Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 1–21

Primitive Semifields and Fractional Planes of order q^5

MINERVA CORDERO – VIKRAM JHA

Dedicated to Professor Marialuisa de Resmini

ABSTRACT: *The dimension of an affine plane π of order n, relative to a subplane π_0 of order m, is specified by $\dim_{\pi_0} \pi = \log_m n$. The exotic embeddings of a plane in another plane of the "wrong" characteristic, pioneered by H. Neumann, and systematically considered by de Resmini and her associates, yield planes with transcendental dimensions. On the other hand, infinitely many rational but non-integral dimensional, or fractional, planes were discovered relatively recently and all known examples of such planes are among semifield planes. Such semifield planes must have order $\geq p^5$, p prime. We show:*

Theorem A: Let π be a semifield plane of order p^5, that contains no fractional subplanes. Then for sufficiently large p, every semifield coordinatizing π is right primitive and left primitive.

Here, a semifield $(D, +, \circ)$ is considered right primitive if every non-zero element in D is the right principal power of some $\omega_R \in D$; left primitivity is defined analogously. G. P. Wene Conjectured that all fractional semifields are right primitive. If the fractional hypothesis on π is dropped, counterexamples to the Conjecture are known to arise in semifield planes of order 2^5 and 2^6, as shown by I. F. Rúa and I. R. Hentzel. These are the only known orders for which the Wene Conjecture fails. We provide further support for the Wene Conjecture.

Theorem B: All semifields coordinatizing semifield flock spreads are right primitive.

We also prove the 3-dimensional analogue of this result.

Theorem C: Let π be a semifield spread in $PG(5, q)$ such that $\pi \supset \mathcal{R}$, a regulus of degree $q + 1$ such that the shears axis $Y \in \mathcal{R}$. Then for all sufficiently large q, every semifield coordinatizing π is right primitive.

This result extends a Theorem of Rúa who showed that semifields D of order q^3 that are three-dimensional over the center Z, hence, by Menichetti's Theorem, are Albert semifields with center $GF(q)$, are right primitive and left primitive. The Theorem above is not restricted to such Albert systems.

KEY WORDS AND PHRASES: *Semifields – Spreads – Flocks – Loops – Translation planes*
A.M.S. CLASSIFICATION: 51A40, 17A35.

1 – Introduction

In this paper, we consider two properties of a finite affine plane π that might be considered as reflecting the extent to which π differs from, or is similar to, a Desarguesian plane of the same order. One of these properties, related to the "dimension" that π may have relative to its subplanes, identifies planes that have subplanes of unexpected orders. The other property, which is algebraic in nature, is concerned with the loop structure of the "best" planar ternary rings, that coordinatize any considered π. The basic question here is whether planar ternary rings that are "closest" to fields, viz., quasifields and semifields, have multiplicative loops that are "cyclic", hence share the "primitivity" property of finite fields.

We begin with a brief survey of the notion of dimension, and how it derives from Professor de Resmini's pioneering investigations concerning exotic embeddings of one plane in another.

– Fractional-Dimensional Planes

Bearing in mind that the dimension of a finite field $F = GF(q^n)$, over a subfield $K = GF(q)$, is the integer $\log_{|K|} |F|$, one may more generally define the dimension of an arbitrary finite plane with respect to any subplane. For our convenience we state the Definition for affine rather than projective planes.

DEFINITION 1.1. Let Π be an affine plane of order n, with an affine subplane Ψ of order m. Then the dimension of Π relative to Ψ is specified by $\dim_\Psi \Pi = \log_m n$.

In particular, Π has transcendental dimension, fractional dimension, or integer dimension, relative to Ψ, according to whether $\log_m n$ is transcendental, rational (but not an integer), or an integer.

Similarly if D is a planar ternary ring with a subplanar ternary ring E then $\dim_E D = \log_{|E|} |D|$; D is transcendental, fractional or integer dimensional, relative to E, according to whether $\dim_E D$ is transcendental, rational but not an integer, or an integer.

In the 1950's, H. Neumann [19], showed that any projective Hall plane Π of odd order contains Fano subplanes. It follows that infinitely many affine planes are transcendental dimensional over suitable subaffine planes.

PROPOSITION 1.2. *To each square integer p^{2n}, p an odd prime, corresponds an affine Hall plane Π that contains an affine Fano subplane Φ. Hence $\dim_\Phi \Pi = \theta$, a transcendental number.*

PROOF. Let π be a projective Hall plane of order p^{2n} and ϕ one of its Fano subplanes, whose existence is guaranteed by Neumann, ibid. Choose an affine Hall plane $\Pi = \pi^\ell$ such that the infinite line ℓ is a secant to a Fano plane ϕ, so $\Phi = \phi^\ell$ is a subaffine plane of Π. Hence $\dim_\Phi \Pi = \theta$ where θ satisfies the condition $2^\theta = p^{2n}$. But, by the Gelfond-Schneider Theorem, Schneider [22,23], if $1 < M < N$ are integers, then the equation $M^x = N$ is satisfied by $x > 0$ only if x is rational or transcendental. The result follows since $(2, p) = 1$. □

Following Neumann, Professor de Resmini pioneered what might be considered the study of planes admitting transcendental dimensions. She and her coworkers discovered spectacular examples of such phenomena. For instance, they showed that the Hughes plane of order 25, and also its derivative, the Ostrom-Rosati plane, admit subplanes of order 2 and 3, de Resmini and Puccio,[20], de Resmini and Leone, [17].

Further examples of transcendental affine planes have been obtained in this century by generalizing Neumann's contruction, Proposition 1.2. Thus, by carefully deriving Hall planes, so as not to lose at least one of its Fano subplanes, one obtains a range of translation planes, corresponding to subregular spreads, that contain Fano subplanes, as demonstrated by Fisher and Johnson, [7]. There are also other translation planes that are transcendental dimensional relative to suitable subplanes, Johnson [13].

Thus, transcendental dimensions signal an exotic embedding of one type of plane in a quite different type plane, one with the "wrong" characteristic. By way of contrast, if we consider any affine translation plane $\Pi = \pi^{\ell_\infty}$ (with ℓ_∞ the translation axis of π) of order p^n, then its dimension relative to any affine subplane Π_0, is always a rational number n/m, where p^m is the order of Π_0. Recent work, suggested by Theorems such as those indicated above, has concentrated on the contrasting question: are there planes that are neither transcendental-dimensional nor (as in the overwhelming majority of the known cases) integral-dimensional, that is: *Is it possible for a plane to be fractional dimensional?*

Until a very few years ago, only one fractional dimensional plane was known[(1)]: the Knuth semifield plane of order 32. In the last five years or so, Wene discovered other sporadic examples of fractional dimensional semifield planes, again of characteristic 2. Then Johnson and the second author found infinitely many fractional-dimensional semifields, [11], again of even order. In recent work, the authors of the present paper have shown that infinitely many semifield planes of characteristic 3 are fractional dimensional, Cordero-Jha, [4].

In all these cases, the planes shown to be fractional-dimensional are among various classes of known planes (due to Knuth, Kantor, Coulter-Matthews, Ding-

[(1)] And possibly only to one person — R. J. Walker, who had classified the semifields of order 32, almost 50 years ago, in his independent verification of the Knuth classification of the semifield planes of order 32, [24].

Yuan, cf. the survey by Kantor, [15]). Thus, in the study of fractional dimensions, as for transcendental dimensions, the aim is not so much to find new planes, but to find subplanes Π_0 of possibly "known" planes Π, that have fractional (or transcendental) dimension, $\dim_{\Pi_0} \Pi$.

Note that *all known fractional-dimensional planes* Π *are semifield planes*, and they are only known to be fractional dimensional relative to some subsemifield plane Π_0 of order p^2. (Thus Π_0 is Desarguesian and its projective closure includes the shears point of Π.) In particular, by the Baer condition, Π has order $\geq p^5$.

Actually, this minimality condition concerning the existence of fractional sub-semifield planes Π_0, of a semifield plane Π, may be formulated more generally for semifield planes Π of order q^n that are n-dimensional over a central subplane[(2)], coordinatized by $GF(q)$. Thus, by the Baer condition:

REMARK 1.3. Let Π be a semifield plane of order q^n with center $GF(q)$ such that Π has fractional dimension relative to a subsemifield plane Π_0 that contains a central subplane of Π. Then the integer $n \geq 5$, and, when $n = 5$, the fractional subplane Π_0 has order q^2 (and hence must be Desarguesian).

COROLLARY 1.4. *A semifield plane of order p^n, p prime, is fractional dimensional relative to a subsemifield plane Π_0 only if $n \geq 5$ and, when $n = 5$, Π_0 has order p^2.*

NOTE. In all cases known to us, any fractional dimensional *translation* plane of order p^5 satisfies *all* the hypotheses of Corollary 1.4 above.

One of our main goals is to show that, in a suitable asymptotic sense, *semifield planes Π of order p^5, or more generally in the 'minimal' semifield planes of order q^5 considered in Remark 1.3, the absence of fractional subplanes guarantees that all the semifields D that coordinatize Π are "primitive"*, in a sense analogous to finite fields, see Corollary A, p.6, (also cf. Theorem 5.6 and Corollary 5.7). Before stating our result explicitly, we define primitivity and a related Conjecture of Wene, to which our result may be seen as an explicit contribution.

– Primitive Semifields and the Wene Conjecture

An algebraic, measure of how "close" a plane is to being Desarguesian is to examine the structure of the "best" planar ternary ring that coordinatizes the plane. We consider this approach when applied to the multiplicative loops of semifields (finite non-associative fields). Following Wene and others, [25, 26,

(2) The center of a semifield is a plane invariant, thus all semifields coordinatizing a plane have centers isomorphic to the same $GF(q)$.

21, 9], we consider whether finite semifields have "cyclic" multiplicative loops, in a sense analogous to fields but taking into account the non-associative nature of their multiplicative loops.

DEFINITION 1.5. Let $\mathcal{D} = (D, +, \circ)$ be a semifield. Then $\mathcal{D}$ is a right primitive semifield if the multiplicative loop $(D^*, \circ)$ contains an element $\omega \in D$ such that every $d \in D^*$ is a right principal power $d = \omega^{k)}$, for some $k \geq 1$, where $\omega^{i)}$ is defined recursively by

$$\omega^{1)} = \omega, \omega^{i+1)} = \omega^{i)} \circ \omega.$$

Similarly, $\mathcal{D}$ is left primitive if every element of $(D^*, \circ)$ is a left principal power $\mu^{(k}$, $k \geq 1$, where the left principal power $\mu^{(i}, i \geq 1$ are defined analogously:

$$\mu^{(1} = \mu, \mu^{(i+1} = \mu \circ \mu^{(i}, i \geq 1.$$

The semifield $\mathcal{D}$ is *primitive* if it is both left primitive and right primitive.

NOTE. One can define primitive and right/left primitivity in exactly the same way for arbitrary finite planar ternary rings. The authors have shown, [3], that there are infinitely many finite quasifields (coordinatizing translation planes) that are primitive, and also infinitely many finite quasifields that are not primitive.

On the basis of a specific class of semifields and some computer-based investigations of small cases, Wene [25, 26] suggested:

CONJECTURE 1.6. (Wene, [26]) Every finite semifield is right primitive.

Rúa, [21], has shown that Conjecture 1.6 is false for the Knuth commutative semifield of order 32: this is neither left primitive nor right primitive. Moreover, Rúa also showed (ibid.) that some of the semifields of order $n = 2^5$ are left primitive but not right primitive and vice-versa (by duality). Hentzel and Rúa, [9], have established that the Wene Conjecture 1.6 does not hold for some semifields of order $n = 2^6$, and again there are semifields of order 64 that are left primitive but not right primitive and vice versa. But there are no known violations of the Wene conjecture for semifields of order $n \neq 2^5, 2^6$.

Since semifields of order q^2 with center $\supseteq GF(q)$ are fields, the first case of interest are semifields of order q^3 with center $GF(q)$. All such semifields are known: they are either fields or the twisted fields of Albert, as established by a celebrated Theorem of Menichetti [18]. Rúa, [21], has shown the Wene conjecture holds for these semifields. The present author's have given a different proof of Rúa's Theorem, Cordero-Jha, [3], without assuming Menichetti's classification, [18].

In this paper, one of our main concerns is whether 5-dimensional semifields, with center $GF(q)$, are primitive. Note that Menichetti's Theorem does not apply here since the Coulter-Matthews and the Ding-Yuan commutative semifields,

[15], have orders 3^n, $n \geq 5$ odd; also, the failure of the Wene conjecture for the case 2^5 needs to be taken into account.

The Knuth commutative semifield D of order 2^5, which violates the Wene Conjecture 1.6, coordinatizes a fractional dimensional semifield plane. On the other hand, the Coulter-Matthews plane of order 3^5 is fractional dimensional but does not violate the Wene conjecture.

Thus, part of the motivation for this paper was to examine how these facts concerning semifields of order p^5, which seem to be pulling in opposite directions, may be reconciled. Thus, we established the following asymptotic result.

COROLLARY A. (cf. Corollary 5.7) *For all sufficiently large primes p, the semifields coordinatizing a semifield plane Π of order p^5 are all primitive (right and left) if Π does not contain any proper subplane Π_0 of order $> p$.*

NOTE.

(1) More generally, cf. Theorem 5.6, suppose $q = p^r$, with r fixed. Then **there is an integer N_r such that for all $p > N_r$ any semifield plane Π of order q^5 with center $GF(q)$ is coordinatized only by semifields that are (left and right) primitive, whenever Π has no fractional subplanes.**
(2) In the p^5-case the non-existence of fractional subplanes is equivalent to the assertion that Π has no proper subplanes.
(3) It is conceivable that the theorem holds for all primes p, rather than for "sufficiently large" p. (Although the commutative semifield plane of order 2^5 admits coordinatization by a non-primitive semifield, the corresponding Knuth plane admits fractional subplanes, so the hypothesis of the above corollary does not apply.)

The key to the proofs of our results is the structure of the slope maps of *regulus* quasifields of low-dimension.

– Primitivity of Low-Dimensional Regulus Semifields

So far we have considered semifields D that have dimension n over the *center* $K = GF(q)$. We now turn to the more general case when K is the subfield of the left nucleus $N_\ell(D)$, or *kern*, that commutes multiplicatively with D. We refer to such subfields as regulus subfields of D. Every semifield is a regulus semifield over its central fields, but often has other regulus subfields as well.

DEFINITION 1.7. Let D be a semifield with a subfield

$$K = \{k \in N_\ell : k \circ d = d \circ k \forall k \in N_\ell\}.$$

If $\dim_K D = n$, then D is a *regulus semifield* of dimension n relative to the regulus subfield K.

NOTE.

(1) Every semifield D of order p^n is a regulus semifield over every subfield in the center $Z(D)$, hence over $GF(p)$.
(2) More generally, *a quasifield Q is a regulus quasifield if its kern contains a subfield K that commutes with K multiplicatively.* We determine the slope structure of Q for the cases $\dim_K Q \leq 5$, $k \neq 4$, cf. Theorem 3.8, and use the information to establish the right primitivity of semifields of dimension $n \leq 5, n \neq 4$.
(3) The n-dimensional regulus semifields D, of order q^n over a regulus field $GF(q)$, are precisely the semifields that coordinatize a semifield spread $\mathcal{S} < PG(2n-1,q)$ such that there is a regulus $\mathcal{R} \subset \mathcal{S}$ of degree $q+1$ with the shears axis $Y \in \mathcal{R}$.
(4) The 2-dimensional regulus semifields are precisely the semifields that coordinatize the flock semifields in $PG(3,q)$, *e.g.*, Gevaert and Johnson, [8]. Infinitely many 2-dimensional regulus semifields exist (including the Kantor-Knuth semifield flocks). Only the semifield flocks of even order q have been classified: the corresponding 2-dimensional regulus semifields are fields, *i.e.*, the flocks are linear, Johnson [14]. Thus for odd q only, the 2-dimensional *regulus* semifields form a strictly larger class than the 2-dimensional *central* semifields (which are merely fields). Moreover, each non-linear flocks is coordinatizable by several non-isomorphic regulus semifields.
(5) Although the semifields D of dimension 3 over the center $GF(q)$ have been classified by Menichetti, the 3-dimensional *regulus* semifield planes have not been classified.

By considering 2-dimensional regulus semifields and using note (4), we will show:

THEOREM. (cf. Corollary 7.3) *All the semifields coordinatizing conical flocks are right primitive.*

NOTE. The duals of non-linear flock semifields are not flock semifields, unless the semifields are fields. Hence, we may only assert that the duals are left primitive: we do not know if they are right primitive.

For dimension 3 we prove an extension of Rúa's Theorem: thus we prove Wene's Conjecture, Conjecture 1.6, for *regulus* semifields that are 3-dimensional over a regulus field $GF(q)$, provided q is large enough.

THEOREM. (cf. Theorem 6.2) *Let π be a semifield spread in $PG(5,q)$ such that $\pi \supset \mathcal{R}$, a regulus of degree $q+1$ such that the shears axis $Y \in \mathcal{R}$. Then for all sufficiently large q, every semifield coordinatizing π is right primitive.*

The above are proved by determining the slope maps of regulus quasifields for dimension ≤ 5 (but not dimension 4 — where different arguments seem necessary), cf. paragraph 3. These results are implicit in Theorem 3.8, and the argument used in proving it.

2 – Preliminaries

We assume the reader to be familiar with affine translation planes and their coordinatization by quasifields, particularly semifields, [10], and their connections with spread sets and spreads, *e.g.*, [12, pp. 36–48], or [1]. To fix our notation, particularly in regard to the non-standard notion of a "regulus" quasifield/semifield, we recall some terminology. Quasifields obey the right distributive law: $(a+b)\circ c = a\circ c + b\circ c$.

DEFINITION 2.1 **(Slope Maps and Regulus Quasifields)** Let Q is a finite quasifield. Then its kern is the field

$$\{k \in Q : \forall a, b \in Q : k\circ(a+b) = k\circ a + k\circ b, k\circ(a\circ b) = (k\circ a)\circ b\},$$

and any (sub)field $K \cong GF(q)$ of Q is a *kern (sub)field* of Q; now $|Q| = q^n$ for some integer $n \geq 1$, since Q is a K vector space.

The *slope* [map] of any non-zero $m \in Q$ is $T_m \in GL(Q, K)$ specified by $T_m : x \mapsto x\circ m, x \in Q$. Thus, T_m may (when convenient) be identified with a non-singular K-matrix of order $n \times n$, which depends on the choice of the K-basis for Q. Also the *slope set* for Q (regarding T_0 as is the zero map) is $\tau_Q = \{T_m : m \in Q\}$.

If the slopes of the elements $k \in K$ are the scalar elements $k\mathbf{1}_5$, then Q is a *regulus quasifield*, and K a *regulus* subfield. (Equivalently, a kern field K is a regulus field if each $k \in K$ commute multiplicatively with every $d \in Q$.)

NOTE. The regulus quasifields, as described above, are the quasifield that coordinatize the spreads $\mathcal{S}$ in $PG(2n-1, q)$ that contain a regulus $\mathcal{R}$ of degree $q+1$: regulus quasifields arise when the coordinatizing triad of components defining the quasifield are selected from among the components in any regulus $\mathcal{R} \subset \mathcal{S}$.

The above attributes of quasifields and semifields are also assigned to the spread sets that they define.

DEFINITION 2.2. Let V be a vector space of dimension n over a field $K \cong GF(q)$, $q = p^r$. Then a set of linear maps

$$\tau \subset GL(V, K) \cup \{\mathbf{0}_n\} := \overline{GL(n, K)},$$

is a *spread set* on the K-space V if $|\tau| = |V| = q^n$, $\tau \supset \{\mathbf{0}_n, \mathbf{1}_n\}$, and

$$A, B \in \tau \implies A - B \in GL(n, K).$$

(1) τ is a *regulus* spread-set if $\tau \supset \mathcal{K}$, where $\mathcal{K} = k\mathbf{1}_n : k \in K$.
(2) τ is *additive* if it is closed under addition (equivalently, τ is an additive group of order $|V|$, with all non-zero elements non-singular and including $\mathbf{1}_V$).
(3) An additive spread set τ is *linear* if τ is a K-subspace of the ring $\mathrm{Hom}(V, +, K)$.

The following properties relating quasifields/semifields to their spread sets are obvious.

Remark 2.3.
(1) If Q is a quasifield then its slope set τ_Q is a spread set.
(2) If Q is a regulus quasifield, relative to a field K, then τ_Q is a regulus spread set, *i.e.*, τ_Q contains the scalar subfield $\mathcal{K} \cong K$.
(3) If $(D, +, \circ)$ is a semifield containing a field $K \subset N_\ell(D)$ then
   (a) $\tau_D \subset GL(D, K) \cup \{\mathbf{0}\}$ is an additive spread set;
   (b) If D is a regulus semifield over K then the additive spread set τ_D is a K-regulus spread set;
   (c) If D has K in its center (so K is a subfield of the nucleus $N(D) = N_\ell(D) \cap N_m(D) \cap N_r(D)$ such that D centralizes K multiplicatively) then τ_D is a K-linear vector space.

Note that an obvious "converse" of each part of Remark 2.3 is also valid, but we shall only use the fact that every additive spread set is the slope set of a semifield, cf. Remark 4.1.

3 – Slope Map Structure for 5-Dimensional Regulus Quasifields

The slope maps of the non-zero elements of an n-dimensional quasifield Q, over a kern field $K = GF(p^r)$, are elements of $GL(n, q)$. Constraints on the permitted structure of the non-zero slope maps $A \in \tau_Q$ obviously influences the structure of Q, hence also on the geometry of the associated translation plane. We consider the case when Q is a regulus quasifield over K, so

$$\tau_Q \subset GL(n, K), \tau_Q \supset \mathcal{K} = \{k\mathbf{1}_n : k \in K\}.$$

When $n = 3$, we showed, in, [3], that each non-scalar maps $A \in \tau_Q$ is irreducible, thus yielding an alternative proof to Rúa Theorem, establishing the primitivity of all semifields of order q^3 with center $GF(q)$. The key step was to show $(|A|, p) = 1$.

Here we consider the analogous problem for regulus quasifields Q of order q^5. It turns out, that now there are more possibilities than in the q^3-case: A still has order relatively prime to p, but A might not be irreducible. Our goal here is to describe the slope structure for 5-dimensional regulus quasifields, Definition

2.1; in a later section we will specialize to the case when Q is a semifield to obtain a criterion for Q to be a fractional semifield.

We begin with some Lemmas without imposing the dimensional restriction. Thus, we consider a quasifield Q of order q^n, characteristic p, that contains a regulus subfield $K = GF(q)$.

LEMMA 3.1. *Let A be a slope map of a regulus quasifield Q over $GF(q)$, Definition* 2.1. *Then A cannot leave invariant any one-space over $GF(q)$, unless A is one of the scalar slopes of Q.*

PROOF. Otherwise, A has a $GF(q)$-eigenvector, and hence a corresponding eigenvalue λ in $GF(q)$. So there is a matrix X such that XAX^{-1} is a matrix with first column λe_1, and now $X(A-\lambda I_n)X^{-1}$ is singular, hence so is $A-\lambda I_n$, which means A and λI_n cannot both be slope maps in the same spread set unless $A = \lambda I_n$. ∎

We use $\langle A\rangle$ to denote the multiplicative group generated by any non-singular matrix A.

COROLLARY 3.2. *Let Q be a regulus quasifield over a subfield K. Let A be the slope map of any element of $Q \setminus K$. Then, regarding Q as a vector space over K:*

(1) *A does not fix any one-space or hyperplane of Q.*
(2) *No subgroup S of $\langle A\rangle$ fixes a unique one-space or a unique hyperplane of Q.*

PROOF. Consider the first part. Lemma 3.1 states A cannot fix a one-dimensional K-space. Hence A cannot fix a hyperplane, since the number of fixed one-spaces is the number of fixed hyperplanes, *e.g.*, [5, 12, p. 81]Dembowski. The second part follows since $\langle A\rangle$ is abelian. ∎

Unless the contrary is indicated, A denotes the slope of some element of the quasifield Q that does *not* lie in the scalar field $I_nK = GF(q)$. So the cyclic group $\langle A\rangle = P \oplus R$, where P denotes the (possibly trivial) p-Sylow subgroup of $\langle A\rangle$ and R is its Hall p'-subgroup. Much of our effort will be devoted to showing that P is often the trivial group. As a default assume P is non-trivial, so $Fix(P) := F_P$ is a non-trivial K-subspace of Q. So R, which centralizes P, leaves F_P invariant. We count the set of Maschke R-complements of F_P.

LEMMA 3.3. [# P-complements] *Suppose P is non-trivial, with fixed space F_P. Then for some integer $k \geq 1$, R has kp distinct Maschke-complements C of P, on the K-space Q. Also, R is completely reducible on F_P*

PROOF. Note that P can't leave invariant any R-complement C of F_P, since P would then fix non-zero points on C. Hence each of the Maschke complements of F_P, for the p'-group R, must lie in a non-trivial P-orbit. The final sentence holds because R is a p'-group that leaves F_P invariant. □

COROLLARY 3.4. 1) *R cannot fix a 1-space in F_P;* 2) *F_P cannot be a 1-space.*

PROOF. 1) Suppose R fixes a 1-space of F_P. Then so does A since R and P must both fix this space and hence so must the group they generate, viz., $A \in R \oplus P = \langle A \rangle$. But now the eigenvalue argument, Lemma 3.1, yields a contradiction so 1) follows. Part 2) is a special case since A, hence also R, leaves F_P invariant. □

Up to now we have not imposed any restrictions on the dimension on the dimension of regulus quasifield Q. For the remainder of the section we restrict ourselves to the 5-dimensional case: Thus, *Q is a quasifield of order q^5 with a regulus subfield K such that $dim_K Q = 5$, so $|Q| = q^5$.* So by Corollary 3.2 above, we may assume F_P has rank three or two: we consider each case in turn.

– **Case: F_P has rank 3.**

We require a Corollary to:

LEMMA 3.5. *Suppose $(m, n) = 1$ and that q is any prime power. Then an irreducible abelian group $G < GL(n, q)$ cannot be isomorphic to an irreducible subgroup of $GL(m, q)$.*

PROOF. Since G is abelian, by Schur's Lemma G is in a field $GF(q^n)$, but not in any subfield of it. Hence $|G|$ divides $q^n - 1$ but not $q - 1$. However,

$$(q^m - 1, q^n - 1) = q^{(m,n)} - 1 = q - 1,$$

shows that $|G|$ does not divide $q^m - 1$, the order of the multiplicative subgroup of $GF(q^m)$. However, if G were an abelian irreducible subgroup of $GL(m, q)$ then, by Schur again, G would also be an irreducible subgroup of $GF(q^m)$, contradicting the fact that $|G|$ does not divide $q^m - 1$. □

COROLLARY 3.6. *For any prime power q, an irreducible abelian subgroup G of $GL(3, q)$ cannot be isomorphic to any subgroup of $GL(2, q)$.*

PROOF. By the Lemma above, we need merely exclude the possibility that G acts reducibly on the vector space $V_2(q)$. By Maschke, G diagonalizes hence $|G|$ divides $(q-1)^2$, contradicting the irreducibility of G on $V_3(q)$. □

If R fixes a one-space on $Fix(P)$ then so does A, contradicting Corollary 3.2. If R fixes a 2-space T in $Fix(P)$ then it still fixes a one-space, the Maschke complement of T in $Fix(P)$, so we have the same contradiction. Hence R acts irreducibly on $Fix(P)$. Now any R-complement S of F_P, has rank two, and since, by Corollary 3.6, R cannot be faithful on a two-space, being irreducible on a 3-space, a non-trivial subgroup R_1 of R fixes S elementwise. Hence $S_1 = Fix(R_1) \geq S = Fix(R)$ is P-invariant. There are the following cases to consider: i) $S_1 = S$ implies P leaves S invariant and hence fixes non-zero vectors in S contradicting the fact that S is a complement to F_P; ii) $S_1 > S$ so $S_1 \cap F_P$ is a non-trivial proper subspace of F_P since $S \oplus F_P = Q$, and now we contradict the fact that S acts irreducibly on F_P. So the case F_P has rank 3 can never occur.

– **Case: F_P has rank 2.**

By Corollary 3.2 again, R has at least p distinct Maschke complements of the subspace F_P. Since these have rank 3 any two of them, say X and Y, must intersect. Now if $H := X \cap Y$ has rank 2 then $X + Y$ has rank 4, and either $X + Y$ intersects F_P in a one-space, contrary to the eigenvalue argument, or F_P is a rank 2 subspace of the 4-space $X + Y$ and now F_P is too large to be in a complement of X in $X + Y$: recall this is required because F_P has X as a complement.

Thus, H must have rank one, and $F_P < X + Y$, since $X + Y$ has rank 5 because $H = X \cap Y$ has rank one. Since R fixes H, a rank one-space, and R acts irreducibly on F_P, by the eigenvalue argument, we conclude $H \cap F_P$ is trivial. But since now R is irreducible on the rank 2 vector space F_P, of order q^2, and moreover the rank one vector space H of order q is R invariant, it follows that a non-trivial subgroup R_1 of R acts trivially on H, since no scalar group, hence of order dividing $q-1$, can be irreducibly on F_P since this is 2-dimensional over $K = GF(q)$. Note that since the p-group P, centralizes $R_1 < R$, P must leave $F_1 = FixR_1$ invariant, and hence fix non-zero points on it. Hence $F_1 \cap F_P \neq 0$. If $F_1 \cap F_P$ is a one-space then R fixes this one-space, a possibility already excluded (because A, generated by R and P, would be forced to fix this one-space, contrary to Corollary 3.2). Hence $F_1 \geq F_P$ but then $F_1 > F_P$, since $F_1 > H$ and $H \cap F_P = 0$.

Hence F_1 must have rank 3: otherwise R_1 fixes a hyperplane elementwise which is A-invariant, since R_1 is centralized by A, contrary to Corollary 3.2(1). Now if R leaves invariant at least two rank-one subspaces of F_1 that complement F_P, say C_i, $i = 1, 2$, then $C_1 \oplus C_2$ meets F_P in a rank-one subspace fixed by R, contradicting the fact that R is irreducible on the 2-space F_P. Thus R leaves

invariant the unique complement C of F_P in F_1. Since A centralizes R_1, it leaves F_1 invariant, and hence the unique complement C of F_1, contrary to Corollary 3.2. So F_P is not a rank 2 space.

Hence, since we have ruled out all putative dimensions for F_P, we have shown the order of A is not divisible by p:

PROPOSITION 3.7. *A is a p'-element in all cases, i.e. $\langle A\rangle = R$.*

So either (1) A is irreducible, or (2) A has a $3+2$-split, Corollary 3.2. So we have

THEOREM 3.8. *Let D be a quasifield of order q^5, with regulus field $K = GF(q)$. Then the order of any slope map $A := T_d$, for $d \in D \setminus K$, is not divisible by p. Hence any A is either scalar, irreducible or has a decomposition into irreducible subspaces $V_3 \oplus V_2$, where V_d denotes a K-subspace of D with rank d.*

COROLLARY 3.9. *The slope-map $A = T_d$ not reducible if and only if $|A|^{q^5-1} = 1$.*

PROOF. If A is irreducible or scalar then A lies in $GF(q^2)$, hence in both cases $|A|^{q^5-1} = 1$. If A is reducible but non-scalar then by Theorem 3.8 $A|V_3$ is irreducible hence by Schur's Lemma $|A|$ is divisible by a p-primitive divisor v of q^3-1. But since $(q^3-1, q^5-1) = q-1$, it follows that $|A|^{q^5-1} \neq 1$. ∎

4 – Primitive Spread Sets

Any spread set is the slope set of some quasifield. The case when the spread set is additive is of special relevance:

REMARK 4.1. Let $\mathcal{S} \subset GL(V,K) \cup \{\mathbf{0}\}$ be an additive spread set, on the finite vector space $(V,+)$ over a field K. Then for each non-zero choice of $e \in V$, there is a semifield $\mathcal{D}_e = (V,+,\circ)$ with slope set $\mathcal{S}$, and multiplicative identity e.

PROOF. Define $x \circ y = xT_y$, where $T_y \in \mathcal{D}$ is chosen such that $y = eT_y$. ∎

NOTE.

The semifields D_e, as e varies over V^*, are all isomorphic only if $\mathcal{S}$, equivalently D_e, are all fields.

Suppose D_e is a semifield, coordinatizing a semifield plane Π, when the unit point e is chosen on (fixed) unit line Z. The following Lemma implies that if D is right primitive then all the semifields D_f, based on choosing unit point $f \in Z$,

are right primitive, cf. Corollary 4.4. The Lemma will be used in the proof of our main result, Theorem 5.6.

LEMMA 4.2. *Let $\mathcal{S}$ be an additive spread set of order q^n, over any finite field $K = GF(q)$. Then the following are equivalent*

(1) *Some $\Omega \in \mathcal{S}$ has order $q^n - 1$.*
(2) *Every semifield D with slope set $\tau_D = \mathcal{S}$ is right cyclic.*
(3) *Some semifield D with slope set $\tau_D = \mathcal{S}$ is right cyclic.*

PROOF. (1) $\Longrightarrow$ (2). Some $\Omega \in \mathcal{S}$ has order $q^n - 1$. Let D be any semifield with slope set $\tau_D = \mathcal{S}$, and multiplicative identity e. Let $e\Omega = \omega$. Thus, by Remark 4.1,

$$\begin{aligned} e \circ \omega, (e \circ \omega) \circ \omega, ((e \circ \omega) \circ \omega) \circ \omega, \ldots &= e\Omega, (e\Omega)\Omega, ((e\Omega)\Omega)\Omega, \ldots \\ &= e\Omega, e\Omega^2, e\Omega^3, \ldots, e\Omega^{p^n-1}, \ldots \end{aligned}$$

However, since the cyclic group $\langle \Omega \rangle \subset GL(n, K)$ is the multiplicative group of a matrix field $\cong GF(q^n)$, the group $\langle \Omega \rangle$ is sharply 1-transitive on the non-zero elements of the K-space K^n. So the above sequence imcludes all the $p^n - 1$ non-zero elements of K^n, which means the right powers of ω:

$$\omega, (\omega \circ \omega), ((\omega \circ \omega)) \circ \omega, (((\omega \circ \omega)) \circ \omega) \circ \omega, \ldots,$$

run over all of D^*: so D is right primitive. Thus, (1) $\Longrightarrow$ (2) holds. (2) $\Longrightarrow$ (3) is immediate. (3) $\Longrightarrow$ (1). Suppose D is right primitive, and $\tau_D = \mathcal{S}$ its slope set. Let ω be a right primitive element of D, and $\Omega = T_\omega$ be its (right) slope map. Then, as above, it is easy to see that Ω has order $p^n - 1$.

Since right primitive semifields are those that admit a primitive matrix as a slope map, Lemma 4.2(1), and the fact that duals of right primitive semifields are left primitive Lemma 4.2 yields:

COROLLARY 4.3. *Let Π be a semifield plane. Then the following conditions are equivalent.*

(1) *All semifields D coordinatizing Π are right primitive.*
(2) *All semifields D coordinatizing the dual plane of Π are left primitive.*
(3) *All semifields D coordinatizing Π^t the transpose plane of Π are right primitive.*

As indicated earlier, p.5, the work of Rúa, and Hentzel-Rúa, [21, 9], shows that left primitivity and right primitivity for a semifield are not mutually equivalent concepts, for semifields, of order 16 and 64. Lemma 4.2, suggests a possible approach for finding further examples. Thus, applying Lemma 4.2 to a commutative semifield D which is right primitive, hence also left primitive, we obtain a chain of semifields of type:

left & right primitive $\rightarrow$ right primitive [transpose]$\rightarrow$ left primitive [dualize],

and the middle semifield might only be right primitive in which case the final semifield would be left primitive but not right primitive.

Lemma 4.2 also yields the following geometric characterization of planes all whose coordinatizing semifields are right primitive semifields.

COROLLARY 4.4. *Let Π be an affine semifield plane with shears axis Y. Suppose Π is coordinatized by a semifield based on choosing any axis $X \neq Y$ as the x-axis and unit point $e \in Z$, where $Z \notin \{X, Y\}$ is any fixed line through $O = X \cap Y$. Then the semifield D_e coordinatizing Π with the above choices is primitive iff every semifield D_f, based on unit point $f \in Z \setminus \{O\}$, is right primitive.*

PROOF. Interpret the claim in terms of spreads. Thus π is a spread specified by a spread set $\mathcal{S}$ such that line Z is identified with $y = x\mathbf{1}$, $\mathbf{1} \in \mathcal{S}$. Now the semifields D_f and D_e have the same slope set. □

5 – Proof of Main Theorem

In this section we prove Theorem 5.6 . The proof of the following Lemma implicitly describes a technique for detecting fractional subplanes of a given semifield plane. Given a 5-dimensional semifield D, not necessarily fractional, with slope set τ_D, the Lemma shows how to replace D by a fractional semifield D', such that D' is fractional and $\tau_{D'} = \tau_D$, whenever such a D' exists. An elaboration of this method is used to construct fractional dimensional planes of odd order in Cordero and Jha, [3]. Note that the argument makes crucial use of the fact that D is 5-dimensional over a subfield field $K = GF(q)$ in the *center* of D, rather than merely requiring that D be a regulus subfield over K.

LEMMA 5.1. *Let $\mathcal{D} := (D, +, \circ)$ be a 5-dimensional semifield over its center $K = GF(q)$, with slope-set $\mathcal{S} \subset GL(D, K)$. Then either there is a fractional semifield $\mathcal{D}^* := (D, +, *)$ relative to a field $(F, +, *) \cong GF(q^2)$, with center $Z(\mathcal{D}^*) \subset (F, +, *)$, such that $\mathcal{S}$ is also the slope-set of $\mathcal{D}^*$, or every non-scalar element $m \in D \setminus K$ has irreducible slope map $T_m \in \mathcal{S}$.*

PROOF. Suppose the irreducible condition fails. So there is an $m \in D \setminus K$ such that its slope-map $A := T_m$ is not irreducible. Then by Theorem 3.8, A admits a decomposition $V_2 \oplus V_3$, where V_2 and V_3 are irreducible A-invariant subspaces of D that, as K-subspaces, are of dimensions 2 and 3 respectively. By Remark 2.3((c)), $\mathcal{S}$ is closed under both addition, and *multiplication* by the scalar field $\mathcal{K} \subset \mathcal{S}$, $\mathcal{K} \cong GF(q)$. So $\mathcal{S} \supset \mathcal{K} + \mathcal{K}A$, and this additively closed partial spread set, of size q^2, leaves V_2 invariant and hence, by counting, $\mathcal{K} + \mathcal{K}A$ clearly induces an additive spread on V_2. Fix any non-zero $e \in V_2$. Then, cf. Remark 4.1, define a new semifield $(D, +, *)$ by the rule $x * y = x\theta_y$ where $\theta_y \in \mathcal{S}$ such that $e\theta_y = y$. It is straightforward to verify that $(D, +, *)$ is a semifield with center $(K, +, *)$, and obviously $\tau_{D^*} = \tau_D = \mathcal{S}$. Moreover, since V_2 is invariant under $\mathcal{K} + \mathcal{K}A \subset \mathcal{S}$, $(V_2, *)$ is multiplicatively closed, hence by finiteness, the multiplicative loop of $(D^*, *)$ induces a loop on $(V_2, *)$. Thus $(D, +, *)$ is a semifield with a sub-semifield $(V_2, +, *)$. Put $K_2 = (e)\mathcal{K}$ and observe that $V_2 \supset K_2$ and that K_2 is in the center of $(D, +, *)$: K_2 is actually the full center of $(D, +, *)$, by the Baer condition. Thus, since $\dim_{K_2} V_2 = 2$, V_2 must be a field, since semifields that are 2-dimensional extensions over a field are field. So choosing $F := V_2$, completes the proof. ∎

We require a fundamental Theorem of Davenport, which we describe using the following:

NOTATION 5.2. Let F be finite field. So for any subfield $G < F$, and $x \in F^*$ the ring $G[x]$, of x-polynomials over G, is the subfield of F generated by $G \cup \{x\}$. We consider $G[x]$ to be the FIELD GENERATED BY x OVER G.

RESULT 5.3.(Davenport, [6, Theorem 1].) There exists a positive integer function, $\delta : \mathbb{P} \to \mathbb{P}$, such that in any field $F = GF(p^k) > GF(p) = Z_p$, for $k \leq r$ the following holds: if $\theta \in F$ generates F over Z_p then there exists $\alpha \in Z_p$ such that $\theta - \alpha$ is a primitive element of F.

We require a consequence of this result for which the subfield chosen is not necessarily Z_p. The proof makes extensive use of notation 5.2.

LEMMA 5.4. *Let $F = GF(q^d) > GF(q) = K$, where d is prime and $q = p^r$, and assume that the prime $p > \delta(rd)$. Then to each $t \in F \setminus K$ correspond $\alpha, \beta \in K$ such that $\beta t + \alpha$ is a primitive element of F.*

PROOF. Let $Z_p \leq K$ be the prime subfield of F. Since the dimension $[F : K] = d$ is prime, for any $T \in F \setminus K$ we have $F = K[T]$. Let $F_T = Z_p[T] = GF(p^t)$ for some $t > 1$. By Davenport, result 5.3, $T + z$ is a primitive element of F_T, hence the result holds unless neither of the fields K and F_T contains the other field. So $T + z \notin K$, hence without loss of generality we may assume T itself is a primitive element of F_T. Let ω be a primitive element of the maximal subfield K, so $T\omega$ is not in $K \cup F_T$, and $(p^r - 1)(p^t - 1)$ is an exponent of $T\omega$. We concentrate on the main case:

Case: Neither K nor F_T has order p^2 when $p+1=2^x$.

Let ρ and τ be respectively p-primitive divisor of p^r-1 and p^t-1. Now ω^{p^t-1}, a power of ωT, has order divisible by ρ; for if not then ρ divides p^t-1 so an element of F_T is a generator of K, over Z_p, so $F_T > K$ a contradiction. Hence $Z_p[\omega^{p^t-1}] = K$, so $Z_p[\omega T] \supseteq K$.

By a similar argument, T^{p^s-1}, also a power of ωT, has order divisible by τ (otherwise τ divides p^s-1 and K contains an element of order τ so $K \supseteq F_T$, a contradiction), and hence $Z_p[\omega T] \supseteq F_T$.

Hence we have shown the field $Z_p[\omega T]$ includes $K \cup T$, hence, since K is maximal in F, $F = Z_p[\omega T]$. But now by Davenport again, result 5.3, for some $\alpha \in Z_p$, $\omega T + \alpha$ is a primitive of F. This is the required result.

We turn to the exceptional case when one of the fields K or F_T has no p-primitive divisors. Note that since p is large we may assume $p > 64$. Thus we need only consider:

Case: $p+1=2^x$, and exactly one of $K, F_T \cong GF(p^2)$.

Consider the case $K = GF(p^2)$, $p+1=2^x$, and $F_T = GF(p^t)$, $t > 1$ odd. So ωT has exponent $(p^2-1)(p^t-1)$, and $(\omega T)^{(p^t-1)} = \omega^{(p^t-1)}$. But since $\gcd(p^2-1, p^t-1) = p-1$, implies $p^t-1 = (p-1)\nu$, ν an odd integer > 1, it follows that $\omega^{(p^t-1)} = \omega^{(p-1)\nu} \notin Z_p$, since $\omega^{(p-1)\nu}$ is a 2-element, of order $p+1$. Hence $K = Z_p[\omega^{(p^t-1)}] \subseteq Z_p[\omega T]$.

It remains to rule out the case $K = GF(p^w)$, and $F_T = GF(p^2), p+1=2^x$, $t > 1$ odd. Arguing as before, $p^t-1 = (p-1)\nu$, ν odd, and now ωT has exponent $(p^2-1)(p^w-1)$, so $(\omega T)^{(p^w-1)} = T^{(p^w-1)}$, where $T^{(p^w-1)} = T^{(p-1)\nu} \notin Z_p$. Hence $F_T = Z_p[T^{(p^w-1)}] \subseteq Z_p[\omega T]$. ∎

We will use the special case of the Lemma, when $F = GF(q^5)$.

Corollary 5.5. *Let $F = GF(q^5) > GF(q) = K$, where $q = p^r$. Then there is a function $\Delta(r), r \in \mathbb{P}$, such that for all $p > \Delta(r)$, to every $t \in F \setminus K$ correspond $\alpha, \beta \in K$ such that $\beta t + \alpha$ is a primitive element of F.*

Theorem 5.6. *Let Π be any semifield plane of order q^5 with center $GF(q), q = p^r$, with r fixed. Suppose the prime $p > \Delta(r)$, where the function Δ is a Davenport function, as in Corollary 5.5. Then all the semifields coordinatizing Π are right primitive and left primitive, whenever Π contains no fractional subplanes Ψ [that contain a central subplane of Π] .*

Proof. We suppose Ψ does not exist. Let D be any semifield coordinatizing Π, with center $K \cong GF(q)$, and let τ_D denote the slope set of D. Thus τ_D is an additive spread set that includes the scalar field $\{\mathcal{K} = k\mathbf{1} : k \in K\}$, and in fact τ_D is a linear spread set over the field $\mathcal{K} \cong GF(q)$. Let π be the corresponding spread on $D \oplus D$; thus $X = D \oplus \mathbf{0} \in \pi$ and $Y = \mathbf{0} \oplus D \in \pi$, where Y is

the shears axis. Suppose $T_d \in \tau_D \setminus \mathcal{K}$ is reducible. Then by Lemma 5.1, Π may be recoordinatized by a fractional semifield E, that contains $GF(q)$ in its center, so the plane Π_E coordinatized by E has a fractional central subplane, but since $\Pi = \Pi_E$ we contradict our assumption that contains no fractional central subplane.

Hence, every non-scalar in τ_D is irreducible. Choose any non-scalar $T \in \tau$. Then since T is irreducible, Schur's Lemma implies that there is a field Θ of K-linear maps containing $\{\mathcal{K}, T\}$, and since D must be a vector space over Θ, it follows that $GF(q^5) \cong \Theta \supset \mathcal{K}$. Hence T, viewed as a $\mathcal{K}$-linear map, is an irreducible element of the field Θ, over the subfield $\mathcal{K}$. So by Corollary 5.5, there are elements $\alpha, \beta \in \mathcal{K}$ such that $W = \alpha T + \beta \in GL(D, K)$ is a primitive element of the field Θ, hence W, as an element $GL(D, K)$, has multiplicative order $|W| = q^5 - 1$. Moreover, since τ_D is a $\mathcal{K}$-linear set, we also have $W \in \tau_D$. But then, by Lemma 4.2(1), D is right-primitive. We still need to check that all such D are left primitive.

Consider the dual plane Π' of Π. Suppose, if possible, that Π' has a fractional subplane, containing a central subplane. So there is a semifield $\mathcal{D}' := (D, +, *)$, with center $K = GF(q)$, coordinatizing Π' such that $\mathcal{D}' := (D, +, *)$ contains a subfield $\mathcal{F} := (F, +, *) > (K, +, *)$, with $\mathcal{F} \cong GF(q^2)$. Now the dual semifield, of $\mathcal{D}' := (D, +, *)$, is a semifield $\mathcal{D} := (D, +, \circ)$ (thus $x \circ y = y * x, x, y \in D$), with center $(K, +, *)$, and this contains the subfield $(F, +, \circ) = (F, +, *) \cong GF(q^2)$, hence the corresponding plane $\Pi(D)$ is fractional relative to the central plane $\Pi(F)$. However, $\Pi(D) \cong \Pi$, which has no fractional subplane. This contradiction shows that Π' cannot be coordinatized by a fractional subplane. Hence, by what has been proved above, the semifields coordinatizing Π' are right primitive, so the semifields coordinatizing Π are left primitive. Thus all the semifields coordinatizing Π are both right primitive and left primitive. ∎

COROLLARY 5.7. *Let Π be any semifield plane of order p^5. If Π does not admit fractional planes, and p is sufficiently large, then every semifield coordinatizing Π is right primitive and left primitive.*

6 – Generalization of Rúa's Theorem to Regulus Semifields in $PG(7, q)$

Recall that Rúa has shown that semifields of order q^3 with center $GF(q)$ are both right primitive and left primitive. However, in view of the Menichetti classification of such semifields, [18], this result is essentially a result concerning the Albert semifields of order q^3, with center $GF(q)$.

On the other hand, 3-dimensional *regulus* semifields have yet to be classified. These semifields are precisely the semifields that coordinatize semifield spreads $\mathcal{S}$ in $PG(7, q)$ that contain a regulus $\mathcal{R}$ of degree $q + 1$. We show that such semifields are right primitive if q is sufficiently large, Theorem 6.2. For this we require a stronger form of Lemma 5.4, for $q^d = q^3$, due to Mills and McNay.

RESULT 6.1. (Mills and McNay, [16, Paragraph 5]) Suppose $GF(q^3) \cong F > K \cong GF(q)$. Then for sufficiently large values of q, to each $\theta \in F \setminus K$, corresponds an element $k \in K$ such that $\theta + k$ is a primitive element of F.

We may now generalize Rúa's Theorem, [21, Theorem 4], by establishing the right primitivity of semifields 3-dimensional over a regulus subfield $GF(q)$, as opposed to a central subfield $GF(q)$.

THEOREM 6.2. *Let D be a semifield of order q^3 with kern $K = GF(q)$ such that K centralizes D multiplicatively. Then for sufficiently large q, D is right primitive.*

PROOF. Let τ_D be the (additive) spread set of D, and $\mathcal{K}$ be the scalar field in $GL_K(D,+) \cup \{\mathbf{0}\}$, associated with the slope set of K. Then any $T \in \tau_D \setminus \mathcal{K}$ is irreducible. This follows by noting that by the "eigenvalue-argument", Lemma 3.1, T fixes no one-space of the projective plane $PG(D,K)$, hence also no "hyperplane". Thus, by Schur's Lemma, the centralizer of T in $GL_K(D,+) \cup \{\mathbf{0}\}$ is a field $\mathcal{F}_T \supset \{T\} \cup \mathcal{K}$, whenever $T \notin \mathcal{K}$. Since $\mathcal{F}_T \cong GF(q^3)$ and $\mathcal{K} \cong GF(q)$, Mills and McNay, result 6.1, shows that $T + \kappa$, for some $\kappa \in \mathcal{K}$, has multiplicative order $q^3 - 1$. Since, by the additivity of τ_D, $T + \kappa \in \tau_D$, we have τ_D contains a primitive matrix, so $(D,+,\circ)$ is right primitive by Lemma 4.2. ∎

7 – Right Primitivity of Flock Semifields

The following result is part of a slightly more general Theorem due to S. D. Cohen:

RESULT 7.1. (Cohen, [2].) Let $F = GF(q^2) \supset GF(q) = K$, q any prime power. Then to each $\theta \in F \setminus K$ there correspond $\alpha \in K$ such that $\theta + \alpha$ is a primitive element of F, hence of multiplicative order $q^2 - 1$.

LEMMA 7.2. *Let $\mathcal{D} := (D,+,\circ)$ be a semifield with kern K such that K commutes multiplicatively with D and $\dim_K Q = 2$. Then D is right primitive.*

PROOF. The slope set τ_D may be regarded as an additive group in $GL(2,q) \cup \{\mathbf{0}_2\}$, acting on the K-space $(D,+)$, such that $\tau_D \supset \mathcal{K}$, where $\mathcal{K}$ is the scalar field $\{k\mathbf{1}_2 : k \in K\}$. Let $T \in \tau_D \setminus \mathcal{K}$. Now T is $\mathcal{K}$-linear and acts irreducibly on $(D,+)$, by the "eigenvalue-argument", Lemma 3.1, so by Schur's Lemma the centralizer of T in $Hom_(D,+)$ is a field $\mathcal{F}_T \supset T \cup \mathcal{K}$. Evidently, we have shown the field $\mathcal{F}_T \cong GF(q^2)$, contains $\mathcal{K} \cong GF(q)$, with $T \in \mathcal{F} \setminus \mathcal{K}$. Hence, by Cohen's Theorem, result 7.1, we have $T + A$, for some $A \in \mathcal{K}$, is a primitive element of $\mathcal{F}_T$. However, as τ_D is an additive group $T + A \in \tau_D$ is an element in $GL(2,q)$ with multiplicative order $q^2 - 1$. Hence $(D,+,\circ)$ is right primitive by Lemma 4.2. ∎

The semifields D that are 2-dimensional over their central kern are precisely the semifields that coordinatize the flock semifield planes. Thus, Lemma 7.2 is equivalent to:

COROLLARY 7.3. *The semifields coordinatizing a flock semifield plane are are all right primitive.*

Note that any non-Desarguesian flock semifield plane admits coordinatization by several non-isomorphic semifields, and all these are flock semifields hence right primitive. However, it is not clear to us whether they are left primitive.

NOTE. The duals of flock semifields are always left primitive, by Corollary 7.3. But the duals of flock semifields are not flock semifields unless the semifield is a field.

Acknowledgement

The second author thanks Flaminio Flamini and the other researchers at the University of Rome for their tremendous support. The work was done when the second author was a visiting professor at the University of Texas at Arlington, 2008-9. The author expresses his cordial thanks to Professors Jianping Zu and the mathematics department at UTA

REFERENCES

[1] M. BILIOTTI – V. JHA – N. L. JOHNSON: *Foundations of Translation Planes*, Marcel Dekker, Inc., New York, Basel.

[2] S. D. COHEN: *Primitive roots in the quadratic extension of a finite field*, J. London Math. Soc., **27** (1983) 221–228.

[3] M. CORDERO – V. JHA: *On the multiplicative structure of quasifields and semifields, cyclic and acyclic loops*, submitted.

[4] M. CORDERO – V. JHA: *Fractional dimensional semifield planes of odd order*, submitted.

[5] P. DEMBOWSKI: *Finite Geometries*, Springer Verlag, Berlin, Heidelberg, New York, 1968.

[6] H. DAVENPORT: *On primitive roots in finite fields*, Quarterly J Math (Oxford), **8** (1937) 308–312.

[7] J. C. FISHER – N. L. JOHNSON: *Fano planes in subregular spreads*, Advances in Geometry, to appear.

[8] H. GEVAERT – N. L. JOHNOSN: *Flocks of quadratic cones, generalized quadrangles and translation planes*, Geom. Dedicata, **27** (1981) 301–317.

[9] I. R. HENTZEL – I. F. RÚA: *Primitivity of finite semifields with 64 and 81 elements*, International J. Algebra and Computation, **17** (2007) 1411–1429.

[10] D. R. Hughes – F. C. Piper: *Projective Planes*, Springer Verlag, New York, 1973.

[11] V. Jha – N. L. Johnson: *The dimension of a subplane of a translation plane*, Bulletin of the Belgian Math. Soc. to appear.

[12] N. L. Johnson – V. Jha – M. Biliotti: *Handbook on Translation Planes*, Taylor and Francis Group, 2007.

[13] N. L. Johnson: *Fano configurations in translation planes*, Note di Mathematica **27** (2007) 21–38.

[14] N. L. Johnson: *Semifield flocks of quadratic cones*, Simon Stevin, **61** (1987) 313–324.

[15] W. Kantor: *Finite semifields*, Proc. Conf. at Pingree Park, (2005) 103–114.

[16] D. Mills – G. McNay: *Primitive roots in cubic extensions of finite fields*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), (2002) 239–250, Springer, Berlin.

[17] A. O. Leone – M. J. de Resmini: *Subplanes of the derived Hughes planes of order 25*, Simon Stevin, **67** (1993) 289–322.

[18] G. Menichetti: *On a Kaplansky Conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra, **47** (1977) 400–410.

[19] H. Neumann: *On some finite non-desarguesian planes*, Arch. Math., **6** (1955) 36–40.

[20] L. Puccio – M. J. de Resmini: *Subplanes of the Hughes planes of order 25*, Arch. Math. (Basel), (1987) 151–165.

[21] I. F. Rúa: *Primitive and non-primitive finite semifields*, Communications in Algebra, **22** (2004) 791–803.

[22] T. Schneider: *Transzendenzuntersuchen periodischer Funktionen I*, J. Reine Angew, Math, **172** (1934) 65–69.

[23] T. Schneider: *Transzendenzuntersuchen periodischer Funktionen II*, J. Reine Angew, Math, **172** (1934)b 70–74.

[24] R. J. Walker: *Determination of division algebras with 32 elements*, Proc. Symposia Appl. Math., **15** (1962) 83–85.

[25] G. P. Wene: *On the multiplicative structure of finite division rings*, Aequationes Math., **41** (1991) 222–233.

[26] G. P. Wene: *Semifields of dimension* $2n$*,* $n \geq 3$*, over* $GF(p^m)$ *that have left primitive elements*, Geom. Dediciata, **41** (1992) 1–3.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo degli Autori:

Minerva Cordero – Mathematics Department – University of Texas – Arlington, TX
E-mail:cordero@uta.edu

Vikram Jha – 2 Marchmont Terrace – Glasgow, G12 9LT – Scotland
E-mail: vjha267@googlemail.com