SOME NEW FINITE TRANSLATION PLANES

BY
F. W. WILKE AND J. L. ZEMMER

1. **Introduction.** A projective plane π is called a translation plane with respect to the line l_∞ provided π is C-l_∞ transitive for every C on l_∞. If coordinates are introduced in π as in [4, p. 353] by choosing points X, Y on l_∞ and O, I two additional points, such that no three of X, Y, O, I are collinear, the resulting ternary ring is a (right) Veblen-Wedderburn system. Throughout this paper a (right) Veblen-Wedderburn system will be called simply a V-W system. Two V-W systems $F(+, \cdot)$ and $F'(\oplus, \circ)$ are said to be isotopic if there exist three 1-1 mappings α, β, γ of F' onto F such that $0\gamma=0$, and $(x \circ y \oplus z)\gamma = x\alpha \cdot y\beta + z\gamma$ for all $x, y, z \in F'$. This definition may be found in [6, p. 187]. It is known that nonisotopic V-W systems can coordinatize the same plane π.

Classes of finite V-W systems have been constructed by Hall [4, p. 364], Andre [2, p. 182] and Ostrom [7, p. 461]. It is not immediately obvious that the translation planes obtained from these systems are not all obtainable from the Andre V-W systems. The main object of this paper is to construct a class of V-W systems which properly contains the class of Andre V-W systems and then to show that the class of finite translation planes obtainable from these V-W systems contains planes which cannot be coordinatized by any Andre V-W system.

The new class of V-W systems is described in §3, after giving in §2 a general construction of quasigroups and loops using groups. This construction is applied in §3 to the multiplicative group of a near-field to obtain the new V-W systems. The proof of the existence of translation planes which cannot be coordinatized by any Andre V-W system is contained at the end of the paper in §6. This proof requires some information about the nuclei of the multiplicative loops of certain V-W systems, particularly the Andre V-W systems, and about collineations of the Andre V-W planes. Theorems concerning these are found in §§4 and 5. Many of these theorems are interesting on their own. Another side result, which may be of interest, is contained in §3, where it is shown that a certain class of Andre V-W systems have multiplicative loops with the right inverse property. A geometric consequence of this fact is that the translation planes obtained from these systems possess collineations which interchange $X=(0)$ and $Y=(\infty)$.

2. **Some loops and quasigroups obtained from groups.** Let $G(\cdot)$ be a group and T a permutation of G. Let $\sigma: G \to Z$ be a mapping of G into the integers such that,

Received by the editors January 3, 1967.

for $a, b \in G$ there exists a unique integer m satisfying $m=\sigma((aT^m)^{-1}\cdot b)$. An operation $\circ$ may now be defined on G by

$$x \circ y = xT^{\sigma(y)}\cdot y. \tag{1}$$

THEOREM 1. *The system $G(\circ)$, defined as above, is a quasigroup.*

Proof. Clearly, for x, y in G, $x \circ y$ is a uniquely determined element of G. Let $a, b \in G$, and consider the equation $x \circ a=b$. If x is a solution, then $x \circ a=xT^{\sigma(a)}\cdot a=b$, whence $x=(b\cdot a^{-1})T^{-\sigma(a)}$. Since $(ba^{-1})T^{-\sigma(a)}$ satisfies the equation, we see that $x \circ a=b$ has a unique solution for each pair a, b in G. Further, if the equation $a \circ y=b$ has a solution, say y_0, then $a \circ y_0=aT^{\sigma(y_0)}\cdot y_0=b$, and hence $y_0=(aT^{\sigma(y_0)})^{-1}\cdot b$, whence

$$\sigma(y_0) = \sigma((aT^{\sigma(y_0)})^{-1}\cdot b).$$

By the condition imposed on σ there exists a *unique* integer m such that $m=\sigma((aT^m)^{-1}\cdot b)$. Hence $\sigma(y_0)=m$, and $y_0=(aT^m)^{-1}\cdot b$. Clearly, $(aT^m)^{-1}\cdot b$ satisfies the equation $a \circ y=b$, and hence this equation also has a unique solution. Thus, $G(\circ)$ is a quasigroup.

COROLLARY 1. *Let e be the identity of the group $G(\cdot)$. If $\sigma(e)=0$ and $eT=e$, then $G(\circ)$ is a loop with identity e.*

Proof. Let $x \in G$. Then $x \circ e=xT^{\sigma(e)}\cdot e=xT^0\cdot e=x\cdot e=x$; and $e \circ x=eT^{\sigma(x)}\cdot x=e\cdot x=x$.

To see that there exist mappings $\sigma\colon G \to Z$ satisfying the condition stated above, let T be an automorphism of G and G_1 the subgroup of G generated by the subset of elements of the form $xT\cdot x^{-1}$. Define $\sigma(x)$ as follows:

$$\begin{aligned} \sigma(x) &= 0 \quad \text{if } x \in G_1, \\ &= 1 \quad \text{if } x \notin G_1. \end{aligned}$$

It is not difficult to show that for $a, b \in G$, there exists a unique integer m ($m=0$ or 1 in this case) such that $m=\sigma((aT^m)^{-1}\cdot b)$. In case T is an involution, we have the following corollary.

COROLLARY 2. *Let T be an automorphism of order two of the group $G(\cdot)$, and G_1 the subgroup of $G(\cdot)$ generated by the subset of elements of the form $uT\cdot u^{-1}$. With σ defined as above, the loop $G(\circ)$ has the right inverse property.*

Proof. The proof of this corollary is based on the fact that each element of G of the form $uT\cdot u^{-1}$ is mapped by T into its own inverse. From this it follows that $x \in G_1$ implies $xT \in G_1$ and hence that x is in G_1 if and only if $xT \in G_1$. Now, for $x \in G$, denote by xJ the solution of $x \circ y=e$, then $xT^{\sigma(y)}\cdot y=e$, whence $xJ=y=(x^{-1})T^{\sigma(y)}$ or $xJ=(x^{-1})T^{\sigma(xJ)}$. If $x \in G_1$, then $x^{-1} \in G_1$ and hence $(x^{-1})T^{\sigma(xJ)} \in G_1$, whether $\sigma(xJ)=0$ or 1. Thus, $\sigma(xJ)=\sigma[(x^{-1})T^{\sigma(xJ)}]=0=\sigma(x)$. If $x \notin G_1$ then $x^{-1} \notin G_1$ and hence $(x^{-1})T^{\sigma(xJ)} \notin G_1$ and we have $\sigma(xJ)=\sigma[(x^{-1})T^{\sigma(xJ)}]=1=\sigma(x)$.

Thus, in general, $\sigma(xJ)=\sigma(x)$ and we have $xJ=(x^{-1})T^{\sigma(x)}$. To complete the proof, we compute $(y \circ x) \circ xJ$. Thus,

$$\begin{aligned}(y \circ x) \circ xJ &= (yT^{\sigma(x)} \cdot x)T^{\sigma(xJ)} \cdot xJ \\ &= (yT^{\sigma(x)} \cdot x)T^{\sigma(x)} \cdot (x^{-1})T^{\sigma(x)} \\ &= y \cdot xT^{\sigma(x)} \cdot (x^{-1})T^{\sigma(x)} = y.\end{aligned}$$

Further examples of mappings satisfying the conditions of Theorem 1 will be found in the next section where it is shown that the multiplication, $\circ$, in an Andre V-W system of order p^n is related to the multiplication, $\cdot$, in the finite field $GF(p^n)$ as in (1) above. Before proceeding to this, however, it is desirable to consider a special class of mappings σ satisfying the condition used in Theorem 1.

THEOREM 2. *Let $G(\cdot)$ be a group, T a permutation of G, and let*

$$\{1\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n \subset G_{n+1} = G$$

be a strictly increasing sequence of subgroups of G. Let $0=k_0, k_1, k_2, \ldots, k_n$ be a set of $n+1$ distinct integers satisfying $(xT^{k_i})^{-1} \cdot x \in G_i$, for all x in G and $i=0, 1, 2, \ldots, n$. Define $\sigma(x)$ as follows

$$\begin{aligned}\sigma(x) &= 0 \qquad \text{if } x = 1, \\ &= k_i \qquad \text{if } x \in G_{i+1}-G_i, \quad i = 0, 1, 2, \ldots, n,\end{aligned}$$

where $G_{i+1}-G_i=\{x \in G \mid x \in G_{i+1}$ and $x \notin G_i\}$. If a binary operation $*$ is defined on G by $x * y=xT^{\sigma(y)} \cdot y$, then $G(*)$ is a quasigroup.

Proof. In view of Theorem 1 it is sufficient to show that the mapping σ defined here satisfies the condition used in Theorem 1, that is, for each $a, b \in G$ there is a unique integer m such that $m=\sigma[(aT^m)^{-1} \cdot b]$. This will follow from showing that for $a, b \in G$, $a^{-1} \cdot b \in G_{i+1}-G_i$ if and only if $(aT^{k_i})^{-1} \cdot b \in G_{i+1}-G_i$, since in this event $m=\sigma(a^{-1}b)$ is the unique integer m satisfying $m=\sigma[(aT^m)^{-1} \cdot b]$.

Let $a, b \in G$, and suppose that $a^{-1} \cdot b \in G_{i+1}-G_i$. If $(aT^{k_i})^{-1} \cdot b \notin G_{i+1}$ then clearly $(aT^{k_i})^{-1} \cdot a=(aT^{k_i})^{-1}b \cdot b^{-1}a \notin G_{i+1}$, but $(aT^{k_i})^{-1} \cdot a \in G_i \subset G_{i+1}$. Since $(aT^{k_i})^{-1} \cdot b \notin G_{i+1}$ leads to a contradiction, we conclude that $(aT^{k_i})^{-1} \cdot b \in G_{i+1}$. Further, if $(aT^{k_i})^{-1} \cdot b \in G_i$, then since $a^{-1}b \notin G_i$, we have

$$(aT^{k_i})^{-1} \cdot a = (aT^{k_i})^{-1} \cdot b \cdot b^{-1}a \notin G_i,$$

again a contradiction. Hence $(aT^{k_i})^{-1} \cdot b \notin G_i$, and we have $(aT^{k_i})^{-1} \cdot b \in G_{i+1}-G_i$.

A similar argument shows that $(aT^{k_i})^{-1} \cdot b \in G_{i+1}-G_i$ implies that $a^{-1} \cdot b \in G_{i+1}-G_i$. Thus, by Theorem 1, $G(*)$ is a quasigroup.

COROLLARY. *The quasigroup $G(*)$ in Theorem 2 is a loop if and only if $eT^{\sigma(x)}=e$ for all x in G, where e is the identity of $G(\cdot)$.*

Proof. Since $\sigma(e)=0$, e is a right identity for $G(*)$. Thus, if $G(*)$ has an identity it must be e. Now, $e * x=eT^{\sigma(x)} \cdot x=x$ if and only if $eT^{\sigma(x)}=e$ for x in G.

Theorem 2 may be extended to include the case of an infinite strictly increasing, sequence, $\{1\}=G_0\subset G_1\subset G_2\subset\cdots$, of subgroups of G. This can be done by letting $G_\infty=\bigcup G_i$, and adding to Theorem 2 the hypothesis that there exists an integer k_∞ such that $(xT^{k_\infty})^{-1}\cdot x\in G_\infty$ for all x in G. For $x\in G-G_\infty$, define $\sigma(x)=k_\infty$. A slight modification of the proof of Theorem 2 then gives this extended version.

3. **The class** (C) **of Veblen-Wedderburn systems.** Let $F(+,\cdot)$ be a right near-field with additive identity 0 and multiplicative identity 1, and let T be an automorphism of the additive group of F, with $1T=1$. Denote by F' the nonzero elements of F and let $\sigma\colon F'\to Z$ be a mapping of F' into the integers such that for each $a, b\in F'$ there is a unique integer m satisfying $m=\sigma((aT^m)^{-1}\cdot b)$. If, further $\sigma(1)=0$ and an operation $*$ is defined on F by $x*y=xT^{\sigma(y)}\cdot y$ for $x, y\in F'$ and $0*x=x*0=0$ for all x in F, then it is not difficult to show that $F(+,*)$ is a right V-W system.

DEFINITION 1. The class of all V-W systems obtainable from near-fields in the manner described above will be called class (C).

The main result of this section is the following theorem.

THEOREM 3. *Every finite Andre V-W system is in class* (C).

Following Hughes [5] any finite Andre V-W system may be defined in terms of a finite field as follows. Denote by $F(+,\cdot)$ the finite field $GF(p^n)$ and let S be an automorphism of F of order t. If K is the fixed field of S, let μ be a mapping of K into Z_t (the integers modulo t) such that $\mu(0)=\mu(1)=0$. Let $\nu(x)=x\cdot xS\cdots xS^{t-1}$ for all $x\in F$, so that $\nu(x)\in K$ for all $x\in F$. Define $x\circ y=xS^{\mu\nu(y)}\cdot y$. Then $F(+,\circ)$ is an Andre V-W system.

It will now be shown that this Andre V-W system is in class (C). Denote by F' the nonzero elements of F and let $\sigma(x)=\mu\nu(x)$ for x in F'. If $a, b\in F'$ and m is an integer then $\sigma[(aS^m)^{-1}\cdot b]=\sigma[(a^{-1}S^m)\cdot b]=\mu\nu[(a^{-1}S^m)\cdot b]=\mu[\nu(a^{-1}S^m)\cdot\nu(b)]$ $=\mu[\nu(a^{-1})\cdot\nu(b)]=\mu\nu[a^{-1}b]=\sigma(a^{-1}b)$. Thus, $m=\sigma(a^{-1}b)=\mu\nu(a^{-1}b)$ is the unique integer m such that $m=\sigma[(aS^m)^{-1}\cdot b]$. Further, since $\sigma(1)=\mu\nu(1)=\mu(1)=0$ and $1S=1$, we see that the Andre V-W system is in class (C).

The following discussion is included here because, aside from illustrating Theorem 3 to some extent, it points out an advantage to considering the multiplication in an Andre V-W system in the form described in Theorem 1 rather than in the form described by Hughes [5].

Denote by $F(+,\cdot)$ the finite field $GF(p^{2n})$, p a prime and n an arbitrary positive integer. Let T be a generating automorphism of the group of automorphisms of F over $GF(p)$, and let $S=T^n$ so that S has order two. Then the fixed field of F is $K=GF(p^n)$. As above, for x in F let $\nu(x)=x\cdot xS$, so that $\nu(x)\in K$ for all x in F. Finally, define $\mu\colon K\to Z_2$ (the integers modulo 2) by $\mu(0)=\mu(1)=0$ and $\mu(y)=1$ if $0\neq y\neq 1$, and consider the Andre V-W system $F(+,*)$ where $*$ is given by $x*y=x^{\mu\nu(y)}\cdot y$. To describe this V-W system as in Theorem 1, let $F'(\cdot)$ be the multiplicative group of nonzero elements of $F(+,\circ)$ and F_1 the subgroup of $F'(\cdot)$

generated by elements of the form $uS\cdot u^{-1}$. Define the mapping $\sigma: F\to Z$ (the integers) by

$$\begin{aligned}\sigma(x) &= 0 \quad \text{if } x = 0 \text{ or } x\in F_1,\\ &= 1 \quad \text{if } x\neq 0 \text{ and } x\notin F_1.\end{aligned}$$

Let $F(+,\circ)$ be the V-W system whose multiplication $\circ$ is given by $x\circ y=xS^{\sigma(y)}y$. To see that $x\circ y=x*y$, it is sufficient to show that $\sigma(x)=\mu\nu(x)$ for all x in F. This is trivial for $x=0$. If $x\neq 0$, then $x\in F'$ and $\mu\nu(x)=0$ if and only if $\nu(x)=1$. From a well-known theorem on cyclic extensions [1, p. 200], $\nu(x)=1$ if and only if $x=uS\cdot u^{-1}$ for some $u\in F'$. Since $F'(\cdot)$ is a commutative group, $x=uS\cdot u^{-1}$ if and only if $x\in F_1$. Finally $x\in F_1$ if and only if $\sigma(x)=0$. Thus for $x\neq 0$ $\mu\nu(x)=0$ if and only if $\sigma(x)=0$. It follows that $\sigma(x)=\mu\nu(x)$ for all x in F, and hence that $x\circ y=x*y$ for all $x, y\in F$. Since $S^2=I$, it follows from Corollary 2 of Theorem 1 that the multiplicative loop of $F(+,\circ)$ has the right inverse property. This fact is not as easily observed when one considers the multiplication in the form presented by Hughes.

It seems appropriate to point out here a geometric consequence of the right inverse property for a V-W system. Let $F(+,\cdot)$ be a right V-W system in which the multiplicative loop has the right inverse property. Let π be the projective plane coordinatized by $F(+,\cdot)$ as in Hall [4, p. 356]. Denote by L and P respectively the sets of lines and points of π, and define mappings $\alpha: P\to P$ and $\beta: L\to L$ by

$$\begin{aligned}(a,b)^\alpha &= (b,a), & (y=xm+b)^\beta &= (y=xm^{-1}-bm^{-1}), \quad \text{if } m\neq 0,\\ (m)^\alpha &= (m^{-1}) \quad \text{if } m\neq 0, & (y=c)^\beta &= (x=c),\\ (0)^\alpha &= (\infty), & (x=c)^\beta &= (y=c),\\ (\infty)^\alpha &= (0) & (l_\infty)^\beta &= l_\infty,\end{aligned}$$

where m^{-1} is the right inverse of m in $F(+,\cdot)$. It can be shown that this pair of mappings is a collineation of π. The proof is entirely straightforward and hence will be omitted.

4. **The nuclei of certain V-W systems.** If $F(+,\cdot)$ is a V-W system we shall refer to the right, middle and left nuclei of the multiplicative loop of nonzero elements of F simply as the nuclei of the V-W system F, and they will be denoted by F_ρ, F_μ and F_λ respectively, except when it is necessary to note the operation and then they will be written $F_\rho(\cdot)$, $F_\mu(\cdot)$, $F_\lambda(\cdot)$ respectively.

THEOREM 4. *Let S be an automorphism of order t of the finite field $GF(p^n)$, L the fixed field of S, $\nu(x)=x\cdot xS\cdots xS^{t-1}$, the norm of x over L, and $\mu: L\to Z_t$ (the integers modulo t) with $\mu(1)=\mu(0)=0$. Let $H=\{x\in GF(p^n)\mid \nu(x)=1\}$, and denote by $F(+,\circ)$ the Andre V-W system obtained from $GF(p^n)$, where $x\circ y=xS^{\mu\nu(y)}\cdot y$. Then $F_\rho=F_\mu\supset H$ and $F_\lambda\cap D\supset L$, where $D=\{a\in F\mid a\circ(x+y)=a\circ x+a\circ y$ for all $x, y\in F\}$.*

Proof. Straightforward computation shows that $a \in F_\rho$ if and only if $\mu\nu(y)+\mu\nu(a)=\mu\nu(y \circ a)$ for all y in F and $a \in F_\mu$ if and only if $\mu\nu(a)+\mu\nu(y)=\mu\nu(a \circ y)$ for all y in F. Another simple computation shows that $\mu\nu(a \circ y)=\mu\nu(y \circ a)$ for all a, y in F. These two results give $F_\rho=F_\mu$. Further, if $a \in H$, then $\mu\nu(a)=0$ and $\nu(a \circ y)=\nu(aS^{\mu\nu(y)} \cdot y)=\nu(a) \cdot \nu(y)=\nu(y)$ so that $\mu\nu(a \circ y)=\mu\nu(y)$. Hence $\mu\nu(y)+\mu\nu(a)=\mu\nu(y \circ a)$ which implies $a \in F_\rho=F_\mu$. Hence $F_\rho=F_\mu \supset H$.

Again, a simple computation shows that if $a \in L$, that is, $aS=a$ then $(a \circ x) \circ y = a \circ (x \circ y)$ and $a \circ (x+y)=a \circ x+a \circ y$ for all $x, y \in F$, that is $a \in F_\lambda \cap D$. Hence $F_\lambda \cap D \supset L$.

We shall now consider a particular class of V-W systems in (C). Let $n=k_1 t$, where k_1 is a proper divisor of n, be an odd integer, and consider the field $F=GF(3^n)$. Denote by ρ a generator of the multiplicative group F' of nonzero elements of $GF(3^n)$ and let $G_1=(\rho^{3^{k_1}-1})$, $G_2=(\rho^2)$ be the subgroups of F' generated by $\rho^{3^{k_1}-1}$ and ρ^2 respectively. Let T be the automorphism of $GF(3^n)$, $x \to xT=x^3$ and define a multiplication $*$ by

$$x * y = xT^{\sigma(y)} \cdot y$$

for $x, y \in F$, where

$$\begin{aligned} \sigma(y) &= 0 && \text{if } y \in G_1, \\ &= k_1 && \text{if } y \in G_2 - G_1, \\ &= 1 && \text{if } y \notin G_2. \end{aligned}$$

It is seen that with $0 * x=x * 0=0$ for all x in F, $F(+, *)$ is a V-W system in (C).

THEOREM 5. *For the V-W system $F(+, *)$ defined above, we have $F_\rho=F_\mu=G_1$ and $F_\lambda=\{x \in F' \mid xT=x\}=\{1, -1\}$.*

Proof. A simple computation shows that $a \in F_\rho$ if and only if

$$\sigma(y)+\sigma(a) \equiv \sigma(y * a) \bmod n \tag{2}$$

holds for all y in F. Thus, let $a \in F_\rho$ and suppose $a \notin G_1$. Then either $a \in G_2-G_1$ or $a \notin G_2$. We consider these cases separately. Suppose $a \in G_2-G_1$, then $\sigma(a)=k_1$. Choose $y \notin G_2$ so that $\sigma(y)=1$. Then $y * a=yT^{k_1} \cdot a$. Now, since G_2 is the subgroup of squares of the multiplicative group of F, and $y \notin G_2$ it follows that $yT^{k_1} \notin G_2$, that is yT^{k_1} is a nonsquare of F. Since $a \in G_2$, it follows that $y * a=yT^{k_1}a$ is a nonsquare in F, that is $y * a \notin G_2$ so that $\sigma(y * a)=1$. Since $a \in F_\rho$ we have $\sigma(y)+\sigma(a) \equiv \sigma(y * a) \bmod n$. This implies that $1+k_1 \equiv 1$ or $k_1 \equiv 0 \bmod n$. This is not possible since k_1 is a proper divisor of n. Thus $a \in G_2-G_1$ leads to a contradiction. Suppose then that $a \notin G_2$, then $\sigma(a)=1$. Choose $y \in G_2-G_1$ so that $\sigma(y)=k_1$ and y is a square. Since y is a square yT is also a square and hence since a is a nonsquare we have $y * a=yT \cdot a$ a nonsquare. Hence, $y * a \notin G_2$ and $\sigma(y * a)=1$. As before, $\sigma(y)+\sigma(a) \equiv \sigma(y * a) \bmod n$ implies that $k_1 \equiv 0 \bmod n$, a contradiction. It follows that $a \in G_1$ and hence $F_\rho \subseteq G_1$.

Conversely if $a \in G_1$ then $\sigma(a)=0$ and condition (2) will hold for all $y \in F$ if and only if $\sigma(y) \equiv \sigma(y * a) \pmod{n}$ for all y in F. To see that this does indeed happen, let $y \in G_1$ then $\sigma(y)=0$ and $y * a = y \cdot a \in G_1$, since $y, a \in G_1$. Hence $\sigma(y * a)=0=\sigma(y)$ in case $y \in G_1$. Next, let $y \in G_2 - G_1$ so that $\sigma(y)=k_1$. Now, $y * a = y \cdot a \in G_2$ since $y \in G_2$ and $a \in G_1 \subset G_2$. Suppose $y * a = y \cdot a \in G_1$. Since $a \in G_1$ this implies $y \in G_1$, a contradiction. Hence $y * a \in G_2 - G_1$ and $\sigma(y * a) = k_1 = \sigma(y)$. Finally, let $y \notin G_2$ so that $\sigma(y)=1$. Again $y * a = y \cdot a$ and $y \cdot a \in G_2$ is equivalent to $y \cdot a$ a square in F. Since $a \in G_1 \subset G_2$ is also a square in F, $y \cdot a \in G_2$ implies y is a square in F, that is $y \in G_2$, a contradiction. Thus $y \cdot a \notin G_2$ and hence $\sigma(y * a)=1=\sigma(y)$. Thus condition (2) holds for all $y \in F$ and hence $a \in F_\rho$. Thus $G_1 \subseteq F_\rho$ and we have $F_\rho = G_1$.

A similar proof shows that $F_\mu = G_1$. To see that $F_\lambda = \{x \in F' \mid xT = x\} = \{1, -1\}$, we observe that $a \in F_\lambda$ if and only if

$$aT^{\sigma(x)+\sigma(y)-\sigma(x*y)} = a \tag{3}$$

for all $x, y \in F$. Clearly, $a=1$ and $a=-1$ satisfy condition (3). Conversely, let a be an element satisfying (3). Let $x = \rho^{3^{k_1}-1}$ and $y = \rho^{-1}$ (where ρ^{-1} is the inverse of ρ in F). Then $x \notin G_2$, $y \notin G_2$ so that $\sigma(x)=\sigma(y)=1$. Further $x * y = \rho^{3^{k_1}-1} * \rho^{-1} = \rho^{3^{k_1}-1} T \cdot \rho^{-1} = \rho^{3^{k_1}-1} \cdot \rho^{-1} = \rho^{3^{k_1}-1} \in G_1$ so that $\sigma(x * y)=0$. Then condition (3) implies that $aT^2 = a$. Since n is odd there exists an integer q such that $2q \equiv 1 \bmod n$. and since $aT^{2q} = a$, it follows that $aT = a$, that is $a^3 = a$. Finally since $a \neq 0$, the conclusion follows. This completes the proof of the theorem.

The next theorem is crucial to the main objective of this paper. It should be pointed out also that this next theorem can be generalized to include a much larger class of V-W systems than those of order 3^n. In fact, V-W systems in (C) which are not isotopic to any Andre V-W system can be constructed with orders p^n, where p is an odd prime and n is a nonprime integer and 2^n where n has a nonprime proper divisor. For the sake of brevity these generalizations are omitted.

THEOREM 6. *The V-W system $F(+, \cdot)$ of order 3^n, discussed in Theorem 5, is not isotopic to any Andre V-W system.*

Proof. Let $F(+, \circ)$ be an Andre V-W system of order 3^n isotopic to the V-W system $F(+, *)$ described above. Then $F(+, \circ)$ is obtained from the field $GF(3^n)$ by defining the multiplication $\circ$ in terms of the multiplication of $GF(3^n)$ by $x \circ y = xS^{\mu\nu(y)}y$ where $S = T^q$, T the automorphism $x \to x^3$ of $GF(3^n)$ and μ, ν as described earlier. We shall make use of the fact that since $F(+, *)$ and $F(+, \circ)$ are isotopic the multiplicative loops are also isotopic (this follows almost immediately from the definition of isotopy for ternary rings, see [6, p. 188]) and hence the respective nuclei are isomorphic groups (see [3, p. 57, item (i)]). By Theorem 4 $F_\rho(\circ) \supset H$, where $H = \{x \in GF(3^n) \mid \nu(x)=1\}$. Now, H may be described as the subgroup of the multiplicative group of $GF(3^n)$ generated by the elements of the form $xS \cdot x^{-1}$, and further this cyclic group is seen to be generated by ρ^{3^q-1}, where ρ is a generator

of the multiplicative group of $GF(3^n)$. For any set M, let $|M|$ be the cardinal number of M. Thus,

$$|H| = (3^n-1)/(3^q-1, 3^n-1).$$

By Theorem 5, $F_\rho(*)=G_1=(\rho^{3^{k_1}-1})$ and hence

$$|G_1| = (3^n-1)/(3^{k_1}-1).$$

Since $F_\rho(*)\cong F_\rho(\circ)\supset H$ we see that $F_\rho(*)$ contains a subgroup isomorphic to H. Hence $|H|$ divides $|G_1|$. This implies that $3^{k_1}-1$ divides 3^q-1 and hence that k_1 divides q. Thus $q=k_1\cdot f$.

Again by Theorem 4, $F_\lambda(\circ)\supset L$, the fixed field of S. Since $S=T^q$, it follows that L is the field $GF(3^q)$. Thus $F_\lambda(\circ)$ contains at least 3^q-1 elements. But $3^q-1=3^{k_1 f}-1 \geqq 3^{k_1}-1>2$, since k_1 is a proper divisor of n. Also, by Theorem 5, $F_\lambda(*)$ contains exactly two elements. Thus $F_\lambda(\circ)\cong F_\lambda(*)$ gives a contradiction and this proves the theorem.

It is our main objective to show that the translation plane π obtained from the V-W system $F(+,*)$ of order 3^n, described above, is not included among the translation planes obtained from any of the Andre V-W systems. To achieve this we digress to prove some properties of collineations of translation planes. This is done in the next section.

5. **On the collineations of translation planes.** Some of the theorems contained in this section are contained implicitly in some of the theorems in Hall [4]. Before proceeding to the main part of this section we digress further to prove two lemmas from elementary number theory, which are probably well known, but which the authors have not been able to locate in the literature.

LEMMA 1. *Let d, n, q be positive integers and p a positive prime. If d is a divisor of n with $1\leqq d<n$, and $1\leqq q<n$ then $(p^n-1)/(p^d-1)$ is not a factor of p^q-1.*

Proof. Suppose that $(p^n-1)/(p^d-1)$ is a factor of p^q-1. Then there is a positive integer k such that

$$p^q-1 = [(p^n-1)/(p^d-1)]\cdot k \quad \text{and} \quad 1 \leqq k < p^d-1. \tag{4}$$

The last inequality gives

$$p^d > k+1. \tag{5}$$

Now, let $n=d\cdot m$, so that

$$[(p^n-1)/(p^d-1)]\cdot k = [(p^d)^{m-1}+(p^d)^{m-2}+\cdots+p^d+1]\cdot k. \tag{6}$$

Equations (4) and (6) give

$$(p^d)^{m-1}\cdot k+(p^d)^{m-2}\cdot k+\cdots+p^d\cdot k+(k+1) = p^q. \tag{7}$$

Since $d<n$ we have $m\geqq 2$ and hence from (7) we obtain the inequalities

$$p^q \geqq p^d\cdot k+(k+1) > p^d$$

which imply that $d<q$. Hence p^d divides p^q. It then follows from (7) that p^d divides $k+1$, a contradiction since $p^d>k+1$. Thus, the assumption that $(p^n-1)/(p^d-1)$ is a factor of p^q-1 is false and the lemma is proved.

LEMMA 2. *Let q, n be positive integers and p a positive prime. If $(q, n)=d$ then $(p^q-1, p^n-1)=p^d-1$.*

Proof. Since d is a divisor of both q and n, we see that p^d-1 is a divisor of $k=(p^q-1, p^n-1)$. Further, $(q, n)=d$ implies that there exist integers x, y such that

$$xq+yn = d, \qquad \text{where } xy < 0.$$

Let m be a common divisor of p^q-1 and p^n-1, so that m divides k. Then

$$p^q \equiv 1 \quad \text{and} \quad p^n \equiv 1 \pmod{m}.$$

If $y<0$ then $x>0$ and we have $p^{qx}\equiv 1 \pmod{m}$. Further $p^{-yn}\equiv 1 \pmod{m}$, and hence m divides $p^{qx}-p^{-ny}$. Thus, m divides $p^{-ny}(p^d-1)$, hence, since $(m, p)=1$, we see that m is a divisor of p^d-1. Clearly, p^d-1 is a common divisor of p^q-1 and p^n-1, and the lemma is proved.

In the following theorems, unless otherwise indicated, $F(+, \cdot)$ will denote a *V-W* system and π the translation plane obtained from $F(+, \cdot)$ as in Hall [4, p. 356]. The right, middle and left nuclei of the multiplicative loop of nonzero elements of $F(+, \cdot)$ are denoted by F_ρ, F_μ, F_λ respectively. The points O, X, Y are the points of π with coordinates (0, 0), (0), (∞) respectively.

THEOREM 7. *There is a one-one correspondence between* (a) *the elements of F_ρ and the Y-OX perspectivities of π*; (b) *the elements of F_μ and the X-OY perspectivities of π*; *and* (c) *the elements of $F_\lambda \cap D$ and the O-XY perspectivities of π, with D defined as in Theorem* 4.

Proof. (a) Let σ be a *Y-OX* perspectivity of π. Since Y is the center of σ, we see that $(1, 1)^\sigma=(1, a)$ for some $a\in F$, $a\neq 0$. Since $(0, 0)^\sigma=(0, 0)$, we then see that the line $y=x$ is mapped by σ onto the line $y=xa$. Now, if $b\in F$, we see that $(b, b)^\sigma=(b, ba)$, since $(b, b)^\sigma$ is the intersection of $y=xa$ and $x=b$. Let c, $d\in F$ and (c, d) a point of π, so that (c, d), (d, d) and X are collinear. It follows that $(c, d)^\sigma$, $(d, d)^\sigma=(d, da)$ and $X^\sigma=X$ are collinear and hence, since $(c, d)^\sigma$ is also on the line $x=c$, we have $(c, d)^\sigma=(c, da)$. Further, since $(1, m)^\sigma=(1, ma)$ we see that $(m)^\sigma=(ma)$. To see that $a\in F_\rho$, let c, $m\in F$ and observe that the line $y=xm$ is mapped by σ onto the line $y=x(ma)$. Since (c, cm) is on $y=xm$, $(c, cm)^\sigma=(c, (cm)a)$ is on $y=x(ma)$. Hence $c(ma)=(cm)a$.

Conversely, let $a\in F_\rho$, and consider the mappings α, β of points into points and lines into lines, respectively, given by

$$\begin{aligned} (c, d)^\alpha &= (c, da), & (y = xm+b)^\beta &= (y = x(ma)+ba), \\ (m)^\alpha &= (ma), & (x = c)^\beta &= (x = c), \\ (\infty)^\alpha &= (\infty), & (l_\infty)^\beta &= l_\infty. \end{aligned}$$

It is easily verified that these mappings determine a Y-OX perspectivity of π. Further, it is not difficult to show that the mapping η of F_ρ onto the group of Y-OX perspectivities is one-one and onto. Indeed it can be shown that the group F_ρ is isomorphic with the group of Y-OX perspectivities.

(b) Let σ be an X-OY perspectivity of π, then clearly $(1, 1)^\sigma = (a, 1)$ for some $a \in F$, $a \neq 0$. Denote by $R(a)$, $L(a)$, respectively, the right and left multiplications by a in the multiplicative loop of F, and by aJ, the solution of the equation $a \cdot aJ = 1$. Then $aJ = 1L(a)^{-1}$. Since $(1, 1)^\sigma = (a, 1)$ we see that the line $y = x$ is mapped by σ onto the line $y = x(aJ)$, and hence that $(1)^\sigma = (aJ)$. Further we see that $(c, c)^\sigma$ is the intersection of the lines $y = c$ and $y = x \cdot aJ$, that is, $(c, c)^\sigma = (cR(aJ)^{-1}, c)$. This holds for all c in F. Since Y, (c, c) and $(c, 0)$ are collinear, we have $Y^\sigma = Y$, $(c, c)^\sigma = (cR(aJ)^{-1}, c)$ and $(c, 0)^\sigma$ collinear, thus $(c, 0)^\sigma$ is on the line $x = cR(aJ)^{-1}$. Also, since $(c, 0)$ is on the line $y = 0$, we have $(c, 0)^\sigma$ on $y = 0$ and hence $(c, 0)^\sigma = (cR(aJ)^{-1}, 0)$. It then follows that $(c, d)^\sigma = (cR(aJ)^{-1}, d)$ for all $c, d \in F$. From $(1, d)^\sigma = (1R(aJ)^{-1}, d) = (a, d)$, it follows that the line $y = xd$ is mapped by σ onto the line $y = xm$ which is incident with (a, d), so that $d = am$ or $m = dL(a)^{-1}$. Hence $(d)^\sigma = (dL(a)^{-1})$, and we now see that the line $y = xm$ is mapped onto the line $y = x(mL(a)^{-1})$, for all m in F. Let $c \in F$, then since (c, cm) is on $y = xm$ we have $(c, cm)^\sigma = (cR(aJ)^{-1}, cm)$ on $y = x(mL(a)^{-1})$. From this it follows that

$$cm = [cR(aJ)^{-1}][mL(a)^{-1}]. \tag{8}$$

Letting $c = aJ$ in (8) gives $(aJ)m = mL(a)^{-1}$, whence

$$L(a)^{-1} = L(aJ). \tag{9}$$

Replacing $L(a)^{-1}$ by $L(aJ)$ in (8) we obtain

$$cm = [cR(aJ)^{-1}][(aJ)m]. \tag{10}$$

Equation (10) with c replaced by $c(aJ)$ becomes $[c(aJ)]m = c[(aJ)m]$. Since this holds for c, m in F, we conclude that $aJ \in F_\mu$, and hence that $a \in F_\mu$.

Note that if m is replaced by a in equation (8) we get $ca = cR(aJ)^{-1}$, and hence $(c, d)^\sigma = (cR(aJ)^{-1}, d) = (ca, d)$.

Conversely, let $a \in F_\mu$, and consider the mappings α, β of points into points and lines into lines, respectively, given by

$$(c, d)^\alpha = (ca, d), \qquad (y = xm + b)^\beta = (y = x(mL(a)^{-1}) + b),$$
$$(m)^\alpha = (mL(a)^{-1}), \qquad (x = c)^\beta = (x = ca),$$
$$(\infty)^\alpha = (\infty), \qquad (l_\infty)^\beta = (l_\infty).$$

As before, it can be shown that these mappings determine an X-OY perspectivity of π, and that the mapping η of F_μ into the group of X-OY perspectivities, described here, is a one-one mapping of F_μ onto the group of X-OY perspectivities.

(c) Let σ be an O-XY perspectivity, then the line $y=x$ is fixed and we have $(1, 1)^\sigma=(a, a)$, for some $a \in F$, $a \neq 0$. Further we see that the line $x=1$ is mapped onto the line $x=a$. Then, since the line $y=xb$ is mapped onto itself, we have $(1, b)^\sigma=(a, ab)$. It follows from this that $(b, b)^\sigma=(ab, ab)$.

Now if c, $d \in F$, we see that $(c, d)^\sigma$ is the intersection of the lines joining $(d, d)^\sigma=(ad, ad)$ with X and $(c, c)^\sigma=(ac, ac)$ with Y, that is $(c, d)^\sigma=(ac, ad)$. Let c, m be arbitrary elements of F, then since the line $y=xm$ is mapped onto itself, we see that $(c, cm)^\sigma=(ac, a(cm))$ is incident with $y=xm$. Hence $a(cm)=(ac)m$ which implies that $a \in F_\lambda$. Further, if $r, s \in F$, we see that the line $y=xr+s$ is mapped by σ into the line $y=xr+as$. Since the point $(1, r+s)$ is on the line $y=xr+s$, it follows that $(1, r+s)^\sigma=(a, a(r+s))$ is on the line $y=xr+as$. Hence, $a(r+s)=ar+as$, and thus $a \in D$, whence $a \in F_\lambda \cap D$.

Finally, as in parts (a) and (b) of this theorem, we conclude that there is a one-one correspondence between the O-XY perspectivities and the elements of $F_\lambda \cap D$ by considering the O-XY perspectivity of π determined by an arbitrary element a in $F_\lambda \cap D$, and defined by the mappings α, β as follows:

$$(c, d)^\alpha = (ac, ad), \qquad (y = xm+b)^\beta = y = xm+ab,$$
$$(m)^\alpha = (m), \qquad (x = c)^\beta = (x = ac),$$
$$(\infty)^\alpha = (\infty), \qquad (l_\infty)^\beta = (l_\infty).$$

The proof, given below, for Theorem 8 is essentially contained in the proof of a theorem in Hall [4, Theorem 20.5.2, p. 367].

THEOREM 8. *Let $F(+, \cdot)$ be a V-W system, and π the corresponding translation plane. If β is a Y-O Y perspectivity of π with $X^\beta=(m)$, then $(x, y)^\beta=(x, xm+y)$ and $(n)^\beta=(n+m)$.*

Proof. Let (a, b) be a point of π not on l_∞. Then X, (a, b) and $(0, b)$ are collinear. Hence $X^\beta=(m)$, $(a, b)^\beta$ and $(0, b)^\beta=(0, b)$ are also collinear. Further, it is clear that $(a, b)^\beta$ is on the line $x=a$, and it follows that $(a, b)^\beta=(a, am+b)$. In particular, if $n \in F$, $(1, n)^\beta=(1, m+n)$; hence the line $y=xn$ is mapped onto the line $y=x(m+n)$. It follows that $(n)^\beta=(m+n)$.

In the next three theorems π is a translation plane coordinatized by a V-W system $F(+, \cdot)$ as in Theorem 8 above. The next four theorems deal with Y-OY perspectivities in such a plane.

THEOREM 9. *The translation plane π has a Y-O Y perspectivity with $X^\beta=(m)$ if and only if $a(m+b)=am+ab$ for all $a, b \in F$.*

Proof. Let β be a Y-OY perspectivity with $X^\beta=(m)$, and let a, b be arbitrary elements of F. By Theorem 8, $(a, c)^\beta=(a, am+c)$ and $(b)^\beta=(b+m)$. Let $c=ab$, then the point (a, c) is on the line $y=xb$. It follows that $(a, c)^\beta=(a, am+c)$ is on the line $y=x(b+m)$. Hence $am+c=a(b+m)$ or since $c=ab$, $am+ab=a(m+b)$.

Conversely, suppose $am+ab=a(m+b)$ for all $a, b \in F$. Define mappings β and γ of points onto points and lines onto lines respectively as follows:

$$\begin{aligned} (x, y)^\beta &= (x, xm+y), & (y = xk+b)^\gamma &= (y = x(k+m)+b), \\ (n)^\beta &= (n+m), & (x = c)^\gamma &= (x = c), \\ Y^\beta &= Y, & (l_\infty)^\gamma &= (l_\infty). \end{aligned}$$

These mappings clearly fix all of the lines on Y and all of the points on OY, and are easily seen to be one-one mappings. Suppose, (a, c) is incident with $y=xb+d$ then $c=ab+d$. It follows that $am+c=am+ab+d=a(m+b)+d$, that is $(a, c)^\beta = (a, am+c)$ is incident with $(y=xb+d)^\gamma=(y=x(b+m)+d)$. It is not difficult to see that the remaining incidences are preserved, and hence that the mappings determine a Y-OY perspectivity with X mapped into (m).

THEOREM 10. *Let π be a translation plane, as above, and $M=\{m \in F \mid \exists$ a Y-OY perspectivity β with $X^\beta=(m)\}$. Then $M(+)$ is a subgroup of $F(+)$.*

COROLLARY. *If F has order p^n then M has order p^q for some $0 \leqq q \leqq n$.*

Proof. Let $m \in M$ and β the Y-OY perspectivity with $X^\beta=(m)$. Then $X^{\beta^{-1}}=(-m)$, so that $-m \in M$. Let $n, m \in M$, and $a, b \in F$. Then $a[(m+n)+b]=a[m+(n+b)]$. By using Theorem 9 twice we have

$$a[m+(n+b)] = am+a(n+b) = am+an+ab.$$

Again by Theorem 9, $am+an=a(m+n)$. Thus,

$$a[(m+n)+b] = a(m+n)+ab,$$

which, by Theorem 9, implies $m+n \in M$. It follows that $M(+)$ is a subgroup of $F(+)$.

The corollary follows immediately from the theorem.

THEOREM 11. *Let π be a translation plane, as above, and M the subgroup of F described in Theorem* 10. *If $a \in F_0$ and $m \in M$ then $ma \in M$.*

COROLLARY. *If p^q is the order of M and r is the order of F_0 then r is a divisor of p^q-1.*

Proof. Let $m \in M$, $a \in F_0$ and $b, c \in F$. Then

$$\begin{aligned} b(ma+c) &= b[(m+ca^{-1})a] = [b(m+ca^{-1})]a \\ &= [bm+b(ca^{-1})]a = (bm)a+[b(ca^{-1})]a \\ &= b(ma)+bc. \end{aligned}$$

Thus, by Theorem 9, $ma \in M$.

To prove the corollary, let M' be the set of nonzero elements of M. Then M' has order p^q-1. Define a relation $\sim$ on M' as follows, for $m, n \in M'$ let $m \sim n$ if

and only if $m=na$ for some $a \in F\rho$. It is easily seen that $\sim$ is an equivalence relation, and that each equivalence class contains r elements. Thus, if t is the number of equivalence classes, we have $p^q-1=t\cdot r$.

THEOREM 12. *Let $F(+, \circ)$ be a finite Andre V-W system, and π the translation plane coordinatized by F. If π has a nonidentity Y-O Y perspectivity then π is Y-O Y transitive.*

Proof. Let $F(+, \circ)$ be an Andre *V-W* system of order p^n. Then, as noted earlier, the multiplication $\circ$ is given in terms of the multiplication of $F(+, \cdot)=GF(p^n)$ by $x \circ y=xS^{\mu\nu(y)}y$, where S is an automorphism of $F(+, \cdot)$, of order t, $\nu(x)=x\cdot xS\cdot xS^2 \cdots xS^{t-1}$, and μ is a mapping of K (the fixed field of S) into Z_t (the integers modulo t). Let F_ρ and F_μ be the right and middle nuclei respectively, of the multiplicative loop of nonzero elements of $F(+, \circ)$; and let $H=\{x \in F \mid \nu(x)=1\}$. By Theorem 4, $F_\rho=F_\mu \supset H$. Now, H may be described as the subgroup of the multiplicative group of nonzero elements of $F(+, \cdot)$ consisting of all elements of the form $uS\cdot u^{-1}$ (this follows from a well-known theorem on cyclic extensions, see [1, p. 200]). If ρ is a generator of the multiplicative group of $F(+, \cdot)$ and $S=T^k$, where T is the automorphism of $F(+, \cdot)$ sending x into x^p, then it is easily seen that ρ^{p^k-1} is a generator of the subgroup H. It follows that the order of H is

$$h = (p^n-1)/(p^k-1, p^n-1).$$

Let r be the order of F_ρ, then h is a divisor of r. Let $d=(k, n)$, then by Lemma 2, $h=(p^n-1)/(p^d-1)$. If π has a nonidentity *Y-O Y* perspectivity then the set M of Theorem 10 has order p^q for some integer $0<q\leqq n$. By the Corollary to Theorem 11, r is a divisor of p^q-1. It follows that $h=(p^n-1)/(p^d-1)$ is a divisor of p^q-1, and then Lemma 1 implies that either $d=n$ or $q=n$. If $d=n$, then $k=n\cdot s$, whence $S=T^{ns}=I$ which implies that the Andre *V-W* system $F(+, \circ)$ is the finite field $F(+, \cdot)$. In this case it is clear that π is *Y-O Y* transitive. If $q=n$ then M contains all of the elements of F, and hence by the definition of M, π is *Y-O Y* transitive.

The next theorem is an analogue of Theorem 12, with *Y-O Y* perspectivity replaced by *X-O X* perspectivity. This can be proved directly without reference to Theorem 12, but since it will be needed later, in another connection, the following lemma will be used to obtain a proof of the analogous theorem which follows immediately from Theorem 12.

LEMMA 3. *Let $F(+, \circ)$ be the finite Andre V-W system described in Theorem* 12, *and π the corresponding translation plane with $X=(0)$, $Y=(\infty)$, $O=(0, 0)$ and $I=(1, 1)$. If π is recoordinatized by leaving unchanged all of the coordinates of the points on OI, and permuting the coordinates of the points on $l_\infty=XY$ in such a way that $Y'=X$ is given the coordinate (∞) and $X'=Y$ is given the coordinate* (0), *then the V-W system corresponding to the new coordinates is also an Andre V-W system.*

Proof. It is clear that the new ternary ring is a *V-W* system and that the permutation of the coordinates of the points on l_∞ does not change the coordinate of the intersection of OI and XY. It is also clear that the new coordinates of (a, b) are (b, a). Further, it is easily verified that for u, v in F, $u \oplus v = v+u = u+v$, that is, the addition in $F(\oplus, *)$ is the same as in $F(+, \circ)$.

Denote by bJ the right inverse of b in the Andre *V-W* system $F(+, \circ)$. Then $1 = b \circ bJ$ whence $bJ = (b^{-1})S^{\mu\nu(bJ)}$ and $\nu(bJ) = \nu(b^{-1})$, where b^{-1} is the inverse of b in the field $F(+, \cdot)$. Thus, $bJ = (b^{-1})S^{\mu\nu(b^{-1})}$. To express the product $a * b$ in terms of the multiplication in the field $F(+, \cdot)$, let P be the point of π whose new coordinates are $(1, b)$. Then $a * b$ is the new y-coordinate of the point Q of intersection of the lines OP and $Y'A$, where $A = (a, a)$. In terms of the old coordinates we see then that $a * b$ is the (old) x-coordinate of the point Q. To determine this x-coordinate we find the equation of OP in the old coordinate system and find the x-coordinate of the intersection of this line with the line $Y'A$ whose (old) equation is $y = a$. The (old) equation of any line on 0 is of the form $y = x \circ m$. Since $P(b, 1)$ is on OP, m satisfies $1 = b \circ m$, whence $m = bJ = (b^{-1})S^{\mu\nu(b^{-1})}$. Thus, the (old) equation of OP is

$$y = x \circ [(b^{-1})S^{\mu\nu(b^{-1})}]$$

and we see that the x coordinate of Q is the solution x of $a = x \circ [(b^{-1})S^{\mu\nu(b^{-1})}]$, and hence of $a = xS^{\mu\nu(b^{-1})} \cdot (b^{-1})S^{\mu\nu(b^{-1})}$. It follows that

$$a * b = x = aS^{-\mu\nu(b^{-1})}b. \tag{11}$$

Define a mapping μ^* of the fixed field of S into the integers modulo t by

$$\begin{aligned} \mu^*(c) &= -\mu(c^{-1}) && \text{if } c \neq 0, \\ &= 0 && \text{if } c = 0. \end{aligned}$$

Then (11) becomes $a * b = aS^{\mu^*\nu(b)} \cdot b$, and it follows that $F(\oplus, *)$ is an Andre *V-W* system.

A proof for the following theorem is now obtained immediately from Theorem 12 and the preceding lemma.

THEOREM 13. *Let $F(+, \circ)$ be a finite Andre V-W system, and π the translation plane coordinatized by F. If π has a nonidentity X-OX perspectivity then π is X-OX transitive.*

6. **Translation planes obtained from the *V-W* systems in class** (C). We are now closer to the main objective of this paper, which is to show that the translation plane obtained from the *V-W* system of order 3^n, discussed in Theorem 5, is not isomorphic to any of the translation planes obtained from the Andre *V-W* systems. The remaining sequence of theorems will show that such an isomorphism implies that our new *V-W* system is isotopic with some Andre *V-W* system, which by Theorem 6 is not possible.

THEOREM 14. *Let π be a translation plane relative to $l_\infty = X_1 Y_1$. Let O_1, X_1, Y_1 and O_2, X_2, Y_2 be two triples of noncollinear points with $O_1 = O_2$, $Y_1 = Y_2$, and $X_2 \neq X_1$, where X_2 is incident with $l_\infty = X_1 Y_1$. Let F_1 and F_2 be the V-W systems obtained from π using the quadruples O_1, X_1, Y_1, I_1 and O_2, X_2, Y_2, I_2 respectively (where I_1, I_2 are arbitrary, except that $O_i X_i Y_i I_i$ contains no collinear triple, $i = 1, 2$). Further, let r_1, r_2 be the orders of $F_{1\rho}$, $F_{2\rho}$ respectively, where $F_{i\rho}$ is the right nucleus of the multiplicative loop of F_i. If π has no nonidentity $Y_1 - O_1 Y_1$ perspectivity then the line $O_1 Y_1$ contains at least $r_1 r_2 + 2$ points.*

Proof. Let P be a point on $O_1 Y_1$, $O_1 \neq P \neq Y_1$, and for $i = 1, 2$ let α_i be a $Y_1 - O_1 X_1$ perspectivity and β_i a $Y_2 - O_2 X_2$ perspectivity of π. Then $P^{\alpha_i \beta_i}$ is incident with $O_1 Y_1$ and $O_1 \neq P^{\alpha_i \beta_i} \neq Y_1$. Suppose that $P^{\alpha_1 \beta_1} = P^{\alpha_2 \beta_2}$, then $P^{\alpha_1 \beta_1 \beta_2^{-1} \alpha_2^{-1}} = P$. Now, $\alpha_1 \beta_1 \beta_2^{-1} \alpha_2^{-1}$ is a collineation of π which fixes Y_1 and every line on Y_1. Further $\alpha_1 \beta_1 \beta_2^{-1} \alpha_2^{-1}$ fixes the point O_1. It follows that $\alpha_1 \beta_1 \beta_2^{-1} \alpha_2^{-1}$ is a perspectivity of π with center Y_1 and axis some line on O_1. If the axis is $O_1 Y_1$, then $\alpha_1 \beta_1 = \alpha_2 \beta_2$ since the only Y_1-$O_1 Y_1$ perspectivity of π is the identity. If the axis is not $O_1 Y_1$, then $\alpha_1 \beta_1 \beta_2^{-1} \alpha_2^{-1}$ is a perspectivity which fixes a point, P, different from the center Y_1 and not on the axis. This also implies that $\alpha_1 \beta_1 \beta_2^{-1} \alpha_2^{-1}$ is the identity and hence we have $\alpha_1 \beta_1 = \alpha_2 \beta_2$. It follows that $\alpha_1^{-1} \alpha_2 = \beta_1 \beta_2^{-1}$, and hence that $X_1 = X_1^{\alpha_1^{-1} \alpha_2} = X_1^{\beta_1 \beta_2^{-1}}$. Thus, $\beta_1 \beta_2^{-1}$ is a Y_2-$O_2 X_2$ perspectivity of π which fixes the point X_1 not on the axis $O_2 X_2$ and different from the center Y_2. It follows that $\beta_1 = \beta_2$ and hence $\alpha_1 = \alpha_2$.

Let $\mathfrak{M} = \{Q \mid Q = P^{\alpha_j \beta_k}$, α_j, β_k Y_1-$O_1 X_1$, Y_2-$O_2 X_2$ perspectivities of $\pi\}$. By Theorem 7, we see that j runs from 1 to r_1 and k from 1 to r_2. The argument above shows that the images of P under the $r_1 r_2$ perspectivities $\alpha_j \beta_k$ are $r_1 r_2$ distinct points of $O_1 Y_1$, that is, the cardinal number of $\mathfrak{M}$ is $r_1 r_2$. Since $\mathfrak{M}$ does not include the points O_1 and Y_1 we see, finally, that $O_1 Y_1$ contains at least $r_1 r_2 + 2$ distinct points.

THEOREM 15. *Let π be a translation plane relative to $l_\infty = X_1 Y_1$. Let $O_1 X_1$, Y_1 and O_2, X_2, Y_2 be two triples of noncollinear points with $O_1 = O_2$, $X_1 = X_2$, $Y_1 \neq Y_2$, where Y_2 is incident with $l_\infty = X_1 Y_1$. As in Theorem* 14, *let F_1 and F_2 be the V-W systems obtained from π using the quadruples O_1, X_1, Y_1, I_1 and O_2, X_2, Y_2, I_2 respectively. Further, let $F_{1\rho}$, $F_{2\rho}$, r_1, r_2 be the same as in Theorem* 14. *If π has no nonidentity X_1-$O X_1$ perspectivity then there are at least $r_1 r_2 + 2$ distinct lines on the point $X_1 = X_2$.*

A proof for Theorem 15 can be obtained essentially by dualizing the arguments used in the proof of Theorem 14.

Before proceeding it is necessary to state several results which will be referred to in proving the next theorem.

(i) A right Andre *V-W* system in which the left distributive law holds is a field [2, p. 185].

(ii) If π is the translation plane obtained from a right Andre *V-W* system which

is not a field, then π has no nontrivial Y-OY perspectivities. This follows from Theorem 12 and one part of the proof of a theorem in [4, Theorem 20.5.2, p. 367]. In view of Lemma 3, it is seen further that π has no nontrivial X-OX perspectivities.

(iii) Under any isomorphism of two proper translation planes, the lines at infinity correspond, [4, p. 372].

(iv) If F_1 and F_2 are ternary rings and π_1, π_2 the corresponding projective planes, and if σ is an isomorphism of π_1 with π_2 such that $O_1^\sigma = O_2$, $X_1^\sigma = X_2$, $Y_1^\sigma = Y_2$ (where $O_i = (0, 0)$, $X_i = (0)$, $y_i = (\infty)$ in π_1, π_2 respectively) then F_1 and F_2 are isotopic. See [6, Theorem 3.3.1, p. 189].

This last result will be referred to, in the sequel, as Knuth's theorem on isotopy. We are now prepared to prove the next theorem.

THEOREM 16. *Let F_1 be a finite proper Andre V-W system and π_1 the translation plane obtained from F_1. Let $O_1 = (0, 0)$, $X_1 = (0)$, and $Y_1 = (\infty)$. Similarly, let F_2 be a V-W system and π_2 the corresponding translation plane, with $O_2 = (0, 0)$, $X_2 = (0)$, and $Y_2 = (\infty)$. If either the right or middle nucleus, $F_{2\rho}$ or $F_{2\mu}$ of the multiplicative loop of F_2 is nontrivial, and if σ is an isomorphism of π_1 onto π_2 with $O_1^\sigma = O_2$ and either $X_1^\sigma = X_2$ or $Y_1^\sigma = Y_2$ then $X_1^\sigma = X_2$ and $Y_1^\sigma = Y_2$, and F_2 is isotopic to F_1.*

COROLLARY. *Let F_1, π_1, O_1, $X_1 Y_1$ be defined as in the theorem, then any collineation of π_1 which fixes O_1 and either X_1 or Y_1 fixes both X_1 and Y_1.*

Proof. Suppose first that $Y_1^\sigma = Y_2$. To see that this implies $X_1^\sigma = X_2$, assume the contrary. Then we have $Y_1^\sigma = Y_2$ and $X_1^\sigma \neq X_2$. Now, since π_1 is not Y_1-$O_1 Y_1$ transitive by remark (ii) above, it follows that π_2 is not Y_2-$O_2 Y_2$ transitive. However, since either $F_{2\rho}$ or $F_{2\mu}$ is nontrivial, Theorem 7 implies the existence of a perspectivity of π_2 which fixes O_2 and Y_2 (and also X_2) and takes X_1^σ into a point $X_3 \neq X_1^\sigma$, where X_3 is incident with $X_2 Y_2$ and $X_3 \neq X_2$.

Let F_3 and F_4 be the V-W systems obtained by using as a basis for coordinates the triples $O_2 Y_2 X_1^\sigma$ and $O_2 Y_2 X_3$ respectively. Then by Knuth's theorem, remark (iv) above, each of F_1, F_3, F_4 is isotopic to the other. Hence the right nuclei $F_{1\rho}$, $F_{3\rho}$, $F_{4\rho}$ of the multiplicative loops, respectively, are isomorphic groups.

The multiplication in F_1 is given by $x \circ y = xS^{\mu\nu(y)} \cdot y$, where the multiplication on the right is that of the field $F_1(+, \cdot) = GF(p^n)$ (see Theorem 4). Let T be the automorphism $xT = x^p$ of $F_1(+, \cdot)$. Then $S = T^q$. With H as defined in Theorem 4, we have, by Theorem 4, that H is a subgroup of the right nucleus $F_{1\rho}$. As noted earlier, H is identical with the subgroup of the multiplicative group of the field $F_1(+, \cdot)$ generated by the elements of the form $xS \cdot x^{-1}$, and hence H is generated by $\rho^{p^q - 1}$, where ρ is a generator of the multiplicative group of the field $F_1(+, \cdot)$. Thus the order of H is

$$(p^n - 1)/(p^q - 1, p^n - 1) = (p^n - 1)/(p^d - 1)$$

where $d = (q, n)$. Now, let r be the order of $F_1\rho$ and we see that $(p^n - 1)/(p^d - 1)$ is a divisor of r.

Since $F_{3\rho}$ and $F_{4\rho}$ are each isomorphic to $F_{1\rho}$, they also have order r, and since π_3 has no nontrivial Y_2-O_2Y_2 perspectivity, we may apply Theorem 14 to π_2, using the triples O_2, Y_2, X_1^σ and O_2, Y_2, X_3, to conclude that the line O_2Y_2 contains at least r^2+2 points. Since $(p^n-1)/(p^d-1)$ is a divisor of r, we have

$$r \geqq (p^n-1)/(p^d-1).$$

Let $n=d\cdot d_1$. Since F_1 is a proper Andre V-W system we see that $S=T^q\neq I$ and hence that q is not a multiple of n. Thus $d=(q, n)<n$, and consequently $d_1>1$. It follows that

$$p^n-1 = [(p^d)^{d_1-1}+(p^d)^{d_1-2}+\cdots+p^d+1](p^d-1) \geqq (p^d+1)(p^d-1).$$

Combining these last two inequalities, we obtain

$$r^2 \geqq \frac{p^n-1}{p^d-1}\cdot\frac{p^n-1}{p^d-1} \geqq \frac{p^n-1}{p^d-1}\cdot\frac{(p^d+1)(p^d-1)}{p^d-1} = (p^n-1)\frac{p^d+1}{p^d-1} > p^n-1,$$

where the last inequality follows from $(p^d+1)/(p^d-1)>1$. We see then that the line O_2Y_2 contains at least $r^2+2>p^n+1$ points. This contradicts the fact that π_2 is a plane of order p^n and hence that O_2Y_2 contains exactly p^n+1 points. The contradiction implies then that $X_1^\sigma=X_2$.

A proof similar to the above, using Theorem 15 instead of Theorem 14, shows that if $X_1^\sigma=X_2$ then $Y_1^\sigma=Y_2$. In either case, the fact that F_2 is isotopic to F_1 follows from Knuth's theorem on isotopy.

Proof of the Corollary. Since a finite Andre V-W system has nontrivial nuclei, the corollary follows from the Theorem by considering the collineation as an isomorphism of π_1 onto itself.

THEOREM 17. *Let F_1, F_2, π_1, π_2 and the points O_1, X_1, Y_1, O_2, X_2, Y_2 be defined as in Theorem* 16. *If σ is an isomorphism of π_1 onto π_2 with $O_1^\sigma=O_2$, and either $X_1^\sigma=Y_2$ or $Y_1^\sigma=X_2$ then the other holds and F_2 is isotopic to some Andre V-W system whose nuclei have the same orders as the nuclei of F_1.*

Proof. Suppose that $X_1^\sigma=Y_2$. Change the coordinates in π_1 as in Lemma 3. Then $X_1'=Y_1$ and $Y_1'=X_1$. Let F_1^* be the V-W system obtained from the new coordinates. Then, by Lemma 3, F_1^* is also an Andre V-W system. Further, $(Y_1')^\sigma=X_1^\sigma=Y_2$. It follows from Theorem 16 that $(X_1')^\sigma=X_2$. Hence F_2 is isotopic to F_1^* by Knuth's theorem on isotopy [6, Theorem 3.3.1, p. 189]. A simple calculation shows that $F_{1\lambda}=F_{1\lambda}^*$. The X_1-O_1Y_1 perspectivities of π_1 are the same as the Y_1'-O_1X_1' perspectivities and hence $F_{1\mu}$ and $F_{1\rho}^*$ have the same orders. Finally, by Theorem 4, $F_{1\rho}=F_{1\mu}$ and $F_{1\rho}^*=F_{1\mu}^*$, and we see that the nuclei of F_1^* have the same orders, respectively, as the nuclei of F_1.

The same argument, with an obvious modification, is valid in case $Y_1^\sigma=X_2$.

THEOREM 18. *Let F be a finite proper Andre V-W system, as described in Theorem* 4, *and π the corresponding translation plane. If $a, b\in F$, $a\neq 0\neq b$ and $\mu\nu(a)\neq\mu\nu(b)$ then there is a collineation α of π such that $O^\alpha=O$, $(a)^\alpha=(a)$ and $(b)^\alpha\neq(b)$.*

Proof. With the notation of Theorem 4, the multiplication in the Andre system $F(+, \circ)$ is given, in terms of the multiplication in the field $F(+, \cdot)=GF(p^n)$, by $x \circ y = xS^{\mu\nu(y)} \cdot y$, where $S=T^q$. T the automorphism $xT=x^p$ of $F(+, \cdot)$. Let ρ be a generator of the multiplicative group of $F(+, \cdot)$. The subgroup H, of all elements of the form $xS \cdot x^{-1}$, $x \neq 0$, is generated by ρ^{p^q-1}. Let $d=(n, q)$, $n=n_1 d$, $q=q_1 d$, then the order t, of S, is given by $t=n/d=n_1$. Since $F(+, \circ)$ is a proper Andre V-W system, $0<q<n$.

First, it will be shown that if

$$(\rho^{p^q-1})S^l = \rho^{p^q-1}, \tag{12}$$

then $S^l=I$, the identity automorphism. Thus, suppose, on the contrary, that (12) holds for some integer l, with $0<l<t$. Since $p^d-1=(p^q-1, p^n-1)$, we see that the linear congruence $(p^q-1)x \equiv (p^d-1) \bmod (p^n-1)$ has a solution $x=r$. Raising both sides of (12) to the rth power we obtain

$$(\rho^{p^d-1})S^l = \rho^{p^d-1}. \tag{13}$$

Now let $S_1=T^d$, then $S=T^q=S_1^{q_1}$, and hence $S^l=S_1^{q_1 l}=S_1^h$, where $0<h<n_1$, since $S^l=S_1^h \neq I$. Thus, from (13) we obtain

$$(\rho^{p^d-1})S_1^h = \rho^{p^d-1}. \tag{14}$$

Equation (14) gives $\rho^{(p^d-1)(p^{dh}-1)}=1$, which implies that p^n-1 is a divisor of $(p^d-1)(p^{dh}-1)$. Thus we have, for some positive integer s,

$$(p^n-1)s = (p^d-1)(p^{dh}-1). \tag{15}$$

From (15) we obtain $s+1=p^n s-p^{d+dh}+p^{dh}+p^d$, which implies that p^d divides $s+1$, whence

$$p^d \leqq s+1. \tag{16}$$

Since $0<h<n_1=n/d$, we have $0<hd<n$. This implies that $p^{dh}<p^n$. Using this inequality in (15) we see that $(p^n-1)s<(p^d-1)(p^n-1)$. Then $p^d-1>s$ or $p^d>s+1$, which contradicts (16). This proves that (12) implies $S^l=I$.

Since $\mu\nu(a) \neq \mu\nu(b)$, $\mu\nu(a)-\mu\nu(b)$ is a nonzero element of Z_t. Let l be the least positive integer such that $l \equiv \mu\nu(a)-\mu\nu(b) \bmod t$. Then $0<l<t$ and hence $S^l \neq I$. For brevity, let $c=\rho^{p^q-1}$ and $d=cS^{\mu\nu(a)}$. Then, since c, $d \in H \subset F_\rho = F_\mu$, it follows from Theorem 7 that there exists a Y-OX perspectivity, β, of π associated with d, and an X-OY perspectivity γ associated with c, such that, for $m \in F$, $(m)^\beta=(m \circ d)$ and $(m)^\gamma=(mL(c)^{-1})=(mL(cJ))$, where $L(c)$ is the left multiplication in the loop of nonzero elements of $F(+, \circ)$, and cJ is the right inverse of c in this loop.

Let $\alpha=\beta\gamma$. Since β and γ both fix the point O, we have $O^\alpha=O$. Further, $(a)^\alpha=(a)^{\beta\gamma}=(a \circ d)^\gamma=(cJ \circ (a \circ d))=((cJ \circ a) \circ d)$, since $d \in F_\rho$. Also, since $c \in H$, $cJ=c^{-1}$, the multiplicative inverse of c in the field $F(+, \cdot)$. Thus, we have

$$(a)^\alpha = ((cJ \circ a) \circ d) = (c^{-1}S^{\mu\nu(a)} \cdot a \cdot d) = (a).$$

A similar computation gives $(b)^\alpha=(c^{-1}S^{\mu\nu(b)}\cdot b\cdot d)$, and $b=c^{-1}S^{\mu\nu(b)}\cdot b\cdot d$ implies $cS^{\mu\nu(b)-\mu\nu(a)}=c$, or $(\rho^{p^q-1})S^l=\rho^{p^q-1}$, which is impossible since $S^l\neq I$. Thus α is the desired collineation.

THEOREM 19. *Let F and π be defined as in Theorem* 18. *If $a, b\in F$, $a\neq 0\neq b$, and if there is a collineation of π such that $X^\alpha=(a)$ and $Y^\alpha=(b)$, then $\mu\nu(a)=\mu\nu(b)$.*

Proof. It is clear that α fixes the line $l_\infty=XY$ and hence if α moves O, there is a translation τ such that $O^{\alpha\tau}=O$. Also, $X^{\alpha\tau}=(a)$ and $Y^{\alpha\tau}=(b)$. Let $\beta=\alpha\tau$ and suppose that $\mu\nu(a)\neq\mu\nu(b)$. Then by the previous theorem there is a collineation γ such that $O^\gamma=O$, $(a)^\gamma=a$, and $(b)^\gamma=(c)\neq(b)$. Consider the collineation $\beta\gamma\beta^{-1}$. Clearly $\beta\gamma\beta^{-1}$ fixes the point O and $X^{\beta\gamma\beta^{-1}}=X$, $Y^{\beta\gamma\beta^{-1}}=(c)^{\beta^{-1}}\neq Y$, since $Y^\beta=(b)\neq(c)$. This contradicts the corollary to Theorem 16 and hence $\mu\nu(a)=\mu\nu(b)$.

We are now prepared to prove that the translation plane of order 3^n obtained from the V-W system $F(+,*)$, discussed in Theorem 5, cannot be coordinatized by any Andre V-W system. To prove this, suppose the contrary, and denote by F_2 the V-W system $F(+,*)$ of order 3^n, and by π_2 the corresponding translation plane. Let $O_2=(0,0)$, $X_2=(0)$, $Y_2=(\infty)$ in π_2. Denote by $F_1(+,\circ)$ an Andre V-W system which coordinatizes π_2 and let π_1 be the translation plane obtained from $F_1(+,\circ)$. Let $O_1=(0,0)$, $X_1=(0)$, $Y_1=(\infty)$ in π_1. Then there is an isomorphism σ of π_1 onto π_2 which sends the line X_1Y_1 onto the line X_2Y_2. We may suppose that $O_1^\sigma=O_2$ for otherwise there is a translation τ of π_2 sending O_1^σ into O_2 and $\sigma\tau$ is also an isomorphism of π_1 onto π_2.

Because the isomorphism $\sigma\colon\pi_1\to\pi_2$ sends O_1 into O_2 and X_1Y_1 into X_2Y_2, there is a 1-1 correspondence between the O_1-X_1Y_1 perspectivities of π_1 and the O_2-X_2Y_2 perspectivities of π_2. From Theorems 5 and 7 it follows that the order of $F_{1\lambda}\cap D_1$ is two, where $D_1=\{a\in F_1 \mid a\circ(x+y)=a\circ x+a\circ y \text{ for all } x, y\in F_1\}$ and $F_{1\lambda}$ is the left nucleus of the multiplicative loop of $F_1(+,\circ)$. By Theorem 4, we have $F_{1\lambda}\cap D_1\supset L=\{x\in F_1 \mid x\neq 0 \text{ and } xS=x\}$, where S is the automorphism of the field $GF(3^n)$ used to define the multiplication in $F_1(+,\circ)$. Since L contains ± 1 and $F_{1\lambda}\cap D_1$ contains only two elements, we have $F_{1\lambda}\cap D_1=L=\{\pm 1\}$. It follows that S has order n.

Now, consider the images of X_1, Y_1 under σ. If this set, $\{X_1^\sigma, Y_1^\sigma\}$, contains either X_2 or Y_2, then from Theorems 16 and 17 it follows that it contains both. Theorems 16 and 17 are applicable since $F_1(+,\circ)$ is a proper Andre V-W system, for otherwise $F_2(+,*)$ is the field $GF(3^n)$, a contradiction. However, if $\{X_1^\sigma, Y_1^\sigma\}=\{X_2, Y_2\}$, then it follows from Theorems 16 and 17 that F_2 is isotopic to F_1, which contradicts Theorem 6. Thus, $\{X_1^\sigma, Y_1^\sigma\}\cap\{X_2, Y_2\}=\varnothing$, and we have $X_2^{\sigma^{-1}}=(a)$, $Y_2^{\sigma^{-1}}=(b)$, where $a, b\in F_1$, $a\neq 0\neq b$. By Theorem 5, $F_{2\rho}=F_{2\mu}=G_1$, where G_1 is the subgroup of the multiplicative group of $GF(3^n)$ generated by $\rho^{3^{k_1}-1}$. Thus $F_{2\rho}$ and $F_{2\mu}$ each contain $(3^n-1)/(3^{k_1}-1)$ elements. Now, since k_1 is a proper divisor of n, we have $(3^n-1)/(3^{k_1}-1)=3^{k_1(t-1)}+3^{k_1(t-2)}+\cdots+3^{k_1}+1>2$. It follows from Theorem 7 that π_2 possess at least two nontrivial X_2-O_2Y_2 perspectivities and at least two

nontrivial Y_2-O_2X_2 perspectivities. The isomorphism $\sigma^{-1}: \pi_2 \to \pi_1$ then enables one to induce at least two nontrivial (a)-$O_1(b)$ or (b)-$O_1(a)$ perspectivities of π_1. Let us consider the (b)-$O_1(a)$ perspectivities, and let γ be a nontrivial one. If $X_1^\gamma = Y_1$ or $Y_1^\gamma = X_1$ then it follows from Theorem 17 that γ interchanges X_1 and Y_1. If γ_1 and γ_2 both interchange X_1 and Y_1 then γ_1^2, γ_2^2 and $\gamma_1\gamma_2$ each fix both X_1 and Y_1. It follows that $\gamma_1^2 = \gamma_2^2 = \gamma_1\gamma_2 = 1$, whence $\gamma_1 = \gamma_2$. Since there are at least two nontrivial (b)-$O_1(a)$ perspectivities, it follows that there is at least one, say β, such that $Y_1^\beta = (c)$ and $X_1^\beta = (d)$ where $c, d \in F_1$ and $c \neq 0 \neq d$. Then from Theorem 19 we have $\mu\nu(c) = \mu\nu(d)$.

We shall now show that $\nu(c) \neq \nu(d)$. Suppose the contrary, then $\nu(cd^{-1}) = 1$, where cd^{-1} is the product in the field $GF(3^n)$ of c and the field inverse of d. Thus $cd^{-1} \in H = \{xS \cdot x^{-1} \mid x \in F_1, x \neq 0\} \subset F_{1\rho}$. Let α be the Y_1-O_1X_1 perspectivity of π_1 associated with cd^{-1}, as in Theorem 7. Then $(d)^\alpha = (d \circ (cd^{-1})) = (dS^{\mu\nu(cd^{-1})} \cdot cd^{-1}) = (c)$, and $(c)^\alpha = (c \circ (cd^{-1})) = (c \cdot cd^{-1}) = (e)$. To compute e, consider the collineation $\beta\alpha\beta^{-1}$ of π_1. Clearly $O_1^{\beta\alpha\beta^{-1}} = O_1$, and further $X_1^{\beta\alpha\beta^{-1}} = (d)^{\alpha\beta^{-1}} = (c)^{\beta^{-1}} = Y_1$. Then Theorem 17, with $F_2 = F_1$, $\pi_2 = \pi_1$ and $\sigma = \beta\alpha\beta^{-1}$, implies that $Y_1^{\beta\alpha\beta^{-1}} = X_1$. Hence $Y_1^{\beta\alpha} = X_1^\beta$ and we have $Y_1^{\beta\alpha} = (c)^\alpha = (e) = X_1^\beta = (d)$, that is $e = d$. We see then that $c^2d^{-1} = e = d$, whence $c^2 = d^2$, and hence, since $c \neq d$, that $c = -d$. Thus, $cd^{-1} = -1$, and $\nu(cd^{-1}) = \nu(-1) = -1$, since S has order n and n is odd. This contradiction proves that $\nu(c) \neq \nu(d)$.

It was noted earlier that the fixed field of the automorphism S is $GF(3)$. It follows that for any nonzero x in F_1, $\nu(x) = \pm 1$. Since c, d are nonzero elements of F_1, with $\nu(c) \neq \nu(d)$, we see that one of $\nu(c)$, $\nu(d)$ is 1 and the other -1. Finally, since $\mu\nu(c) = \mu\nu(d)$ we have $\mu(-1) = \mu(1) = 0$, and hence $\mu\nu(x) = 0$ for all $x \in F_1$. This implies that the Andre V-W system $F_1(+, \circ)$ is the field $GF(3^n)$, a contradiction. This contradiction proves the desired result.

References

1. A. A. Albert, *Modern higher algebra*, Univ. of Chicago Press, Chicago, Ill., 1937.

2. J. Andre, *Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe*, Math Z. **60** (1954), 156–186.

3. R. H. Bruck, *A survey of binary systems*, Ergebnisse der Math., Heft 20, Springer, Berlin, 1958.

4. Marshall Hall, Jr., *The theory of groups*, Macmillan, New York, 1959.

5. D. R. Hughes, *Review of some results in collineation groups*, Proc. Sympos. Pure Math., Vol. 1, Amer. Math. Soc., Providence, R. I., 1959.

6. D. E. Knuth, *Finite semifields and projective planes*, J. Algebra **2** (1965), 182–217.

7. T. G. Ostrom, *Translation planes and configurations in Desarguesian planes*, Arch. Math. **11** (1960), 457–464.

University of Missouri,
St. Louis, Missouri
University of Missouri,
Columbia, Missouri