. Hence the claim is true. Then P is a group of elations and our plane is a semifield plane, i.e. Σ is additively closed. That contradicts (3.3).

Hence $(H_{(\infty)})_{V(\infty)} > \mathcal{H}_{V(\infty)}$ and as above we deduce $(H_{(\infty)})_{V(\infty)} \simeq \text{GL}(m, q^k)$. Set $L = C_{H_{(\infty)}}(V(\infty))$. Then $(H_{(\infty)})_{V(\infty)} \simeq H_{(\infty)}/L$ and $C_G(V(\infty)) = Z_0 \leq L$. Assume $L > Z_0$. Then

$$1 \neq |L/Z_0| = |L/(\mathcal{H} \cap L)| = |L\mathcal{H}/\mathcal{H}|$$

and therefore $|L|_p > 1$. Consequently $|H_{(\infty)}/L|_p < q^n$, a contradiction. Thus $L = Z_0$ and $|H_{(\infty)}/L : \mathcal{H}/L| = |H_{(\infty)} : \mathcal{H}| = q^n$, i.e. $\text{GL}(m, q^k)$ has a subgroup of index q^n whose order is $(q^n - 1)(q - 1)n$, a contradiction. As $G_{(\infty)}$ normalizes $H_{(\infty)} = \mathcal{H}$ it must fix (0) too.

(b) By (a) we have either $H_{\{(0), (\infty)\}} = \mathcal{H}$ or $|H_{\{(0), (\infty)\}} : \mathcal{H}| = 2$ (and elements in $H_{\{(0), (\infty)\}} - \mathcal{H}$ interchange the points (0) and (∞)).

Assume $H > H_{\{(0), (\infty)\}}$ then H is transitive on L_∞ . Since \mathcal{H} is already transitive on the nontrivial vectors of the fibers $V(0)$ and $V(\infty)$ we see that H is transitive on the nontrivial vectors of W . These groups have been classified by Hering [8], [9], and Liebeck [18]. Since $\dim W = 2n$ and $q > 3$ one either has $H \leq \text{GL}(1, p^{2fn})$, $q = p^f$, or the socle of H is isomorphic to $\text{SL}(m, q^k)$, $km = 2n$; $\text{Sp}(2m, q^k)$, $km = n$. Here we also use that H must lie in $\text{GL}_K(W)$, since the kernel is isomorphic to $\text{GF}(q)$.

The first case is impossible: as $|H| \geq p^{2fn} - 1$ the group H contains a cyclic normal subgroup C of order $\geq (p^{2fn} - 1)/2fn$. Then

$$|Z_1 \cap C| \geq \frac{|Z_1||C|}{|\text{GL}(1, p^{2fn})|} \geq \frac{p^{fn} - 1}{(2fn)^2} > 2$$

as $p > 3$. Let $c \in H$ be an element whose order is a p -primitive prime divisor of $p^{2fn} - 1$. Then c has no fixed points on L_∞ and leaves the set $\{(0), (\infty)\}$ of fixed points of $Z_1 \cap C$ invariant. But $|c| \geq 2fn + 1$, a contradiction.

If $\text{SL}(m, q^k)$ is the socle of H the centralizer of a transvection in W has order $q^{(m-1)k} \leq q^n$. This shows $m = 2$ and it is well known that our plane is desarguesian. But a plane of type (a, r) is not even a semifield plane, a contradiction. The case that the socle of H is $\text{Sp}(2m, q^k)$ leads to the same contradiction. Thus $H = H_{\{(0), (\infty)\}}$. Since H is normal in G and $L_\infty - \{(0), (\infty)\}$ is an H -orbit we also get $G = G_{\{(0), (\infty)\}}$ \square

(4.7) Lemma. *Assume*

$$[\gamma, T_k(x)]^{-1} \Sigma_{a,r} [\gamma, T_k(y)] = \Sigma_{b,s}.$$

(a) *Then $r = s$ or $r = n - s$.*

(b) Assume $r = s$. Then $a^\sigma \equiv b \pmod{(F^*)^{q-1}}$, where $\sigma = \gamma \circ \tau$ and τ is defined by $x^\tau = x^{q^k}$.

Proof. (a) First we claim:

(1) There exist an $a' \in F^*$ such that

$$\Sigma_{a',r} = \Sigma_{b,s}.$$

Define $\hat{a} \in F^*$ by

$$[\gamma, T_k(1)]^{-1} \Sigma_{a,r} [\gamma, T_k(1)] = \Sigma_{\hat{a},r}.$$

Then we get

$$T_0(x)^{-1} \Sigma_{\hat{a},r} T_0(y) = \Sigma_{b,s}.$$

Choose $v \in K^*$ and $z \in F^*$ such that $yx^{-1} = z^2v^{-1}$. Then

$$\text{diag}(T_0(z), T_0(z^{-1}v)) \in Z$$

and

$$\text{diag}(T_0(x), T_0(y)) \text{diag}(T_0(z), T_0(z^{-1}v)) = \text{diag}(T_0(\alpha), T_0(\alpha))$$

with $\alpha = xz$ and

$$T_0(\alpha)^{-1} \Sigma_{\hat{a},r} T_0(\alpha) = \Sigma_{b,s}.$$

On the other hand we compute with $M(1) \in \Sigma_{\hat{a},r}$ that

$$\begin{aligned} T_0(\alpha)^{-1} M(1) T_0(\alpha) &= T_0(\alpha)^{-1} \left(\frac{2}{1 - \text{no}(a)} \sum_i T_r(\hat{a})^i - \mathbf{1} \right) T_0(\alpha) \\ &= \frac{2}{1 - \text{no}(a')} \sum_i T_r(a')^i - \mathbf{1} \end{aligned}$$

with

$$a' = \hat{a}\alpha^{1-q^r}.$$

(2) $r = s$ or $r = n - s$.

Set $A = T_r(a')$ and $B = T_s(b)$. Considering the the first summand in the representation of $M(1) \in \Sigma_{a',r}$ we see that there exist a $z \in K^*$ such that

$$2(\mathbf{1} - A)^{-1} - \mathbf{1} = z(2(\mathbf{1} - B)^{-1} - \mathbf{1}).$$

This shows that $(\mathbf{1} - A)^{-1}$ commutes with $z(\mathbf{1} - B)^{-1}$ and therefore even A and B commute. Multiply the above equation with $(\mathbf{1} - A)(\mathbf{1} - B)$. We obtain

$$\mathbf{1} - B + A - AB = z(\mathbf{1} - A + B - AB)$$

and therefore

$$(1 - z)\mathbf{1} - (1 + z)T_s(b) + (1 + z)T_r(a') - (1 - z)T_{r+s}((a')^{q^s}b) = \mathbf{0}.$$

This forces either $z = 1$, $r = s$, and $A = B$, or $z = -1$, $r = n - s$, and $A = B^{-1}$.

(b) Assume now $r = s$. Adjusting the given transformation by an element from Z we can assume

$$[\gamma, T_k(x)]^{-1} \left(\sum_i T_i(a_i) \right) [\gamma, T_k(y)] = \sum_i T_i(b_i)$$

where $\underline{a} = (a_0, \dots, a_{n-1})$ is the sequence associated to (a, r) and $\underline{b} = (b_0, \dots, b_{n-1})$ is the sequence associated to (b, r) . We compute the left hand site (note that $T_i(u)T_k(v) = T_{i+k}(u^r v)$) and obtain the equations (which will be used in the proof of (4.9) again)

$$\frac{1 + no(a)^\sigma}{1 - no(a)^\sigma} x^{-1} y = \frac{1 + no(b)}{1 - no(b)}, \quad (6)$$

and

$$\frac{2}{1 - no(a)^\sigma} (a^\sigma)^{1+q^r+\dots+q^{(i-1)r}} x^{-q^{ir}} y = \frac{2}{1 - no(b)} b^{1+q^r+\dots+q^{(i-1)r}}, \quad i > 0. \quad (7)$$

Eliminating y we remain with the equations

$$\frac{2}{1 - no(a)^\sigma} (a^\sigma)^{1+q^r+\dots+q^{(i-1)r}} x^{1-q^{ir}} z = \frac{2}{1 - no(b)} b^{1+q^r+\dots+q^{(i-1)r}}, \quad i > 0,$$

where $z = (1 + no(b))(1 - no(a)^\sigma)(1 + no(a)^\sigma)^{-1}(1 - no(b))^{-1}$. Dividing the equation for $i = 2$ by the equation for $i = 1$ we get

$$\frac{a^\sigma}{b} = x^{q^r-1} \quad (8)$$

which implies the claim. \square

Remark. Let $A = T_r(a)$. Then the proof of (4.7) shows $2(\mathbf{1} - A)^{-1} - \mathbf{1} = -(2(\mathbf{1} - A^{-1})^{-1} - \mathbf{1})$. Since $A^{-1} = T_{n-r}(a^{-q^{n-r}})$ a spread of type $(*, r)$ is at the same time of type $(*, n - r)$.

(4.8) Lemma. *Let G be the translation complement of a plane of type (a, r) . Then $G_{(\infty)} = \mathcal{G}$.*

Proof. As the group S (of (4.3)) is characteristic in \mathcal{H} we see from (4.6.b) that we can apply (4.3) to any T be in $G_{(\infty)}$. Hence T has the form

$$T = \text{diag}([\gamma, T_k(x)], [\gamma, T_k(y)]).$$

Apply (4.7.b) with $a = b$, i.e. $a^\sigma \equiv a \pmod{(F^*)^{q-1}}$ for $\sigma = \gamma\tau$ where $x^\tau = x^{q^k}$. Adjusting T with $\mu_{\sigma^{-1}}$ we obtain by (4.5) an element in \mathcal{H} and we are done. \square

(4.9) Lemma. *Let G be the translation complement of a plane of type (a, r) and H the linear translation complement.*

(a) Then $H = H_{(\infty)} = \mathcal{H}$ and $G_{(\infty)} = \mathcal{G}$.

(b) Either there exists an automorphism $\sigma \in \text{Aut}(K)$ with $no(a)^\sigma = -no(a)$ and $|G : G_{(\infty)}| = 2$ holds or $G = G_{(\infty)}$.

Proof. (a) follows from (4.6) and (4.8). Moreover either $G = G_{(\infty)}$ or $|G : G_{(\infty)}| = 2$ and each collineation in $G - G_{(\infty)}$ interchanges the fibers $V(0)$ and $V(\infty)$.

Assume $T \in G - G_{(\infty)}$. As we pointed out in (2.1) this shows that there exists a transformation $T = \text{diag}(T_1, T_2)$ which maps the spread associated with $\Sigma_{a,r}$ onto the spread associated with $\Sigma_{a,r}^{-1} = \Sigma_{-a,r}$ (see (4.1)). Because $\mathcal{H} = H_{(0),(\infty)}$ is a normal subgroup in $G = G_{\{(0),(\infty)\}}$ we can apply (4.3). This implies that T has the form

$$T = \text{diag}([\gamma, T_k(x)], [\gamma, T_k(y)]) \quad (9)$$

with suitable chosen $x, y \in F$, $0 \leq k < n$, and $\gamma \in \Gamma$. Set $\sigma = \gamma\tau$ where $x^\tau = x^{q^k}$. Adjusting T with an element from Z we can even assume

$$[\gamma, T_k(x)]^{-1} \left(\sum_i T_i(a_i) \right) [\gamma, T_k(y)] = \sum_i T_i(a_i^\sigma x^{-q^i} y) = \sum_i T_i(a'_i)$$

with

$$a_0 = \frac{1 + no(a)}{1 - no(a)}, \quad a_i = \frac{2}{1 - no(a)} a^{1+q^r+\dots+q^{(i-1)r}}, \quad i > 0$$

and the a'_i 's are obtained from the a_i 's by replacing a by $-a$. By the proof of (4.7.b) we get equations (6)-(8) where b is replaced by $-a$. In particular $-a^{\sigma^{-1}} = x^{q^r-1}$. This implies $no(a)^{\sigma^\kappa} = -no(a)$. In particular $\sigma_K \neq 1$. This shows $H = H_{(\infty)}$ in any case. Then (a) and one part of (b) is verified.

To complete the proof of (b) assume now that there exist $\sigma \in \text{Aut}(K)$ with $no(a)^\sigma = -no(a)$. By an abuse of the notation we denote by σ also an extension of σ to an automorphism of F . Then $a^\sigma = -ab$ with $no(b) = 1$. Hence there exists an $x \in F$ such that equation (8) holds (with $b = -a$). Then define y by equation (6) and T by equation (9). One checks that all equations (7) are true. It is clear that T maps $\Sigma_{a,r}$ onto $\Sigma_{-a,r}$ \square

(4.10) Lemma. For q and n fixed the following holds:

- (a) A plane of type (a, r) is isomorphic to a plane of type (b, r) iff $no(a)^\sigma = no(b)$ for some $\sigma \in \text{Aut}(K)$.
- (b) The number of pairwise nonisomorphic planes of type (a, r) is equal to the number of orbits of $\text{Aut}(K)$ on $K - \{0, \pm 1\}$.

Proof. Since (b) follows immediately from (a) it suffices to verify (a). Assume, that the pairs (a, r) and (b, r) define isomorphic planes. As usual we can apply (4.3): there exists $x, y \in F$ and a $\sigma \in \text{Aut}(F)$ such that assumptions of (4.7.b) are fulfilled. Hence $a^\sigma \equiv b \pmod{(F^*)^{q-1}}$. The norm map no induces a σ -isomorphism from $F^*/(F^*)^{q-1}$ onto K^* . Therefore $no(a)^\sigma = no(b)$.

Conversely, assume $no(a)^\sigma = no(b)$ for $\sigma \in \text{Aut}(K)$ and denote by σ also an extension of σ to F . Then $a^\sigma \equiv b \pmod{(F^*)^{q-1}}$. Clearly, $\Sigma_{a,r}$ and $\Sigma_{a^\sigma,r}$ are equivalent. The assumption follows from (4.1). \square

(4.11) Proof of the theorem. Let \mathbf{A} be an affine plane of order q^n and type (a, r) . The parameter α in the theorem stands for $no(a)$. Assertion (a) of the theorem follows from (4.4), (b) follows from (4.8) and (4.9), while (c) already follows from (4.2). Assertion (e) is a consequence of (4.10) and the remark following (4.7). It remains to show assertion (d).

From (3.3.b) we deduce that \mathbf{A} is not a generalized twisted field plane and it can not be a nearfield plane by the shape of its translation complement.

Suppose that \mathbf{A} is a plane of Suetake. Then the *linear* translation complement has an orbit of length 2 on L_∞ [22], Lemma 4.9, Theorem 4.13. However by (4.9) we know that an element in G which interchanges (0) and (∞) does not lie in H , a contradiction.

Assume finally that \mathbf{A} is a generalized André plane. The homology group with axis $V(\infty)$ and center (0) is according to (4.2) and (4.6.a) the group Z_0 . But by [19], Thm. 11.7 or [7] this homology group contains a subgroup of order $(q^n - 1)/u$ where $u = \text{lcm}\{q^i - 1 \mid 0 < i < n, i \mid n\}$. Hence a p -primitive prime divisor of $q^n - 1$ would divide $q - 1$. That is in conflict with Zsigmondy's theorem. \square

5 Connections with generalized twisted fields and flag transitive planes

In this section we show that our planes have close connections with generalized twisted field planes and certain flag transitive planes.

A map $f : F \rightarrow F$ is called planar if for $\beta \in F^*$ the mapping $\Delta_\beta : F \rightarrow F$ defined by

$$\Delta_\beta(x) = f(x + \beta) - f(x)$$

is bijective. In the case that f is a DO polynomial the multiplication $* : F \times F \rightarrow F$ defined by

$$x * y = f(x + y) - f(x) - f(y), \quad x, y \in F,$$

is the multiplication of a commutative presemifield (see [6] or [5], p. 245).

(5.1) Lemma. *Let P be a DO polynomial defined in (3.5).*

- (a) *Then P is planar.*
- (b) *The presemifield defined by the polynomial P is isotopic to a field.*

Proof. (a) The proof of (a) is a routine verification (note however the remark at the end of the verification of part (b)).

(b) Let L and A have the meaning of (3.5). The presemifield multiplication has the form $x * y = L(x)y + yL(x)$. Set $x = A(u)$ and $y = A(v)$ then a multiplication of an isotopic presemifield is defined by:

$$\begin{aligned} u \circ v &= L(A(u))A(v) + A(u)L(A(v)) \\ &= (u + au^{q^r})(v - av^{q^r}) + (v + av^{q^r})(u - au^{q^r}) \\ &= 2(uv - a^2(uv)^{q^r}) \end{aligned}$$

Since $u \circ v$ is the image of uv under the linear transformation $x \mapsto 2(x - a^2x^{q^r})$ we see that the multiplication \circ is isotopic to the field multiplication in F . Clearly, the arguments of this proof can be reversed so that one gets the assertion of part (a) too. \square

The next proposition shows a connection to generalized twisted fields.

(5.2) Proposition. *Let L be defined as in (3.5). Then $\Sigma_0 = \{T_0(x)L + LT_0(x) \mid x \in F\}$ is the spread set of a generalized twisted field plane.*

Proof. Let A be defined as in (3.5) and assume for the moment that Σ_0 is a spread set. An isotopic presemifield is defined by the spread set $\frac{1}{2}A\Sigma_0A$. As $A = T_0(1) - T_r(a)$ we see that a typical element of this spread set has the form

$$\frac{1}{2}A(T_0(x)L + LT_0(x))A = T_0(x) - T_{2r}(aa^{q^r}x^{q^r}).$$

The associated multiplication of the presemifield has the form

$$x * y = xy - aa^{q^r}x^{q^{2r}}y^{q^r}$$

which is the multiplication of a generalized twisted field (see [2], sec. 10.3). Since one can read the proof backwards the assumption that Σ_0 is a spread set is automatically fulfilled. \square

Notation. For the remainder of this section we assume

$$q = q_0^2,$$

i.e. q is an even power of the prime p . The involution $\tau \in \text{Aut}(F)$ (i.e. $x^\tau = x^{q_0^n}$) induces the involutory automorphism of K . We may assume $\tau \in \Gamma$ (see (2.2)). Also we denote by

$$F_0 = (F^*)^{q_0^n - 1}, \quad F_1 = \{x \in F \mid x^2 \in F_0\},$$

the subgroups of order $q_0^n + 1$ and $2(q_0^n + 1)$ in F^* .

(5.3) Lemma. *Let G be the translation complement of a translation plane associated with the parameters (a, r) .*

(a) Assume $no(a)^\tau = -no(a)$. Then there exists an element $a_1 \in a(F^*)^{q-1}$ such that $a_1^\tau = -a_1$.

(b) Assume G contains an involution which interchanges $V(0)$ and $V(\infty)$. Then we can assume $a^\tau = -a$ and we can choose the involution as the semilinear mapping

$$\iota : (x, y) \mapsto (y^\tau, x^\tau).$$

(c) The involution ι of (b) is planar. The fixed fibers have the form

$$V(T_0(x)LT_0(x)), \quad x \in F_1.$$

Proof. (a) By assumption there exists $u \in (F^*)^{q-1}$ such that $a^\tau = -au$. Hence $u^\tau = u^{-1}$. As $|(F^*)^{q-1}|$ is odd there exists a $v \in (F^*)^{q-1}$ such that $v^\tau = v^{-1}$ and $v^2 = u$. Set $a_1 = av$.

(b) Using once again (4.3) the involution is represented in the form (see (2.1))

$$\iota = \begin{pmatrix} \mathbf{0} & [\gamma, T_k(y)] \\ [\gamma, T_k(x)] & \mathbf{0} \end{pmatrix}.$$

Then $\iota^2 = \mathbf{1}$ implies $\gamma = \tau$, $xy^\tau = 1$, and $2k \equiv 0 \pmod{n}$. Thus $k = 0$ and from (4.9) we deduce $no(a)^\tau = -no(a)$. Using part (a) and (4.1.b) we (replace if necessary (a, r) by the equivalent pair (a_1, r)) may also assume $a^\tau = -a$. Since

$$[\tau, \mathbf{1}]L[\tau, \mathbf{1}] = L^{-1}$$

(see (3.4.b)) we see that the involution

$$\begin{pmatrix} \mathbf{0} & [\tau, \mathbf{1}] \\ [\tau, \mathbf{1}] & \mathbf{0} \end{pmatrix}$$

also lies in G and interchanges $V(0)$ and $V(\infty)$.

(c) We assume now that $(x, y)\iota = (y^\tau, x^\tau)$. Then

$$V(T_0(x)LT_0(x))\iota = V([\tau, \mathbf{1}](T_0(x)LT_0(x))^{-1}[\tau, \mathbf{1}]).$$

If $x \in F_1$ then $x^\tau = \epsilon x^{-1}$, $\epsilon = \pm 1$. Hence in this case

$$[\tau, \mathbf{1}](T_0(x)LT_0(x))^{-1}[\tau, \mathbf{1}] = \epsilon^2 T_0(x)LT_0(x) = T_0(x)LT_0(x).$$

Set

$$\Sigma_0 = \{T_0(x)LT_0(x) \mid x \in F_1\}.$$

Then

$$|\Sigma_0| = |F_1|/2 = |F_0| = q_0^n + 1.$$

Therefore ι is planar and Σ_0 is precisely the set of fibers being fixed by ι . \square

(5.4) Lemma. *The group $C_Z(\iota)$ acts transitively on Σ_0 , i.e. the fixed plane of ι is a flag transitive plane of order q_0^n .*

Proof. Set $\widehat{Z} = \{\text{diag}(T_0(x), T_0(y)) \mid x, y \in F^*\}$. Then $Z \leq \widehat{Z}$ and

$$C_{\widehat{Z}}(\iota) = \{\text{diag}(T_0(x), T_0(x^\tau)) \mid x \in F^*\}.$$

If $x \in F_0$ then $x^\tau = x^{-1}$ while $x^\tau = -x^{-1}$ if $x \in F_1 - F_0$. Set $\epsilon_x = 1$ for $x \in F_0$ and $= -1$ for $x \in F_1 - F_0$. Then

$$\text{diag}(T_0(x), T_0(x^\tau)) = \text{diag}(T_0(x), T_0(x^{-1}))\text{diag}(\mathbf{1}, T_0(\epsilon_x)) \in C_Z(\iota).$$

We conclude

$$\{\text{diag}(T_0(x), T_0(x^\tau)) \mid x \in F_1\} \leq C_Z(\iota)$$

and (3.3.c) shows the claim. \square

We call the flag transitive planes from [14], [21], and [2], Thm. 67.6, p. 506 of *Kantor-Suetake type*. We have:

(5.5) Proposition. *Let ι be a Baer involution as in (5.3). Then the fixed plane of ι is a flag transitive plane of Kantor-Suetake type.*

Proof. Let A and L have the meaning from (3.5). Clearly, $C_W(\iota) = \{(x, x^\tau) \mid x \in F\}$. If (x, x^τ) lies in $V(L)$ we conclude $x^\tau = 2A^{-1}(x) - x$. Define the linear map $g : F \rightarrow F$ by $g(x) = x - x^\tau + a(x + x^\tau)^{q^r}$. Then

$$U = C_{V(L)}(\iota) = \{(x, x^\tau) \mid x \in \ker g\}.$$

We identify F in an obvious way with $C_W(\iota)$ and U with $\ker g$. Then we deduce from (5.4) that $\mathcal{T} = \{Ux \mid x \in F_1\}$ is a spread in F so that the pair (F, \mathcal{T}) defines a flag transitive plane of order q_0^n . Obviously $\text{Im } g = \{x \in F \mid x^\tau = -x\}$. Thus $g(y) = 2y$ for $y \in \text{Im } g$ which in turn implies $U = \text{Im}(g - 2\mathbf{1})$ and hence

$$U = \{-y + ay^{q^r} \mid y \in \text{GF}(q_0^n)\}.$$

This leads precisely to the description of a plane of Kantor-Suetake type. \square

Final remarks. (a) Let q be of the form p^m where p is a prime. Using the Burnside formula one can express the number M_q of part (e) of the theorem by

$$M_q + 3 = \frac{1}{m} \sum_{d \mid m} \varphi(d)p^d.$$

(b) Kantor and Williams use in [15],[16], and [17], the relation between symplectic and orthogonal geometries in characteristic 2 in order to construct flag-transitive, semifield, and nearly flag-transitive translation planes. This relation between symplectic and orthogonal geometry does not exist in odd characteristic. Nevertheless one would suspect that in odd characteristic one should be

able to construct the analogues of the planes of Kantor and Williams by other methods. The present paper is a first step in this direction.

Acknowledgment. Section 5 was inspired by questions and suggestions of our colleague Bill Kantor.

References

- [1] A. Blokhuis, R. Coulter, M. Henderson, C. O’Keefe: Permutations amongst the Dembowski-Ostrom polynomials, in *Finite Fields and Applications*, Proc. 5-th Int. Conf. on Finite Fields and Appl., 2001, pp. 37-42.
- [2] M. Biliotti, V. Jha, N. Johnson: *Handbook of Finite Translation Planes*, CRC, 2007.
- [3] R. Coulter, R. Matthews: Planar functions and planes of Lenz-Barlotti class II, *Designs, Codes and Cryptography* 10(1997), 167–184.
- [4] R. Coulter, R. Matthews: Dembowski-Ostrom polynomials from Dickson polynomials, *Fin. Fields Appl.* 16(2010), 369-379.
- [5] P. Dembowski: *Finite Geometries*, Springer, 1968.
- [6] P. Dembowski, T. Ostrom: Planes of order n with collineation groups of order n^2 , *Math. Z.* 103(1968), 239-258.
- [7] D. Foulser: A generalization of André’s systems, *Math. Z.* 100(1967), 380-395.
- [8] C. Hering: Transitive linear groups and linear groups which contain irreducible subgroups of prime order I, *Geom. Ded.* 2(1974), 425-460.
- [9] C. Hering: Transitive linear groups and linear groups which contain irreducible subgroups of prime order II, *J. Algebra* 93(1985), 151-164.
- [10] B. Huppert: *Endliche Gruppen I*, Springer 1967.
- [11] D. Hughes, F. Piper: *Projective Planes*, Springer 1973.
- [12] V. Jha, N. Johnson: The planes of Suetake, *J. Geom.* 94(2009), 89-105.
- [13] W. Kantor: Linear Groups containing a Singer Cycle, *Jour. Alg.* 62(1980), 232–234.
- [14] W. Kantor: 2-transitive and flag transitive designs, in: *Coding theory, design theory, group theory (Burlington. VT, 1990)*, pp. 13-30, Wiley 1993.
- [15] W. Kantor, M. Williams: New flag-transitive affine planes of even order, *J. Combin. Theory Ser. A*, 74(1996), 1-13.

- [16] W. Kantor, M. Williams: Symplectic semifield planes and \mathbf{Z}_4 -linear codes, Trans. Amer. Math. Soc. 356(2004), 895-938.
- [17] W. Kantor, M. Williams: Nearly flag-transitive affine planes, Advances in Geometry, 10(2010), 161-183.
- [18] M. Liebeck: The affine permutation groups of rank three, Proc. Lond. Math. Soc. (3)54(1987), 477-516.
- [19] H. Lüneburg: *Translation Planes*, Springer 1980.
- [20] T. Oyama: On quasifields, Osaka J. Math., 22(1985), 35-54.
- [21] C. Suetake: Flag transitive planes of order q^n with a long cycle ℓ_∞ as a collineation, Graphs Combin. 7(1991), 183-195.
- [22] C. Suetake: A family of translation planes of order q^{2m+1} with two orbits of length 2 and $q^{2m+1} - 1$ on ℓ_∞ , Geom. Dedicata, 42(1992), 773-786.
- [23] K. Zsigmondy: Zur Theorie der Potenzreste, Monatshefte Math. Phys. 3(1892), 163-185.

Ulrich Dempwolff
 FB Mathematik, Universität
 67653 Kaiserslautern, GERMANY
 e-mail: dempwolff@mathematik.uni-kl.de

Peter Müller
 Mathematisches Institut, Universität
 97074 Würzburg, GERMANY
 e-mail: peter.mueller@mathematik.uni-wuerzburg.de