PACIFIC JOURNAL OF MATHEMATICS
Vol. 36, No. 3, 1971

TRANSLATION PLANES CONSTRUCTED FROM SEMIFIELD PLANES

NORMAN L. JOHNSON

Let π be an affine plane of order q^2 that is coordinatized by a "derivable" semifield $\mathscr{S} = (\mathscr{S}, +, \cdot)$. If $(\mathscr{S}, +)$ is a right vector space over $F = GF(q)$ then a plane π' may be constructed from π using Ostrom's method of "derivation."

The purpose of this article is to examine the planes π' and their coordinate structures $(\mathscr{S}, +, *)$. It is shown, in particular, that $(\mathscr{S}, +, *)$ is a (right) quasifield which is neither a nearfield nor a semifield. Furthermore, it is shown that π' is always of Lenz-Barlotti class IVa. 1.

The automorphism groups of semifields of square order are also briefly investigated.

1. The Construction of Quasifields from Derivable Semifields. We will assume that the reader is familiar with the concept of "derivation." For background material the reader is referred to [2], [4], [6], and [7].

DEFINITION 1.1. A semifield $\mathscr{S} = (\mathscr{S}, +, \cdot)$ of order q^2, $q = p^r$, p a prime, will be said to be *derivable* if and only if $(\mathscr{S}, +)$ is a vector space over $GF(q) = F$ where $F \subseteq \mathscr{S}$ and $x \cdot \alpha = x\alpha$ (or $\alpha \cdot x = \alpha x$) is scalar product.

If a semifield $\mathscr{S}$ is derivable then either $\mathscr{S}$ or dual $\mathscr{S}$ (i.e., right multiplication becomes left multiplication, and conversely) is a right vector space over $GF(q)$ and hence either the affine plane π coordinatized by $\mathscr{S}$ or an affine restriction of the dual of the projective extension of π is derivable (see sections 3 and 4, [7]).

A projective plane is a semifield plane if and only if it can be coordinatized by a semifield or if and only if the plane is $(P, \underline{l})$-transitive $\forall$ points $P \in \underline{l}$, and $(\underline{Q}, l)$-transitive $\forall$ lines $l \in \underline{Q}$ and $\underline{Q} \in \underline{l}$.

If $\underline{Q}, \underline{l}$ are chosen to be (∞) and l_∞, respectively, then the coordinate structure obtained is a semifield. In dualizing the semifield plane π we shall let $(\infty) \leftrightarrow l_\infty$ and then delete l_∞ to obtain an affine plane coordinatized by a semifield dual to a semifield which coordinatizes π.

DEFINITION 1.2. Let $\mathscr{S} = (\mathscr{S}, +, \cdot)$ be a derivable semifield. $\mathscr{S}$ is *subcommutative* if and only if $a\alpha = \alpha a$ for all $a \in \mathscr{S}$ and for all $\alpha \in GF(q)$.

DEFINITION 1.3. A semifield $\mathscr{S}$ of order q^2 containing $GF(q)$ is

a weak nucleus semifield (*wn*-semifield) if and only if $(ab)c = a(bc)$ whenever any two of a, b, c are in $GF(q)$.

Note that a *wn*-semifield of order q^2 is derivable and a derivable subcommutative semifield is a *wn*-semifield.

Let $\mathscr{S}$ be a derivable semifield which is a *right* 2-dimensional vector space over $GF(q)$. Let $\{1, t\}$, $t \in \mathscr{S} - GF(q)$ be a basis for $\mathscr{S}$ over $GF(q)$.

Then let $\beta(t\alpha) = th(\beta, \alpha) + k(\beta, \alpha)$ and $(t\alpha)(t\beta) = tf(\alpha, \beta) + g(\alpha, \beta)$ for $\alpha, \beta \in GF(q)$ where h, k, f, g are bilinear functions: $GF(q) \times GF(q) \to GF(q)$ which introduce no zero divisors into the multiplication.

Then multiplication in the semifield is given by:

$$(t\alpha + \delta)(t\beta + \gamma) = t(f(\alpha, \beta) + h(\delta, \beta) + \alpha\gamma) + (g(\alpha, \beta) + k(\delta, \beta) + \delta\gamma) .$$

Thus, if $\mathscr{S}$ is any derivable semifield then either the multiplication of $\mathscr{S}$ or dual $\mathscr{S}$ is of the above form.

THEOREM 1.4. *Let $\mathscr{S} = (\mathscr{S}, +, \cdot)$ be a derivable semifield which is a right vector space of dimension 2 over $F = GF(q)$, $q = p^r$, p a prime. Let the multiplication in $\mathscr{S}$ be given by:*

$$(t\alpha + \delta) \cdot (t\beta + \gamma) = t(f(\alpha, \beta) + h(\delta, \beta) + \alpha\gamma) + (g(\alpha, \beta) + k(\delta, \beta) + \delta\gamma) \; \forall \; \alpha, \beta, \delta, \gamma \in F$$

where f, h, g, k are bilinear functions: $F \times F \to F$.

Define a system $\mathscr{S}^* = (\mathscr{S}, +, *)$ when the $*$-multiplication is given by

$$t * \alpha = t\alpha, \; (t\alpha + \beta) * \gamma = t(\alpha\gamma) + \beta\gamma \quad \text{and if } \delta \neq 0$$

$(t\alpha + \beta) * (t\delta + \gamma) = t\rho + \chi$ where

(1) $h(\delta, \mu_1) = 1$,

(2) $k(\delta, \mu_1) + \delta\mu_2 = \gamma$,

(3) $f(\alpha, \mu_1) + h(\rho, \mu_1) + \alpha\mu_2 = \beta$,

(4) $g(\alpha, \mu_1) + k(\rho, \mu_1) + \rho\mu_2 = \chi$

$\forall \alpha, \beta, \delta \neq 0, \gamma \in F$ where μ_1, μ_2 and thus $\rho, \chi \in F$ are determined from the above equations.

Then $\mathscr{S}^* = (\mathscr{S}, +, *)$ is a (right) quasifield.

Proof. The affine plane π coordinatized by $\mathscr{S}$ is derivable (see [2], [6], [7]). Ostrom [6] has shown that the plane π' derived from π is a translation plane and may be coordinatized by a system

$$(\mathscr{S}, +, *) \ni t\alpha = t * \alpha, \; (t\alpha + \beta) * (t\delta + \gamma) = t\rho + \chi$$

if and only if $(t\alpha + \rho)(t\mu_1 + \mu_2) = t\beta + \chi$ where $\delta(t\mu_1 + \mu_2) = t + \gamma$ for $\delta \neq 0$, and $(t\alpha + \beta) * \gamma = (t\alpha + \beta)\gamma$ for all $\alpha, \beta, \delta, \gamma \in GF(q)$. Our equations are obtained by merely equating vector components.

We shall now specialize (1.4) to the case where $\mathscr{S}$ is a *wn*-semifield.

Knuth [4] has shown that if $\mathscr{S}$ is a *wn*-semifield then a basis $\{1, t\}$ can be chosen so that $\alpha t = t\alpha^\sigma \forall \alpha \in GF(q)$ where σ is some automorphism of $GF(q)$. In this case, $h(\delta, \beta) = \delta^\sigma\beta$ and $k(\delta, \beta) = 0$ for all $\delta, \beta \in GF(q)$.

Thus $h(\delta, \mu_1) = \delta^\sigma\mu_1 = 1$ implies $\mu_1 = \delta^{-\sigma}$ and $k(\delta, \mu_1) + \delta\mu_2 = \gamma$ implies that $\mu_2 = \delta^{-1}\gamma$ for $\delta \neq 0$. Thus $f(\alpha, \mu_1) + h(\rho, \mu_1) + \alpha\mu_2 = \beta$ implies that $f(\alpha, \delta^{-\sigma}) + \rho^\sigma\delta^{-\sigma} = \alpha\delta^{-1}\gamma = \beta$. Hence

$$\rho = ((\beta - f(\alpha, \delta^{-\sigma}) - \alpha\delta^{-1}\gamma)\delta^\sigma)^{\sigma^{-1}} = (\beta - f(\alpha, \delta^{-\sigma}) - \alpha\delta^{-1}\gamma)^{\sigma^{-1}}\delta .$$

Also, $g(\alpha, \mu_1) + k(\rho, \mu_1) + \rho\mu_2 = \chi$ implies that $g(\alpha, \delta^{-\sigma}) + \rho\delta^{-1}\gamma = \chi$.

Thus, we have the following theorem.

THEOREM 1.5. *If $\mathscr{S} = (\mathscr{S}, +, \cdot)$ is a weak nucleus semifield of order $q^2 \ni$ multiplication in $\mathscr{S}$ is given by*

$$(t\alpha + \delta)(t\beta + \gamma) = t(f(\alpha, \beta) + \delta^\sigma\beta + \alpha\gamma) + (g(\alpha, \beta) + \delta\gamma) .$$

Define a system $\mathscr{S}^* = (\mathscr{S}, +, *)$ by defining a $*$-multiplication as follows:

$$t * \alpha = t\alpha, (t\alpha + \delta) * (t\beta + \gamma) = t(\delta - f(\alpha, \beta^{-\sigma}) - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\beta + g(\alpha, \beta^{-\sigma}) + (\delta - f(\alpha, \beta^{-\sigma}) - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\gamma$$

for $\delta \neq 0$ and σ an automorphism of $GF(q)$, and

$$(t\alpha + \delta) * \gamma = (t\alpha + \delta)\gamma \forall \alpha, \beta, \delta, \gamma \in GF(q) .$$

Then $\mathscr{S}^*$ is a (right) quasifield.

REMARKS 1.6. Under the assumptions of (1.5)

(i) $\alpha * a = a * \alpha^{\sigma^{-1}} \forall \alpha \in GF(q)$ and $\forall a \in \mathscr{S} - GF(q)$,

(ii) $(a * b) * c = a * (b * c)$ whenever any two of a, b, c are in $GF(q)$.

Proof. The proof of (1.6) is routine and is left to the reader.

2. Automorphisms of derivable semifields which fix $GF(q)$ elementwise. The semifields of order 16 have been tabulated, [3], and are all isotopic (Sec. 3, [4]) to one of two weak nucleus semifields, each of which admits a group of automorphisms of order 3 which fixes $GF(q)$ elementwise (see [4]). The multiplications for the

two systems are given by $(t\alpha)(t\delta) = t\alpha^{2}\delta^{2} + \alpha^{2}\delta$, $\beta t = t\beta^{2} \forall \alpha, \delta, \beta \in GF(4)$ and $(t\alpha)(t\delta) = \omega\alpha^{2}\delta$, $\beta t = t\beta^{2}$ where ω is a primitive root of $GF(4)$.

The semifields of order 16 are exceptions among derivable semifields of order q^{2} in that no derivable semifield of order q^{2}, $q > 4$ can admit such automorphism groups.

THEOREM 2.1 *Let $(\mathscr{S}, +, \cdot)$ be a derivable proper semifield of order q^{2}. Then $\mathscr{S}$ is of order 16 if and only if a derivable isotopic image of $\mathscr{S}$ admits a group of automorphisms of order $q - 1$ which fixes $GF(q)$ elementwise.*

Proof. Suppose the indicated automorphisms τ_{ρ} that the form $t^{\tau}\rho = t\rho \forall \rho \in GF(q) - \{0\}$. (Note: This would be true by (2.2) if $\mathscr{S}$ is a *wn*-semifield and $\sigma \neq 1$, but we are not necessarily assuming this property.) If $\mathscr{S}$ is a left vector space over $GF(q)$, consider dual $\mathscr{S}$. Let $\{1, t\}$ be a basis for $\mathscr{S}$ or dual $\mathscr{S}$.

$((t\alpha)(t\beta))^{\tau\rho} = (tf(\alpha, \beta) + g(\alpha, \beta))^{\tau\rho}$ where f, g are bilinear functions: $GF(q) \times GF(q) \to GF(q)$. Thus,

$$(t(\rho\alpha))(t(\rho\beta)) = t(\rho f(\alpha, \beta)) + g(\alpha, \beta)$$

which implies that $\rho f(\alpha, \beta) = f(\rho\alpha, \rho\beta)$ and $g(\alpha, \beta) = g(\rho\alpha, \rho\beta)$. Since we have $q - 1$ automorphisms τ_{ρ} these previous equations are true for all $\alpha, \beta, \rho \in GF(q) - \{0\}$. If characteristic $F \neq 2$ then $g(2\rho, 2\rho) = g(2, 2)$. But g is bilinear so $g(2, 2) = 4g(1, 1)$. Also $g(\alpha, \alpha) = g(1, 1)$ so that $4g(1, 1) = g(1, 1)$. Moreover $g(1, 1) \neq 0$ since $t^{2} = tf(1, 1) + g(1, 1)$ and multiplication of nonzero elements is a loop.

Hence $4 \equiv 1$ so that characteristic $F = 3$.

Since $g(\rho\alpha, \rho\beta) = g(\alpha, \beta) \forall \alpha, \beta, \rho \in GF(q) - \{0\}$ then

$$g(1, (\alpha + \gamma)^{-1}) = g(\alpha + \gamma, 1) = g(\alpha, 1) + g(\gamma, 1)$$

for $\alpha + \gamma \neq 0$.

Thus, $g(1, (\alpha + \gamma)^{-1}) - (g(\alpha, 1) + g(\gamma, 1)) = 0$, which implies that $g(1, (\alpha + \gamma)^{-1}) + 2(g(\alpha, 1) + g(\gamma, 1)) = 0$.

Clearly, $2g(\beta, 1) = g(2\beta, 1) \forall \beta \in GF(q)$, and $g(2\beta, 1) = g(1, 2\beta^{-1})$, so

$$\begin{aligned} g(1, (\alpha + \gamma)^{-1}) &+ g(2\alpha, 1) + g(2\gamma, 1) \\ &= g(1, (\alpha + \gamma)^{-1}) + g(1, 2\alpha^{-1}) + g(1, 2\gamma^{-1}) \\ &= g(1, (\alpha + \gamma)^{-1} + 2\alpha^{-1} + 2\gamma^{-1}) \\ &= g(1, (\alpha + \gamma)^{-1} - (\alpha^{-1} + \gamma^{-1})) . \end{aligned}$$

If $(\alpha + \gamma)^{-1} \neq \alpha^{-1} + \gamma^{-1}$, then

$$t(t((\alpha + \gamma)^{-1} - (\alpha^{-1} + \gamma^{-1})) = tf(1, (\alpha + \gamma)^{-1} - (\alpha^{-1} + \gamma^{-1}))$$

which cannot be the case. Hence $(\alpha + \gamma)^{-1} = \alpha^{-1} + \gamma^{-1}$. It is easy to see that in this situation $GF(q) = GF(3)$.

But then $\mathscr{S}$ would be a field ([4], p. 208) contrary to our assumption.

Hence, characteristic $F = 2$. Then, using the bilinearity of g we may argue as before (except that $-1 = +1$) to obtain $(\alpha + \gamma)^{-1} = \alpha^{-1} + \gamma^{-1}$ from which it follows that $GF(q) = GF(4)$.

To complete the proof of (2.1) we must show that the automorphisms τ_ρ have the form $t^\tau\rho = t\rho$.

Let π be the affine plane coordinatized by $\mathscr{S}$ and let π_0 be the subplane of π coordinatized by $GF(q)$.

The automorphism group of $\mathscr{S}$ induces a collineation group of π which fixes π_0 pointwise. In the derived plane there is a collineation group of order $q - 1$ fixing the line $\{(x, y) \mid x = 0\}$ pointwise. (The validity of this last statement may be seen by choosing coordinates for the derived plane so that π_0 in π is the point set $\{(x, y) \mid x = 0\}$ in the derived plane. See e.g. [6], Theorem 10.)

Thus, the derived plane π' admits a $(P, x = 0)$-homology group of order $q - 1$ (see [2], remarks following (2.6)). Moreover, this group must fix the set points of π_0' on the line at infinity of the derived plane where π_0' is the line $x = 0$ in π (see [6], Theorem 7). Hence, $P = (\alpha)$ where $\alpha \in GF(q)$. If $\alpha \neq 0$ we can rechoose t in $\mathscr{S}$ so that P is represented by (0).

Now $\{(t\delta + \alpha\delta, t\beta + \alpha\beta)\}$ in π is the same as $\{(t\delta + \beta, t\alpha\delta + \alpha\beta)\}$ in π' ([6], Theorem 10). If we let $t = t + \alpha$ then $\{(t\delta, t\beta)\}$ is $\{(t\delta + \beta, 0)\}$ in π'. Hence, we have relabeled $\{(x, y) \mid y = x\alpha\}$ in π' by $\{(x, y) \mid y = 0\}$. Thus, $P = (\alpha)$ is relabeled by (0).

Now a group of $((0), x = 0)$-collineations which fix π_0' induce automorphisms of the form $\tau_\rho \ni (t\alpha + \beta)\tau_\rho = t(\rho\alpha) + \beta$ in $\mathscr{S}$ (see [2], (2.10), and the proof of (3.10)).

Hence (2.1) is proved.

PROPOSITION 2.2. *Let $(\mathscr{S}, +, \cdot)$ be a wn-semifield of order q^2 with multiplication defined by $(t\alpha)(t\beta) = tf(\alpha, \beta) + g(\alpha, \beta)$, $\delta t = t\delta^\sigma$, σ an automorphism of $GF(q)$, $\forall \alpha, \beta, \delta \in GF(q)$. If $\sigma \neq 1$, and if τ is any automorphism of $(\mathscr{S}, +, \cdot)$ fixing $GF(q)$ elementwise then $(t\alpha + \beta)^\tau = t(\rho\alpha) + \beta$ for some $\rho \in GF(q)$.*

Proof. $(\alpha t)^\tau = \alpha^\tau t^\tau = \alpha t^\tau$. Let $t^\tau = t\rho + \theta$ for some $\rho, \theta \in GF(q)$. Then $\alpha t^\tau = t\alpha^\sigma\rho + \alpha\theta$ and $(\alpha t)^\tau = (t\alpha^\sigma)^\tau$, $t^\tau\alpha^\sigma = t\rho\alpha^\sigma + \theta\alpha^\sigma$. Hence, $\alpha\theta = \theta\alpha^\sigma$ which implies $\theta = 0$.

THEOREM 2.3. *If a derivable semifield $\mathscr{S} = (\mathscr{S}, +, \cdot)$ of order q^2, $q > 2$ admits a nontrivial automorphism group $\mathscr{G}$ which fixes*

$GF(q) = F$ elementwise and $|\mathscr{G}|\,|q$ then $\mathscr{G}$ is an elementary abelian 2-group whose order is strictly less than q.

Proof. Without loss of generality, suppose that $(\mathscr{S}, +)$ is a *right* vector space over F. Then it follows directly from [5], Theorem 1, that if $\tau \in \mathscr{G}$ and $\{1, t\}$ is a basis for $(\mathscr{S}, +)$ over F then $t^\tau = t + \gamma$ for some $\gamma \in F$.

Let $\delta(t\beta) = th(\delta, \beta) + k(\delta, \beta)$,

$$(t\alpha)(t\beta) = tf(\alpha, \beta) + g(\alpha, \beta) \forall \alpha, \beta, \delta \in GF(q)$$

where f, g, h, k are bilinear functions: $GF(q) \times GF(q) \to GF(q)$.

Then, $(t\alpha)(t\beta)^\tau = (tf(\alpha, \beta) + g(\alpha, \beta))^\tau$ if and only if

$$(t\alpha)(t\beta) + t(h(\gamma\alpha, \beta) + \alpha\gamma\beta) + k(\gamma\alpha, \beta) + \gamma^2\alpha\beta = (t\alpha)(t\beta) + \gamma f(\alpha, \beta)\,.$$

Equating vector components:

(1) $h(\gamma\alpha, \beta) = -\alpha\gamma\beta \forall \alpha, \beta$ and

(2) $k(\gamma\alpha, \beta) + \gamma^2\alpha\beta = \gamma f(\alpha, \beta)$.

If $\alpha = \gamma^{-1}$ in (1), then $h(1, \beta) = -\beta$. But, $h(1, \beta) = \beta$. $\therefore$ F is of characteristic 2. Thus, $\mathscr{G}$ is an elementary abelian 2-group.

Now assume $|\mathscr{G}| = q$. Then, by (2), $k(1, \beta) + \gamma\beta = \gamma f(\gamma^{-1}, \beta) = \gamma\beta$ so that $f(\gamma^{-1}, \beta) = \beta$ for all $\gamma \in F$. But

$$f(\mathscr{N}^{-1} + \gamma^{-1}, \beta) = f(\mathscr{N}^{-1}, \beta) + f(\gamma^{-1}, \beta) = 0$$

since f is bilinear and F is of characteristic 2.

Hence, (2.3) is proved.

COROLLARY 2.4. *If $\mathscr{S} = (\mathscr{S}, +, \cdot)$ is a wn-semifield of order q^2 which admits a nontrivial automorphism group $\mathscr{G}$ such that $|\mathscr{G}|\,|q$ then $|\mathscr{G}| = 2$.*

Proof. By (2.3)(2), $k(\gamma\alpha, \beta) + \gamma^2\alpha\beta = \gamma f(\alpha, \beta)$.

We may choose $t \in \mathscr{S} - F \ni k(\gamma\alpha, \beta) \equiv 0 \forall \alpha, \beta, \gamma \in F$ so $\gamma^2\alpha\beta = \gamma f(\alpha, \beta) \Rightarrow \gamma\alpha\beta = f(\alpha, \beta)$. Clearly $|\mathscr{S}| = 2$ for otherwise it would follow that $\gamma\alpha\beta = \mathscr{N}\alpha\beta$ for $\gamma \neq \mathscr{N} \forall \alpha, \beta \in F$.

COROLLARY 2.5. *If $\mathscr{S} = (\mathscr{S}, +, \cdot)$ is a wn-semifield which admits a group $\mathscr{G}$ of* (2.4) *then there is a $t \in \mathscr{S} - F$ such that*

$$(t\alpha + \delta)(t\beta + \gamma) = t(\alpha\beta f + \delta\beta + \alpha\gamma) + (g(\alpha, \beta) + \delta\gamma)$$

where g is a bilinear function $F \times F \to F$ and f is a nonzero constant in F.

Proof. $\exists t \in \mathscr{S} - F \ni \alpha t = t\alpha^{\sigma} \forall \alpha \in F$, σ an automorphism of F. By (2.2), $\sigma = 1$. By (2.4), $|\mathscr{S}| = 2$ and if $\tau \in \mathscr{S} \ni t^{\tau} = t + ff(\alpha, \beta) = \alpha\beta f$.

COROLLARY 2.6. *Let* $(\mathscr{S}, +, \cdot)$ *satisfy the hypothesis of* (2.3) *and* $(\mathscr{S}, +, *)$ *the quasifield of* (1.4). *Consider the following distributive law*:

$$c * (\alpha + b) = c * \alpha + c * b$$

for all $c, b \in \mathscr{S}$ *and for some* $\alpha \in F$.

Then

(i) if $\operatorname{char} F \neq 2$ this distributive law cannot hold for any nonzero $\alpha \in F$,

(ii) if $\operatorname{char} F = 2$ and $(\mathscr{S}, +, \cdot)$ is a *wn*-semifield then the distributive law holds for at most a single nonzero element of F,

(iii) if $\operatorname{char} F = 2$ this distributive law cannot hold for all $\alpha \in F$.

Thus, in particular, $(\mathscr{S}, +, *)$ is not a semifield.

Proof. The given distributive law induces a $((\infty), x = 0, \pi_0)$-collineation in the affine plane coordinatized by $(\mathscr{S}, +, *)$ and hence ([2], see the proof of (3.10)) an automorphism group in $(\mathscr{S}, +, \cdot)$ as in (2.3).

We have seen that $(\mathscr{S}, +, *)$, if $\mathscr{S}$ is a *wn*-semifield, admits some associative properties ((1.6) (ii)). In general, however, we note that $(\mathscr{S}, +*)$ cannot be associative.

THEOREM 2.7. *If* $\mathscr{S} = (\mathscr{S}, +, \cdot)$ *is a derivable semifield* $\ni (\mathscr{S}, +)$ *is a right vector space over* $GF(q)$ *then* $(\mathscr{S}, +, *)$ *is neither associative nor distributive.*

Proof. The affine plane coordinatizing $(\mathscr{S}, +, \cdot)$ is $((\infty), x = 0, \pi_0)$-transitive ([2], [6]) and thus $(\mathscr{S}, +, *)$ admits a group of automorphisms of order q which fix $GF(q)$ elementwise. But regular nearfields clearly cannot admit such automorphisms. The irregular nearfields all have order p^2 where p is a prime. If $\mathscr{S}$ has order p^2 then $\mathscr{S}$ is a field ([4]) in which case $(\mathscr{S}, +, *)$ is a quasifield which coordinatizes a Hall plane.

3. The Knuth multiplication. Let $(\mathscr{S}, +) = (GF(q^2), +)$. Let $t \in \mathscr{S} - GF(q)$ and define $\alpha t = t\alpha^{\sigma}$ where σ is an automorphism of $GF(q)$. The functions $f(\alpha, \beta) = \alpha^{\mathscr{N}}\beta^{\chi}f$, $g(\alpha, \beta) = \alpha^{\rho}\beta^{\delta}g$ where $\mathscr{N}, \chi, \rho, \delta$ are automorphisms of $GF(q)$, $\alpha, \beta \in GF(q)$, f, g constants in $GF(q)$ are bilinear functions: $GF(q) \times GF(q) \to GF(q)$.

$$\alpha t = t\alpha^{\sigma}, (t\alpha)(t\beta) = t\alpha^{\mathscr{N}}\beta^{\chi}f + \alpha^{\rho}\beta^{\delta}g$$

will define multiplication of a semifield $\mathscr{S} = (\mathscr{S}, +, \cdot)$ provided no zero divisors are introduced by the choices of $\sigma, \mathscr{N}, \chi, \rho, \delta, f$ and g. If no zero divisors occur, we shall say that the semifield so defined is a Knuth Semifield.

THEOREM 3.1. (*Knuth* [4]). *Let*

$$\mathscr{S} = (\mathscr{S}, +, \cdot) \ni (\mathscr{S}, +) = GF(q^2)$$

and

$$(t\alpha + \delta)(t\beta + \gamma) = t[\alpha^{\mathscr{N}}\beta^{\chi}f + \alpha\gamma + \delta^{\sigma}\beta] + [\alpha^{\rho}\beta^{\delta}g + \delta\gamma] \forall \alpha, \beta, \delta, \gamma \in GF(q)$$

where $\mathscr{N}, \chi, \sigma, \rho, \delta$ are automorphisms of $GF(q)$ and f, g elements of $GF(q)$.

(a) *If $f = 0$ and g is a nonsquare in $GF(q)$ then the above multiplication defines a Knuth Semifield for an arbitrary choice of automorphisms σ, ρ, δ.*

That is, $\alpha t = t\alpha^{\sigma}$, $(t\alpha)(t\beta) = \alpha^{\rho}\beta^{\sigma}g$ for arbitrary automorphisms ρ, δ of $GF(q)$ and g a nonsquare in $GF(q)$ define a semifield.

(b) *If $f \neq 0$ and σ, f, g are chosen so that $y^{\sigma+1} + fy - g = 0$ has no solutions in $GF(q)$ and $(\mathscr{N}, \chi, \rho, \delta) = (\sigma, \sigma^{-1}, \sigma, \sigma^{-2}), (\sigma, 1, \sigma, 1), (1, \sigma^{-1}, \sigma^{-1}, \sigma^{-2})$ or $(1, 1, \sigma^{-1}, 1)$ then the above multiplication defines a Knuth Semifield. That is, each of the following multiplications define a class of semifields*:

I. $\alpha t = t\alpha^{\sigma}$, $(t\alpha)(t\beta) = t\alpha^{\sigma}\beta^{\sigma^{-1}}f + \alpha^{\sigma}\beta^{\sigma^{-2}}g$

II. $\alpha t = t\alpha^{\sigma}$, $(t\alpha)(t\beta) = t\alpha^{\sigma}\beta f + \alpha^{\sigma}\beta g$

III. $\alpha t = t\alpha^{\sigma}$, $(t\alpha)(t\beta) = t\alpha\beta^{\sigma^{-1}}f + \alpha^{\sigma^{-1}}\beta^{\sigma^{-2}}g$

IV. $\alpha t = t\alpha^{\sigma}$, $(t\alpha)(t\beta) = t\alpha\beta f + \alpha^{\sigma^{-1}}\beta g$.

Furthermore, Knuth [4] has characterized types II, III and IV in terms of the nuclei.

DEFINITION 3.2. Let $(Q, +, \cdot)$ be a ternary system. Let

$$\{x \in Q \mid (ab)x = a(bx) \forall a, b \in Q\} = \mathscr{N}_{\mathscr{R}Q},$$
$$\{x \in Q \mid (ax)b = a(xb) \forall a, b \in Q\} = \mathscr{N}_{\mathscr{M}Q},$$
$$\{x \in Q \mid (xa)b = x(ab) \forall a, b \in Q\} = \mathscr{N}_{\mathscr{L}Q},$$

$\mathscr{N}_{\mathscr{R}Q}, \mathscr{N}_{\mathscr{M}Q}, \mathscr{N}_{\mathscr{L}Q}$ will be called the *right*, *middle*, and *left nucleus* of Q, respectively.

THEOREM 3.3. (*Knuth* [4]). *Let $(\mathscr{S}, +, \cdot)$ be a Knuth Semifield of order q^2. Then $GF(q) = \mathscr{N}_{\mathscr{R}\mathscr{S}} = \mathscr{N}_{\mathscr{M}\mathscr{S}}$ if and only if $\mathscr{S}$ is of type II. $GF(q) = \mathscr{N}_{\mathscr{L}\mathscr{S}} = \mathscr{N}_{\mathscr{M}\mathscr{S}}$ if and only if $\mathscr{S}$ is of type III, and $GF(q) = \mathscr{N}_{\mathscr{L}\mathscr{S}} = \mathscr{N}_{\mathscr{R}\mathscr{S}}$ if and only if $\mathscr{S}$ of type IV.*

By applying (1.4) to (3.1), we obtain the following result:

THEOREM 3.4. *Each of the following multiplications* $*$ *(with field addition) defines a (right) quasifield which is neither a semifield or nearfield. If* $\beta \neq 0$,

(1) $(t\alpha + \delta) * (t\beta + \gamma) = t(\delta - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\beta + (\delta - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\gamma + \alpha^{\mathcal{N}}\beta^{-\sigma\chi}g$, g *a nonsequare in* F

(2) $(t\alpha + \delta) * (t\beta + \gamma) = t(\delta - \alpha^{\sigma}\beta^{-1}f - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\beta + (\delta - \alpha^{\sigma}\beta^{-1}f - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\gamma + \alpha^{\sigma}\beta^{-\sigma^{-1}}g$, $\sigma \neq 1$, $f \neq 0$

(3) $(t\alpha + \delta) * (t\beta + \gamma) = t(\delta - \alpha^{\sigma}\beta^{-\sigma}f - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\beta + (\delta - \alpha^{\sigma}\beta^{-\sigma}f - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\gamma + \alpha^{\sigma}\beta^{-\sigma}g$, $\sigma \neq 1$, $f \neq 0$

(4) $(t\alpha + \delta) * (t\beta + \gamma) = t(\delta - \alpha\beta^{-1}f - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\beta + (\delta - \alpha\beta^{-1}f - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\gamma + \alpha^{\sigma^{-1}}\beta^{\sigma^{-1}}g$, $\sigma \neq 1$, $f \neq 0$

(5) $(t\alpha + \delta) * (t\beta + \gamma) = t(\delta - \alpha\beta^{-\sigma}f - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\beta + (\delta - \alpha\beta^{-\sigma}f - \alpha\beta^{-1}\gamma)^{\sigma^{-1}}\gamma + \alpha^{\sigma^{-1}}\beta^{-\sigma}g$, $\sigma \neq 1$, $f \neq 0$.

Also, $(t\alpha + \delta) * \gamma = t(\alpha\gamma) + \delta\gamma$ *where* σ *is an automorphism of* F *and in cases* (2) *through* (5) $y^{\sigma+1} + fy - g \neq 0 \forall y \in GF(q)$ *and* $\mathcal{N}$, χ *automorphisms of* F *in case* (1).

Proof. See (1.4), (2.7) and (3.1).

4. **The planes coordinatized by the $(\mathcal{S}, +, *)$ quasifields.** A plane Σ is of Lenz-Barlotti Class IV.a.2 or IV.a.3 if Σ can be coordinatized by a (right) nearfield, and of Class V.1 if Σ can be coordinatized by a semifield. Σ is of Class IV.a.1 if Σ is coordinatized by (right) quasifield but no coordinate system for Σ is a (right) nearfield or semifield.

The planes coordinatized by the $(\mathcal{S}, +, *)$ quasifields are therefore of L-B Classes IV.a.1, a.2, a.3, or V.

THEOREM 4.1. *Let* $\mathcal{S} = (\mathcal{S}, +, \cdot)$ *be a derivable semifield* $\ni (\mathcal{S}, +)$ *is a right vector space over* $GF(q)$. *Let* π *be the semifield plane coordinatized by* $\mathcal{S}$. π *is derivable, so let* π' *be the plane derived from* π. *Then* π' *is of Lenz-Barlotti Class* IV.a.1.

Proof. We must show that π' cannot be of type IV.a.2, a.3, or V.1.

Suppose π' is of type V.1, then π' is $((m), l)$-transitive for all lines l incident with (m) where mIl_∞. By (2.7), $(m) \neq (\infty)$ since $\mathcal{S}^* = (\mathcal{S}, +, *)$ is not a semifield. Clearly (m) is fixed by the full collineation group of π' (otherwise π' is Desarguesian and every coordinatizing structure is a field). Recall (see proof of (2.7)), $\mathcal{S}^*$ admits an automorphism

group of order q fixing F pointwise such that $t \to t + \alpha$ for all $\alpha \in F$ (see (2.3) and (2.7)). Hence, $m \in F$ if π' is $((m), l)$-transitive.

We consider two cases:

$$(1) \quad (m) = (0), \qquad (2) \quad m \neq (0) .$$

Case (1). If $(m) = (0)$, consider changing coordinates as follows in $\mathscr{S}$ (in π):

$$(tx_1 + x_2, ty_1 + y_2) \xrightarrow{\text{coordinate change } \sigma} (tx_2 + x_1, ty_2 + y_1) \forall x_1, x_2, y_1, y_2 \in F .$$

$\mathscr{S}\sigma$ is a derivable semifield (see [2], the proofs of (3.6) and (3.7)).

The coordinate change appears as $(x, y) \to (y, x)$ in π' (see [2], (3.7)) and thus induces a Hall coordinate system $\mathscr{S}_{\mathscr{R}}^* \ni \pi'$ is $((\infty), x = 0)$-transitive. $\therefore$ $\mathscr{S}_{\mathscr{R}}^*$ is a (derivable) semifield. However, $\mathscr{S}_{\mathscr{R}}^*$ is constructed from $\mathscr{S}_{\mathscr{R}} = \mathscr{S}^\sigma$ in the same manner that $\mathscr{S}^*$ is constructed from $\mathscr{S}$. $\therefore$ we have a contradiction by (2.7).

(2) $(m) \neq (0)$.

Choose $\bar{t} = t + m$ (recall $m \in F$) in $(\mathscr{S}, +, \cdot)$. Then in π'

$$(y = xm) = \{(x, y) \mid x = t\alpha + \beta, y = t(\alpha m) + (\beta m)\}$$

is the same as $\{(t\alpha + \alpha m, t\beta + \beta m) = (\bar{t}\alpha, \bar{t}\beta)\} \equiv y = 0$ in π'. Hence, by case (1) we have a contradiction.

Assume that π' is of type IV.a.2 or a.3. Then π' is $((P), (Q))$-transitive for some pair of points (P), (Q), $P \neq Q$.

Moreover, every collineation of π' must fix $\{(P), (Q)\}$. Therefore, since $\mathscr{S}^*$ admits an automorphism group of order q it must be that $P, Q \in F$ or $P, Q = \infty$.

Now if we can change coordinates so that $\mathscr{S}_{\mathscr{R}}^*$ is a nearfield and $\mathscr{S}_{\mathscr{R}}^*$ admits an automorphism group of order q, then we have a contradiction since the order of an automorphism group of a nearfield of order $q^2 (q = p^r, r > 1)$ is never this large.

Let $(P) = (\alpha)$ and $(Q) = (\beta)$, $\alpha, \beta \in F$ or $\alpha, \beta = \infty$.

Case (1). $(\alpha) = (\infty)$. Since $\mathscr{S}^*$ is not a nearfield (see (2.7)), $(\beta) \neq (0)$. We can rechoose t in $\mathscr{S}$ (in π) so that $y = x\beta$ is $y = 0$ in π' (i.e., if $\bar{t} = t + \beta$) and (∞) in π' is left fixed. $\therefore$ $\mathscr{S}^*$ with the basis $\{1, \bar{t}\}$ is a nearfield and admits q automorphisms.

Case (2). $(\alpha) \neq (\infty)$, $(\beta) \neq (\infty)$, $(\alpha) = (0)$. We can move (0) to (∞) by the $(x, y) \to (y, x)$ coordinate change of $\mathscr{S}^*$ of the previous argument. Therefore, π' is $((\infty), (\gamma))$-transitive for $(\gamma) \neq (0)$. Then, we may rechoose t in $\mathscr{S}_{\mathscr{R}}$ so that (γ) is (0) in $\mathscr{S}_{\mathscr{R}}^*$ (or in π'). Since $\mathscr{S}_{\mathscr{R}}$ is a (derivable) semifield, $\mathscr{S}_{\mathscr{R}}^*$ admits an automorphism group of

order q which is a contradiction.

Case (3). $(\alpha), (\beta) \neq (\infty)$ or (0). First rechoose t in $\mathscr{S}$ so that (α) is (0), then repeat Case 2.

REMARKS. If $(\mathscr{S}, +, \cdot)$ is a derivable subcommutative semifield then a "derivable chain" (see [1]) can be constructed based on the affine plane coordinatized by $(\mathscr{S}, +, \cdot)$.

$(\mathscr{S}, +, \cdot)$ actually need not be finite to construct $(\mathscr{S}, +, *)$. That is, Ostrom's "derivation process" extends for infinite translation planes. We shall explore this in a later paper.

REFERENCES

1. N. L. Johnson, *Derivable chains of planes*, Bol. Un. Mat. Ital. N. 2, (1970) 167-184.
2. ———, *Derivable semi-translation planes*, Pacific J. Math., **34** (1970).
3. E. Kleinfeld, *Techniques for enumerating Veblen-Wedderburn systems*, J. Assoc. Comput. Math., **7** (1960), 330-337.
4. D. E. Knuth, *Finite semifields and projective planes*, J. Algebra, **2** (1965), 182-217.
5. D. L. Morgan and T. G. Ostrom, *Coordinate systems of some semi-translation planes*, Trans. Amer. Math. Soc., **111** (1964), 19-32.
6. T. G. Ostrom, *Semi-translation planes*, Trans. Amer. Math. Soc., **111** (1964), 1-18.
7. ———, *Vector spaces and construction of finite projective planes*, Arch. Math., **19** (1968), 1-25.

Received June 3, 1970.

UNIVERSITY OF IOWA