WILLIAM M. KANTOR*

TWO FAMILIES OF FLAG-TRANSITIVE AFFINE PLANES

Dedicated to Otto Wagner on the occasion of his 60th birthday

ABSTRACT. Two families of flag-transitive nondesarguesian affine planes of odd order are defined, and isomorphisms among the various planes are studied.

Thirty years ago Wagner [5] proved the important result that every finite flag-transitive affine plane is a translation plane. However, since that time relatively few classes of such planes have been found. The purpose of this note is to comment on two constructions of flag-transitive affine planes due to Suetake [4]. These constructions will be generalized slightly and will be shown to produce fairly large numbers of pairwise nonisomorphic planes. Most of them are new (compare [1], [4] and the references therein), but those that are 2-dimensional over their kernels were known previously [1], [2].

Let $F = \mathrm{GF}(q^{2n})$, $L = \mathrm{GF}(q^n)$ and $K = \mathrm{GF}(q)$, where $n > 1$ and $q = p^e$ is a power of an odd prime p. Let $\sigma \in \mathrm{Gal}(L/K)$; we will assume (unless stated otherwise) that $\sigma \neq 1$. Throughout this note we will identify each such automorphism σ with a power of q inducing it.

Assume that n is odd. Let $b \in F$ be such that $\bar{b} = -b$ (where bar denotes the involutory automorphism of F), so that $b^2 = -b\bar{b} \in L$. Let $s \in F^*$ have order $(q^n + 1)(q - 1)$. Write $h(x) = x + bx^\sigma$ for $x \in F$, and consider the set

$$\mathscr{S}_{b,\sigma} = \{s^i h(L) \mid 0 \leqslant i \leqslant q^n\}$$

of subspaces of F, where F is always viewed as a K-space. This is very slightly more general than Suetake's construction (he assumes that $\sigma = q$ and $q^n \equiv 3 \pmod 4$).

For $\alpha \in F$ let $\tilde{\alpha}$ denote the linear transformation $z \to \alpha z$ from F to itself.

THEOREM 1. (i) *$\mathscr{S}_{b,\sigma}$ is a spread, and defines a nondesarguesian translation plane $\Pi_{b,\sigma}$.*

(ii) *$\Pi_{b,\sigma}$ admits a flag-transitive group inducing a cyclic group on the line at infinity.*

(iii) *The number of pairwise nonisomorphic translation planes arising in this*

*Research supported in part by NSF grant DMS 87-01794 and NSA grant MDA 904-88-H-2040.

Geometriae Dedicata **41:** 191–200, 1992.

manner is at least $\frac{1}{2}(n/n^* - 1)(q^{n^*} - 1)/2en^*$, *where* n/n^* *is the smallest prime factor of* n.

Proof. (i, ii) First of all, h is injective: if $x + bx^\sigma = 0$ with $x \in L$ then also $x + \bar{b}x^\sigma = 0$, so that $x = 0$. Thus, $\mathscr{S}_{b,\sigma}$ consists of n-dimensional K-spaces.

Clearly, $\tilde{s}$ induces a cycle transitive on $\mathscr{S}_{b,\sigma}$, so that (ii) holds if (i) is presupposed.

Assume that $h(x) = s^i h(y)$ with $x, y \in L^*$ and $0 < i \leqslant q^n$. Then

$$(x + bx^\sigma)(x + \bar{b}x^\sigma) = s^i\bar{s}^i(y + by^\sigma)(y + \bar{b}y^\sigma),$$

so that $x^2 - b^2(x^\sigma)^2 = k[y^2 - b^2(y^\sigma)^2]$ with $k = s^i\bar{s}^i \in K$. Then $x^2 - ky^2 = b^2(x^2 - ky^2)^\sigma$. However, $(x^2 - ky^2)^{\sigma-1}$ is the square of an element of L whereas b^2 is not. Consequently, $x^2 - ky^2 = 0$, so that $x = my$ where $m \in L$ and $m^2 = k$. Since n is odd, so is $(q^n - 1)/(q - 1)$, and hence $m \in K$. Then $m(y + by^\sigma) = my + b(my)^\sigma = s^i(y + by^\sigma)$, so that $m = s^i$, $(s^i)^{q-1} = 1$, and hence $(q^n + 1)(q - 1) \mid i(q - 1)$, whereas $0 < i \leqslant q^n$. This contradiction proves (i).

Before proving (iii) we will need an isomorphism criterion. Let $H(\sigma) = \{z \to \alpha^{1-\sigma}z^\varphi \text{ for } z \in F \mid \alpha \in L^*, \varphi \in \mathrm{Aut}\, F\}$, so that $H(\sigma)$ induces a group of permutations of $bL^* = \{d \in F^* \mid \bar{d} = -d\}$. Note that $|H(\sigma)| = 2en(q^n - 1)/(q^n - 1, \sigma - 1)$.

LEMMA 1. (I) $\Pi_{b,\sigma} \cong \Pi_{b^{-1},\sigma^{-1}}$.

(II) *If* $\Pi_{b,\sigma} \cong \Pi_{c,\tau}$ *then* $\tau = \sigma^{\pm 1}$.

(III) $\Pi_{b,\sigma}$ *is nondesarguesian.*

(IV) $\Pi_{b,\sigma} \cong \Pi_{c,\sigma}$ *if and only if* b *and* c *are in the same* $H(\sigma)$*-orbit.*

Proof. The transformation $z \to b^{-1}z$ sends $x + bx^\sigma$ to $x^\sigma + b^{-1}(x^\sigma)^{\sigma^{-1}}$, so (I) holds.

If b and c are in the same $H(\sigma)$-orbit then $c = \alpha^{1-\sigma}b^\varphi$ for some $\alpha \in L$ and $\varphi \in \mathrm{Aut}\, F$. Then $(\alpha y^\varphi) + c(\alpha y^\varphi)^\sigma = \alpha(y + by^\sigma)^\varphi$, so that the transformation $z \to \alpha z^\varphi$ induces an isomorphism $\Pi_{b,\sigma} \cong \Pi_{c,\sigma}$, which proves part of (IV). We will prove (II), (III) and the harder part of (IV) simultaneously.

Note that $\mathscr{S}_{c,\tau}$ and $\Pi_{c,\tau}$ are also meaningful when $\tau = 1$ – in which case $\Pi_{c,\tau}$ is desarguesian (since then $x + cx^\tau = (1 + c)x$). With this in mind, assume that $\Pi_{b,\sigma} \cong \Pi_{c,\tau}$, where we temporarily allow the possibility that $\tau = 1$. Note that K is contained in the kernel of both of these planes. (Recall that the *kernel* of $\Pi_{b,\sigma}$ is the field consisting of all endomorphisms of the abelian group F that map each line through 0 into itself.) It follows that there is a K-semilinear transformation $g: F \to F$ sending $\Pi_{b,\sigma}$ to $\Pi_{c,\tau}$ and hence sending $\mathscr{S}_{b,\sigma}$ to $\mathscr{S}_{c,\tau}$.

Let $s_0 \in \langle s \rangle$ have prime order and generate F^* (s_0 exists by [6]). Then a

Sylow $|s_0|$-subgroup of $\Gamma L(F)$ is cyclic. Clearly, g conjugates the collineation group of $\Pi_{b,\sigma}$ to that of $\Pi_{c,\tau}$. By Sylow's Theorem, we may assume that g conjugates $\langle \tilde{s}_0 \rangle$ to itself. Then g has the form $z \to \alpha z^{\varphi}$ with $\alpha \in F^*$ and $\varphi \in \mathrm{Aut}\, F$ (for all $z \in F$). Since $\Pi_{b,\sigma} \cong \Pi_{b^{\varphi},\sigma}$ (by the part of (IV) already verified) and $\varphi^{-1}g$ is an isomorphism from $\Pi_{b^{\varphi},\sigma}$ to $\Pi_{c,\tau}$, by replacing g by $\varphi^{-1}g$ we may assume that $\varphi = 1$. Similarly, by replacing g by $g\tilde{s}^i$ for some i we may assume that $\alpha h(L) = h(L)^g = h'(L)$, where $h'(x) = x + cx^{\tau}$ for $x \in F$.

Thus, for each $x \in L^*$ there is some $y \in L^*$ such that $x + cx^{\tau} = \alpha(y + by^{\sigma})$; and $x \to y$ defines a permutation of L^*. Then $x - cx^{\tau} = x + \bar{c}x^{\tau} = \bar{\alpha}(y + \bar{b}y^{\sigma}) = \bar{\alpha}(y - by^{\sigma})$. Write $\beta = \alpha + \bar{\alpha}$ and $\delta = \alpha - \bar{\alpha}$. Then $2x = \beta y + \delta b y^{\sigma}$ and $2cx^{\tau} = \delta y + \beta b y^{\sigma}$, so that $c\{\beta y + \delta b y^{\sigma}\}^{\tau} = \delta y + \beta b y^{\sigma}$. Note that $\beta, \delta b \in L$. Then

$$(1) \qquad c\beta^{\tau} y^{\tau} + c(\delta b)^{\tau} y^{\sigma\tau} = \delta y + \beta b y^{\sigma} \text{ for all } y \in L.$$

Write $y = uz$ here, where $u, z \in L$. By two applications of (1),

$$c\beta^{\tau} u^{\tau} z^{\tau} + u^{\sigma\tau}\{\delta z + \beta b z^{\sigma} - c\beta^{\tau} z^{\tau}\} = \delta u z + \beta b u^{\sigma} z^{\sigma},$$

so that

$$(2) \qquad c\beta^{\tau}(u^{\tau} - u^{\sigma\tau})z^{\tau} = \delta(u - u^{\sigma\tau})z + \beta b(u^{\sigma} - u^{\sigma\tau})z^{\sigma} \text{ for all } u, z \in L.$$

If $\tau = 1$ then (since $\sigma \neq 1$) (2) implies that $c\beta = \delta$. Then $c\delta b = \beta b$ by (1), so that $c^2\beta = \beta$. Since $c \neq \pm 1$ it follows that $\beta = 0$; but then $\delta = 0$, so that $\alpha = 0$, which is not the case. This proves (III). From now on we may assume that $\sigma, \tau \neq 1$.

Suppose that $\beta \neq 0$. Choose $u \in L$ not fixed by σ. Then (2) can be rewritten in the form $z^{\tau} = Az + Bz^{\sigma}$ for all $z \in L$, where $A, B \in F$. In particular, $1 = A + B$ and $(Au + Bu^{\sigma})^2 = u^{2\tau} = Au^2 + Bu^{2\sigma}$, so that $(A^2 - A)u^2 + (B^2 - B)u^{2\sigma} + 2ABuu^{\sigma} = 0$. Then $AB(u - u^{\sigma})^2 = 0$, so that $A = 0$ or $B = 0$. It follows that either $z^{\tau} = z$ for all $z \in L$ or $z^{\tau} = z^{\sigma}$ for all $z \in L$. Consequently, $\tau = \sigma$ in this case.

Now suppose that $\beta = 0$. Then $\delta \neq 0$, while (2) states that $\delta(u - u^{\sigma\tau})z = 0$. Thus, $\sigma\tau = 1$ in this case.

This proves (II). We may now assume that $\tau = \sigma$.

Claim: $c\beta^{\sigma} - \beta b = 0$ *and* $\delta = 0$. Namely, (2) states that

$$(c\beta^{\sigma} - \beta b)(u^{\sigma} - u^{\sigma^2})z^{\sigma} = \delta(u - u^{\sigma^2})z \quad \text{for all } u, z \in L.$$

This proves the claim if $\delta = 0$. Since n is odd, $\sigma^2 \neq 1$. If $\delta \neq 0$ then z/z^{σ} is constant for all $z \in L^*$; and then $z/z^{\sigma} = 1$, which is not the case.

Consequently, $c = \beta^{1-\sigma} b$ with $\beta = 2\alpha \in L$, proving the first part of (IV).

□

Proof of Theorem 1 *continued.* (iii) Choose σ to be one of the automorphisms q^{jn^*} with $1 \leqslant j \leqslant \frac{1}{2}(n/n^* - 1)$. Note that no two of these automorphisms are inverses of one another, $(n/n^*, j) = 1$, and

$$|H(\sigma)| = 2en(q^n - 1)/(q^n - 1, \sigma - 1) = 2en(q^n - 1)/(q^{n^*} - 1).$$

For each of the n/n^* automorphisms σ^{2i} with $0 \leqslant i < |\sigma| = n/n^*$, the stabilizer $H(\sigma)_b$ of b contains $z \to b^{(1-\sigma)\cdot(\sigma^{2i}-1)/(\sigma-1)} z^{\sigma^{2i}}$, where $b^{(\sigma^{2i}-1)/(\sigma-1)} \in L$ since $(\sigma^{2i} - 1)/(\sigma - 1)$ is even. Then the orbit $b^{H(\sigma)}$ has length $|b^{H(\sigma)}| \leqslant |H(\sigma)|/|\sigma|$, so that the number of $H(\sigma)$-orbits on bL^* is $\geqslant (q^n - 1)/(|H(\sigma)|/|\sigma|) = (q^{n^*} - 1)/2en^*$. By varying j we obtain at least $\frac{1}{2}(n/n^* - 1)(q^{n^*} - 1)/2en^*$ nonisomorphic planes by Lemma 1. □

REMARKS. 1. The kernel of $\Pi_{b,\sigma}$ is the fixed field of σ. Namely, if K' is the kernel then the K-space F must also be a vector space over K'. Then K is a subfield of K', and s_0 is a K'-linear transformation. It follows that K'^* lies in the centralizer of s_0 in $\mathrm{GL}(F)$–i.e., in F^*.

Now if $g \in K'^*$ then g must fix the line $h(L)$ and hence, in the proof of Lemma 1, $b = c$ and g has the form $z \to \alpha z$ for some $\alpha \in F^*$. That proof yields that $b = \alpha^{1-\sigma} b$ with $\alpha \in L$, so that α is in the fixed field of σ. The converse is trivial.

2. We used n^* in order to minimize the order of $H(\sigma)$. For example, if $\sigma = q^j$ with $(j, n) = 1$ then K is the fixed field of σ, so that $(q^n - 1)/(|H(\sigma)|/|\sigma|) = (q - 1)/2e$ and for composite n we obtain significantly fewer planes than in (iii).

3. It may be instructive to compare the above construction, as well as those in [4], with one in [3]. There, spreads for flag-transitive planes consist of the following subspaces whenever q is even, n is odd, $r \in \mathrm{GF}(q^2) - GF(q)$, and $t(x) = T(x) + rx$ where $T: \mathrm{GF}(q^n) \to \mathrm{GF}(q)$ is the trace map: $\{s^i t(L) \mid 0 \leqslant i \leqslant q^n\}$. Moreover, r and $r' \in \mathrm{GF}(q^2) - \mathrm{GF}(q)$ determine isomorphic planes if and only if $r' + 1 = \alpha(r + 1)^\varphi$ with $\alpha \in \mathrm{GF}(q)^*$, $\varphi \in \mathrm{Aut}\,\mathrm{GF}(q^2)$.

We now turn to a second family of flag-transitive planes. Again let $F = \mathrm{GF}(q^{2n})$, $L = \mathrm{GF}(q^n)$ and $K = \mathrm{GF}(q)$, where $n > 1$ and this time $q^n \equiv 1 \pmod 4$. Let $\sigma \in \mathrm{Gal}(F/K)$, and let $\sigma|_L$ denotes its restriction to L (note the new meaning for σ!). Assume that $\sigma|_L \neq 1$.

Let p, e, s, b and h be as before; write $t = s^2$. Set

$$\mathscr{S}'_{b,\sigma} = \{t^i h(L) \mid 0 \leqslant i \leqslant \tfrac{1}{2}(q^n - 1)\} \cup \{t^i h(bL) \mid 0 \leqslant i \leqslant \tfrac{1}{2}(q^n - 1)\}.$$

This construction again is due to Suetake when $\sigma = q$.

THEOREM 2. (i) $\mathscr{S}'_{b,\sigma}$ *is a spread, defining a translation plane* $\Pi'_{b,\sigma}$.

(ii) $\Pi'_{b,\sigma}$ *admits a flag-transitive group inducing a noncyclic group on the line at infinity.*

(iii) *If the fixed field of* σ *is properly contained in* L *then* $\Pi'_{b,\sigma}$ *does not admit a cyclic group acting transitively on the line at infinity.*

(iv) *The number of pairwise nonisomorphic translation planes arising in* (iii) *is at least*

$$\begin{cases} (n/n^* - 1)(q^{n^*} - 1)/4en^* & \text{if } n \text{ is odd and } n/n^* \text{ is the smallest prime factor of } n \\ (q^{n/2} - 1)/en & \text{if } n \text{ is even.} \end{cases}$$

(v) *If* n *and* q *are primes then the number in* (iv) *is exactly* $(q-1)/2$.

Proof. (i, ii) As before, $\mathscr{S}'_{b,\sigma}$ consists of n-dimensional K-spaces.

Here $\langle \tilde{t} \rangle$ has just two orbits on $\mathscr{S}'_{b,\sigma}$. The transformation $z \to bz^\sigma$ sends $t^i(x + bx^\sigma)$ to $t^{i\sigma}([bx^\sigma] + b[bx^\sigma]^\sigma)$ and $t^i([bx] + b[bx]^\sigma)$ to $t^{i\sigma}([bb^\sigma x^\sigma] + b[bb^\sigma x^\sigma]^\sigma)$, where $bb^\sigma \in L$. This proves (ii) if (i) is presupposed.

As before, if $h(x) = t^i h(y)$ with $x, y \in L^*$ and $0 < i \leqslant \frac{1}{2}(q^n - 1)$, then

$$(x + bx^\sigma)(x + \bar{b}x^\sigma) = t^i\bar{t}^i(y + by^\sigma)(y + \bar{b}y^\sigma),$$

so that $x^2 - b^2(x^\sigma)^2 = k(y^2 - b^2(y^\sigma)^2)$, where this time $k = t^i\bar{t}^i = (s^i\bar{s}^i)^2$ is a square in K. As before, it follows in turn that $x^2 = ky^2$; that $x = my$ with $m \in K$; that $m = t^i$; that $(t^i)^{q-1} = 1$; and finally that $\frac{1}{2}(q^n + 1)(q-1) \mid i(q-1)$, which contradicts the fact that $0 < i \leqslant \frac{1}{2}(q^n - 1)$.

In view of transitivity, it remains to consider the possibility that $h(x) = t^i h(by)$ for some $x, y \in L^*$ and some i. This time

$$\begin{aligned} x^2 - b^2x^{2\sigma} &= (x + bx^\sigma)(x + \bar{b}x^\sigma) \\ &= t^i\bar{t}^i(by + b(by)^\sigma)(\bar{b}y + \bar{b}(\bar{b}y)^\sigma) = -k[b^2y^2 - b^2(by)^{2\sigma}] \end{aligned}$$

where $k = t^i\bar{t}^i$ is a square in K. Then $x^2 + kb^2y^2 = b^2(x^2 + kb^2y^2)^\sigma$, and $(x^2 + kb^2y^2)^{\sigma-1}$ is the square of an element of L but b^2 is not. Consequently, $x^2 + kb^2y^2 = 0$, so that $x = mby$ with $m^2 = -k$. Note that $x, y \in L^*$ but $b \notin L$, so that $m \notin L$. On the other hand, since $q^n \equiv 1 \pmod 4$ we have $-1 = l^2$ for some $l \in L$. Then $(ml)^2 = k$ is a square in K, whereas $ml \notin K$ since $l \in L$ and $m \notin L$. This contradiction proves (ii). (*N.B.* This argument did not use the hypothesis $\sigma|_L \neq 1$. However, if $\sigma|_L = 1$ then $\Pi'_{b,\sigma}$ is desarguesian.)

Once again we need an isomorphism criterion. Let $H_1(\sigma) = \{z \to \alpha^{1-\sigma}z^\varphi$ for $z \in F \mid \alpha \in L^* \cup bL^*, \varphi \in \mathrm{Aut}\, F\}$, so that $H_1(\sigma)$ induces a group of permutations of bL^*. Note that $|H_1(\sigma)| = 2en \cdot 2(q^n - 1)/(2(q^n - 1), \sigma - 1)$.

LEMMA 2. (I) $\Pi'_{b,\sigma} \cong \Pi'_{b^{-1},\sigma^{-1}}$.

(II) *If b and c are in the same $H_1(\sigma)$-orbit then* $\Pi'_{b,\sigma} \cong \Pi'_{c,\sigma}$.

(III) *If* $\Pi'_{b,\sigma} \cong \Pi'_{c,\tau}$ *then* $\tau = \sigma^{\pm 1}$.

(IV) *If* $\Pi'_{b,\sigma} \cong \Pi'_{c,\sigma}$ *then b and c are in the same $H_1(\sigma)$-orbit.*

Proof. (I) The transformation $z \to b^{-1}z$ sends $x + bx^\sigma$ to $x^\sigma + b^{-1}(x^\sigma)^{\sigma^{-1}}$ and $bx + bb^\sigma x^\sigma$ to $b^{-1}(bb^\sigma x^\sigma) + b^{-1}b^{-\sigma^{-1}}(bb^\sigma x^\sigma)^{\sigma^{-1}}$, where $bb^\sigma \in L$.

(II) If $c = \alpha^{1-\sigma}b^\varphi$ with $\alpha \in L^*$, $\varphi \in \mathrm{Aut}\, F$, then the transformation $z \to \alpha z^\varphi$ sends $x + bx^\sigma$ to $(\alpha x^\varphi) + c(\alpha x^\varphi)^\sigma$ and $bx + bb^\sigma x^\sigma$ to $c[(\alpha b^\varphi/c)x^\varphi] + cc^\sigma[(\alpha b^\varphi/c)x^\varphi]^\sigma$, where $\alpha b^\varphi/c \in L$.

If $c = \alpha^{1-\sigma}b^\varphi$ with $\alpha \in bL^*$, $\varphi \in \mathrm{Aut}\, F$, then the transformation $z \to \alpha z^\varphi$ sends $x + bx^\sigma$ to $c[(\alpha/c)x^\varphi] + cc^\sigma[(\alpha/c)x^\varphi]^\sigma$ and $bx + bb^\sigma x^\sigma$ to $[\alpha b^\varphi x^\varphi] + c[\alpha b^\varphi x^\varphi]^\sigma$, where α/c, $\alpha b^\varphi \in L$.

(III, IV) As in Lemma 1, if $\Pi'_{b,\sigma} \cong \Pi'_{c\tau}$ then we may assume that an isomorphism is induced by a transformation g of the form $z \to \alpha z^\varphi$ for some $\alpha \in F^*$ and some $\varphi \in \mathrm{Aut}\, F$. As before, we may also assume that $\varphi = 1$, and, by using $\langle \tilde{t} \rangle$, also that $\alpha h(L) = h'(L)$ or $h'(cL)$. Let θ denote the automorphism $z \to \bar{z}$.

Case 1: $h'(L) = \alpha h(L)$. As in the proof of Lemma 1, (1) and (2) hold and we have $\tau|_L = \sigma^{\pm 1}|_L$. Moreover, by (I) we may assume that $\tau|_L = \sigma|_L$ (so that $\tau = \sigma$ or $\sigma\theta$). This time (2) implies that $c\beta^\tau - \beta b = 0$, and either $\delta = 0$ or $\sigma^2|_L = 1$ (where $\beta = \alpha + \bar{\alpha} \in L$ and $\delta = \alpha - \bar{\alpha}$ as before). Here $\beta^\tau = \beta^\sigma$, so that $c\beta^\sigma = \beta b$.

Since g normalizes $\langle \tilde{t} \rangle$ it must send the $\langle \tilde{t} \rangle$-orbits on $\mathscr{S}'_{b,\sigma}$ to those on $\mathscr{S}'_{c,\tau}$. Thus, $\alpha h(bL) = t^j h'(cL)$ for some j; write $w = t^j$. Then

$$w(cx + cc^\tau x^\tau) = \alpha(by + bb^\sigma y^\sigma) \tag{3}$$

for another permutation $x \to y$ of L^*.

Subcase 1.1: $\sigma^2|_L \neq 1$. We have just observed that $\delta = 0$, so $\beta = 2\alpha$, and that $c = \alpha^{1-\sigma}b$ and b lie in the same $H_1(\sigma)$-orbit. In (III) we still must show that $\tau = \sigma$, so assume that $\tau = \sigma\theta$.

Since $w(cx + cc^\tau x^\tau) = \alpha(by + bb^\sigma y^\sigma) = c(\alpha^\sigma y) + cc^\sigma(\alpha^\sigma y)^\sigma$, it follows that $w(x + c^\tau x^\tau) = v + c^\sigma v^\sigma$, where $v = \alpha^\sigma y \in L$ since $\alpha \in L$. As before we find first that $\bar{w}(x - c^\tau x^\tau) = v - c^\sigma v^\sigma$, then that $k(x^2 - (c^\tau x^\tau)^2) = v^2 - (c^\sigma v^\sigma)^2$ where $k = w\bar{w}$ is a square in K, $c^\tau = \bar{c}^\sigma = -c^\sigma$ and $x^\tau = x^\sigma$, and then that $kx^2 - v^2 = c^{2\sigma}(kx^2 - v^2)^\sigma$.

Now $v^2 = kx^2$ for all $x \in L$, where v is an additive function of x and k is a square in K. Thus, for all $x \in L$, $v = mx$ for some $m \in K$. Then $m^\sigma = m$, and $w(x + c^\tau x^\sigma) = mx + c^\sigma m x^\sigma$ for all $x \in L$. This implies both that $w = m$ and that $wc^\tau = c^\sigma m = -c^\tau m$, which is ridiculous. Thus, $\tau = \sigma$.

Subcase 1.2: $\sigma^2|_L = 1$. Since $\sigma|_L = \tau|_L \neq 1$, $\sigma^2 = \theta = \tau^2$ and hence $\tau = \sigma$ or σ^{-1}. This proves (III) in this situation, so by (I) we may assume that $\tau = \sigma$. Recall that $c\beta^\sigma = \beta b$. If $\beta \neq 0$ then b and c lie in the same $H_1(\sigma)$-orbit.

Assume that $\beta = 0$ and hence $\delta = \alpha - \bar{\alpha} = 2\alpha$. Since (1) holds with $\tau = \sigma$ we have $c\delta^\sigma b^\sigma = \delta$, so that $c\alpha^\sigma b^\sigma = \alpha$. By (3), $\bar{w}(-cx + cc^\sigma x^\sigma) = -\alpha(-by + bb^\sigma y^\sigma)$, so that $(w - \bar{w})cx + (w + \bar{w})cc^\sigma x^\sigma = 2\alpha by$ and $(w + \bar{w})cx + (w - \bar{w})cc^\sigma x^\sigma = 2\alpha bb^\sigma y^\sigma$. Then

$$\{(w + \bar{w})cx + (w - \bar{w})cc^\sigma x^\sigma\}\alpha^\sigma$$
$$= 2\alpha b\alpha^\sigma b^\sigma y^\sigma = \alpha b\{(w - \bar{w})cx + (w + \bar{w})cc^\sigma x^\sigma\}^\sigma$$

for all $x \in K$. Consequently, $(w + \bar{w})c\alpha^\sigma = \alpha b(w + \bar{w})^\sigma c^\sigma c^{\sigma\sigma}$ and $(w - \bar{w})cc^\sigma\alpha^\sigma = \alpha b(w - \bar{w})^\sigma c^\sigma$. If $\bar{w} \neq w$ then $c = \{(w - \bar{w})/\alpha\}^{\sigma-1}b$ with $(w - \bar{w})/\alpha \in L^*$, so that b and c are in the same $H_1(\sigma)$-orbit. Suppose that $\bar{w} = w$. Then $w^2 = w\bar{w}$ is a square in K, so that $w \in K$. Now $\bar{w} = w = w^\sigma$, so that $(w + w)c\alpha^\sigma = \alpha b(w + w)c^\sigma\bar{c}$ and hence $c\alpha^\sigma = -\alpha bc^\sigma c$. Now $-\alpha = (\alpha^\sigma)^\sigma = (-\alpha bc^\sigma)^\sigma = -\alpha^\sigma b^\sigma\bar{c} = \alpha^\sigma b^\sigma c$, whereas we already knew that $c\alpha^\sigma b^\sigma = \alpha$.

Case 2: $h'(cL) = \alpha h(L)$. This time there is a permutation $x \to y$ of L^* such that $cx + cc^\tau x^\tau = \alpha(y + by^\sigma)$. Then $-cx + cc^\tau x^\tau = \bar{\alpha}(y - by^\sigma)$, so that $2cx = \delta y + \beta by^\sigma$ and $2cc^\tau x^\tau = \beta y + \delta by^\sigma$, where $\beta = \alpha + \bar{\alpha}$ and $\delta = \alpha - \bar{\alpha}$ as before. Now $c(\delta y + \beta by^\sigma)^\tau = \beta y + \delta by^\sigma$ for all $y \in L$. As in the proof of Lemma 1 this implies first that $c\delta^\tau(u^\tau - u^{\sigma\tau})z^\tau = \beta(u - u^{\sigma\tau})z + \delta b(u^\sigma - u^{\sigma\tau})z^\sigma$ for all $u, z \in L$, and then that $\tau|_L = \sigma^{\pm 1}|_L$.

Now suppose that $\tau|_L = \sigma|_L$ (cf. (I)). Then

$$(c\delta^\tau - \delta b)(u^\sigma - u^{\sigma^2})z^\sigma = \beta(u - u^{\sigma^2})z \quad \text{for all } u, z \in L,$$

which as before yields that $c\delta^\tau - \delta b = 0$ and either $\beta = 0$ or $\sigma^2|_L = 1$. Now $c\delta^\tau y^\sigma + c\beta^\tau b^\tau y^{\sigma\sigma} = \beta y + \delta by^\sigma$ implies that $c\beta^\tau b^\tau y^{\sigma^2} = \beta y$. Then $c\beta^\tau b^\tau = \beta$, and either $\beta = 0$ or $\sigma^2|_L = 1$. Since we already know that $c\delta^\tau = \delta b$, where $\delta^\tau = \delta^\sigma$ or $\delta^\tau = \bar{\delta}^\sigma = -\delta^\sigma$, one of the following holds:

$$\beta = 0,\ \delta \neq 0 \text{ and } c = \pm\delta^{1-\sigma}b, \text{ or}$$
$$\beta \neq 0,\ c = \beta^{1-\sigma}b^{-\tau} \text{ and } \sigma^2|_L = 1.$$

Since g normalizes $\langle\tilde{t}\rangle$ it must send the $\langle\tilde{t}\rangle$-orbits on $\mathscr{S}'_{b,\sigma}$ to those on $\mathscr{S}'_{c,\tau}$. Thus, $\alpha h(bL) = t^j h'(L)$ for some j; write $w = t^j$. Then

$$w(x + cx^\tau) = \alpha(by + bb^\sigma y^\sigma) \tag{4}$$

for another permutation $x \to y$ of L^*.

Subcase 2.1: $\sigma^2|_L \neq 1$. If $\tau = \sigma$ then $\delta^\tau = \delta^\sigma$, so that $c = \delta^{1-\sigma}b$ and b lie in the same $H_1(\sigma)$-orbit, as required in (III). It remains to assume that $\tau = \sigma\theta$, or equivalently, $c = -\delta^{1-\sigma}b$, and derive a contradiction.

We have $\beta = 0$, $\delta = \alpha - \bar{\alpha} = 2\alpha$ and $c\alpha^\sigma = -\alpha b$. By (4),

$$w(x + cx^\tau) = \alpha(by + bb^\sigma y^\sigma) = -c\alpha^\sigma y - c\alpha^\sigma(-c\alpha^\sigma/\alpha)^\sigma y^\sigma = v - cv^\sigma$$

with $v = -c\alpha^\sigma y$. Here $v \in L$ since $\bar{\alpha} = -\alpha$. Now $k(x^2 - c^2x^{2\sigma}) = v^2 - c^2v^{2\sigma}$ where $k = w\bar{w}$ is a square in K. Then $kx^2 - v^2 = c^2(kx^2 - v^2)^\sigma$ implies that, for some $m \in K$ and all $x \in L$, $v = mx$. Thus, $w(x + cx^\sigma) = mx - cmx^\sigma$, so that $w = m$ and $cw = -cm$, which is impossible.

Subcase 2.2: $\sigma^2|_L = 1$. As in Subcase 1.2 we may assume that $\tau = \sigma$. If $\delta \neq 0$ then $c = \delta^{1-\sigma}b$, and hence b and c are in the same $H_1(\sigma)$-orbit.

Assume that $\delta = 0$, so that $\alpha \in L$ and $\alpha = c\alpha^\sigma b^\sigma$. By (4), $\bar{w}(x - cx^\sigma) = \alpha(-by + bb^\sigma y^\sigma)$, so that $(w + \bar{w})x + (w - \bar{w})cx^\sigma = 2\alpha bb^\sigma y^\sigma$ and $(w - \bar{w})x + (w + \bar{w})cx^\sigma = 2\alpha by$. Then

$$\{(w + \bar{w})x + (w - \bar{w})cx^\sigma\}\alpha^\sigma$$
$$= 2\alpha b\alpha^\sigma b^\sigma y^\sigma = \alpha b\{(w - \bar{w})x + (w + \bar{w})cx^\sigma\}^\sigma$$

for all $x \in K$. Consequently, $(w + \bar{w})\alpha^\sigma = \alpha b(w + \bar{w})^\sigma c^\sigma$ and $(w - \bar{w})c\alpha^\sigma = \alpha b(w - \bar{w})^\sigma$. If $\bar{w} \neq w$ then $c = \{(w - \bar{w})/\alpha\}^{\sigma-1}b$ with $(w - \bar{w})/\alpha \in bL^*$, so that b and c are in the same $H_1(\sigma)$-orbit. Suppose that $\bar{w} = w$. Then $w^2 = w\bar{w}$ is a square in K, so that $w \in K$. Now $\bar{w} = w = w^\sigma$, so that $(w + w)\alpha^\sigma = \alpha b(w + w)c^\sigma$ and hence $\alpha^\sigma = \alpha bc^\sigma$. Then $\alpha = \alpha^{\sigma\sigma} = \alpha^\sigma b^\sigma c^{\sigma\sigma} = \alpha^\sigma b^\sigma \bar{c} = -\alpha^\sigma b^\sigma c$, whereas we already knew that $\alpha = c\alpha^\sigma b^\sigma$. □

Proof of Theorem 2, *continued.* (iii) Assume that there is a cyclic group acting transitively on the line at infinity. By Sylow's Theorem we may assume that $\tilde{s}_0$ lies in that cyclic group. Then that cyclic group is contained in $C_{\Gamma L(F)}(\tilde{s}_0) = \{\tilde{\alpha} \mid \alpha \in F^*\}$. In the notation of the proof of Lemma 2(III, IV) we have $b = c$, and there must be a collineation $g = \tilde{\alpha}$ of $\Pi'_{b,\sigma}$ such that $\alpha h(L) = h(bL)$.

If $\sigma^2|_L \neq 1$ then Case 2 of that proof yields that $\beta = 0$ and $b = \delta^{1-\sigma}b$. Thus, $\delta^\sigma = \delta$ and $\delta = \alpha - \bar{\alpha} \notin L$. Consequently, the fixed field of σ is not contained in L, which is not the case in (iii).

If $\sigma^2|_L = 1$ then we are in the situation of the proof of Lemma 2, Subcase 2.2, where it was shown that $b = \delta^{1-\sigma}b$ or $b = \{(w - \bar{w})/\alpha\}^{\sigma-1}b$. Then δ or $(w - \bar{w})/\alpha$ lies in the fixed field of σ but not in L, which is not the case.

(iv) As in the proof of Theorem 1(iii), if φ is any power of σ then $z \to (b^{(\varphi-1)/(\sigma-1)})^{1-\sigma}z^\varphi$ fixed b, and moreover lies in $H_1(\sigma)_b$ since $b^{(\varphi-1)/(\sigma-1)} \in L^* \cup bL^*$. Thus, $|b^{H_1(\sigma)}| \leqslant |H_1(\sigma)|/|\sigma|$ for any b, so that the number of $H_1(\sigma)$-orbits on bL^* is at least $|\sigma|(q^n - 1)/(H_1(\sigma)|$.

Let n/n^* be the smallest prime factor of n. Choose $\sigma = q^{jn^*}$ where $1 \leqslant jn^* < n$ and j is odd; note that no two of these automorphisms of F are inverses of one another. In (iii) we require that the fixed field of σ is contained in L, and this holds since $(jn^*, 2n) = n^*$ is a factor of n (recall that j is odd). Note that $|\sigma| = 2n/n^*$, and

$$|H_1(\sigma)| = 4en(q^n - 1)/(2(q^n - 1), \sigma - 1) = 4en(q^n - 1)/(q^{n^*} - 1)$$

since $(q^{jn^*} - 1)/q^{n^*} - 1)$ is odd. Consequently, the number of $H_1(\sigma)$-orbits on bL^* is at least $(2n/n^*)(q^n - 1)/|H_1(\sigma)| = (q^{n^*} - 1)/2en^*$.

If $n/n^* = 2$ then this is precisely the assertion of (iv). If n/n^* is odd then, by varying j, we obtain (iv).

(v) Moreover, if n is prime then $n^* = 1$ and $\sigma = q^j$ for some j with $1 \leqslant j < 2n$. By Lemma 2(I) we may assume that $j \leqslant n$; and the requirement in (iii) that $(j, 2n)|n$ forces j to be odd. If, in addition, q is prime, then $|H_1(\sigma)| = 4n(q^n - 1)/(q - 1)$ and $|b^{H_1(\sigma)}| \leqslant |H_1(\sigma)|/|\sigma| = 2(q^n - 1)/(q - 1)$. However, there are $2(q^n - 1)/(q - 1)$ images of b under the linear mappings $z \to \alpha^{1-\sigma}z$ with $\alpha \in L^* \cup bL^*$. Thus, $|b^{H_1(\sigma)}| = 2(q^n - 1)/(q - 1)$ for each b, and hence $H_1(\sigma)$ has exactly $(q - 1)/2$ orbits on bL^*. □

REMARKS. 1. Suppose that $n = n'n''$ is the product of odd integers n', $n'' > 1$, and that $q^n \equiv 1 \pmod 4$. Let σ be the automorphism $q^{n'}$ of F. Then the condition $\sigma|_L \neq 1$ in Theorem 1 is certainly satisfied, and the fixed field of σ is contained in L. By Theorem 2(iii), $\Pi_{b,\sigma} \ncong \Pi'_{b,\sigma}$. Moreover, the spreads $\mathscr{S}_{b,\sigma}$ and $\mathscr{S}'_{b,\sigma}$ share half of their members: some sort of 'net replacement' is at work here.

2. In Theorem 2 suppose that n is odd but the fixed field of σ is *not* contained in L. *Claim: The spreads $\mathscr{S}_{b,\sigma}$ and $\mathscr{S}'_{b,\sigma}$ coincide.* Namely, let $\sigma = q^r$, so the fixed field of σ is $\mathrm{GF}(q^k)$ where $k = (r, 2n)$. Then $k \mid 2n$ but $k \nmid n$, so that $2n/k$ is odd. Let $u \in F^*$ have order $(q^n + 1)(q^{k/2} - 1)$, let $j = \frac{1}{2}(q^n + 1)$, and write $\alpha = u^j$. Since $(q^n - 1)/(q^{k/2} - 1)$ is odd, $\alpha \notin L$ and $\alpha^2 \in L$. Then $\alpha^\sigma = \alpha$, $\bar{\alpha} = -\alpha$, and $\alpha b, \alpha/b \in L$. It follows that $\alpha(x + bx^\sigma) = b(\alpha x/b) + bb^\sigma(\alpha x/b)^\sigma$ and $\alpha(bx + bb^\sigma x^\sigma) = (\alpha bx) + b(\alpha bx)^\sigma$, so that $\langle \tilde{u} \rangle$ is a collineation group transitive on the line at infinity of $\Pi'_{b,\sigma}$. Since the kernel of $\Pi'_{b,\sigma}$ contains $\mathrm{GF}(q^{k/2})$, we are in the situation of Theorem 1 but with K replaced by $\mathrm{GF}(q^{k/2})$ and s by u. This implies the Claim.

In particular, the Claim explains the restriction on the fixed field of σ in Theorem 2(iii).

3. Theorem 2 allows the possibility that $2n = 4$, a case studied intensively by Baker and Ebert [1], [2]. I am indebted to Gary Ebert for pointing out that the construction in Theorem 2 – which is just Suetake's in that case (since we might as well let $\sigma = q$ by Lemma 2(I)) – settles the conjecture made on p. 13 of [2] concerning the coordinate description of the planes studied there. The results in [1], [2] imply that *every odd order nondesarguesian flag-transitive translation plane of dimension 2 over its kernel is one of the planes* $\Pi'_{b,q}$.

In [1] the authors examine the isomorphism problem for these planes. They use an unusual notion of isomorphism, viewing two translation planes as isomorphic if and only if there is a *linear* isomorphism between the planes;

and then they conjecture that the number of pairwise nonisomorphic planes $\Pi'_{b,q}$ is $(q-1)/2$. This conjecture is precisely the content of Theorem 2(v) and its proof (when $n=2$), i.e., it is an *immediate* consequence of Lemma 2(II, IV). On the other hand, if $e>1$ is odd then it is easy to check that the number of planes is greater than $(q-1)/2e$.

4. If $G=\{z\to \alpha z^{\varphi}+u \mid \alpha\in F^*, u\in F, \varphi\in \mathrm{Aut}\, F\}$ then the proofs of Lemmas I and II easily imply that

$$G\cap \mathrm{Aut}\,\Pi_{b,\sigma}=\{z\to \alpha z^{\varphi}+u \mid \alpha\in L^*,\ u\in F,\ \varphi\in \mathrm{Aut}\, F, \text{ and } \alpha^{\sigma-1}=b^{\varphi-1}\}$$

$$G\cap \mathrm{Aut}\,\Pi'_{b,\sigma}=\{z\to \alpha z^{\varphi}+u \mid \alpha\in L^*\cup bL^*,\ u\in F,\ \varphi\in \mathrm{Aut}\, F, \text{ and } \alpha^{\sigma-1}=b^{\varphi-1}\}.$$

However, quite a bit more group theoretic machinery seems to be needed in order to show that

$$\mathrm{Aut}\,\Pi_{b,\sigma}=G\cap \mathrm{Aut}\,\Pi_{b,\sigma} \quad \textit{and} \quad \mathrm{Aut}\,\Pi'_{b,\sigma}=G\cap \mathrm{Aut}\,\Pi'_{b,\sigma} \quad \textit{provided that} \quad q^n>9.$$

It would be nice to have an elementary proof of this fact.

5. In view of the constructions in [3] and [4], there exists at least one nondesarguesian flag-transitive affine plane of order p^n whenever p is a prime, $n>1$, $p^n>81$, and either p is odd or n is odd. It would be very interesting to know whether or not there exist such planes of order 2^{2m} for any $m\geqslant 2$.

REFERENCES

1. Baker, R. D. and Ebert, G. L., 'Enumeration of two-dimensional flag-transitive planes', *Algebras, Groups Geom.* **3** (1985), 248–257.
2. Baker, R. D. and Ebert, G. L., 'Construction of two-dimensional flag-transitive planes', *Geom. Dedicata* **27** (1988), 9–14.
3. Kantor, W. M., 'Spreads, translation planes and Kerdock sets. II', *SIAM J. Algebraic Discrete Methods* **3** (1982), 308–318.
4. Suetake, C., 'Flag transitive planes of order q^n with a long cycle on l_∞ as a collineation' (to appear).
5. Wagner, A., 'On finite affine line transitive planes', *Math. Z.* **87** (1965), 1–11.
6. Zsigmondy, K., 'Zur Theorie der Potenzreste', *Monatsh. Math. Phys.* **3** (1892), 265–284.

Author's address:

W. M. Kantor,
Dept. of Mathematics,
University of Oregon,
Eugene, OR 97403-1222,
U.S.A.

(Received, April 1, 1990)