NEW RESULTS IN FINITE GEOMETRIES PERTAINING TO ALBERT-LIKE SEMIFIELDS

by

ANGELA MICHELLE BROWN

Presented to the Faculty of the Graduate School of
The University of Texas at Arlington in Partial Fulfillment
of the Requirements
for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT ARLINGTON
May 2012

For my parents and my sisters. Thank you for always believing in me.

ACKNOWLEDGEMENTS

First of all, I want to thank my advisor, Dr. Cordero for being there for me as I have completed my dissertation. It has been an honor being your first Ph.D. student and I would not trade it for the world.

Also thank you to my committee members, Dr. Gornet, Dr. Grantcharov, Dr. Jorgensen, and Dr. Vancliff for taking the time out of your schedules to read my dissertation and serve on my committee. Your feedback has been extremely helpful. I need to especially thank Dr. Vancliff. Without your advice and guidance, I do not think I would have made it through graduate school.

I also need to thank the two women than started me on this journey. To the two Dr. J's, Dr. Jensen and Dr. Jones, without you there to push me, I would not have realized my full potential. Dr. Jensen, thanks for putting up with me even more as I finished my master's degree under your tutelage.

To the A^3 girls that complete A^4, thanks for being a sounding board as we have all worked on our Ph.D.s. You all are some the the best friends I could have.

Thank you to all of my friends at UT-Arlington that have been there with me through this awesome journey. Whether through mathematics or sports, I have met some of the people that will be friends for life.

Last of all, I need to thank my family that has supported me throughout. Mom and Dad, thank you for making me believe that being a strong, smart, independent woman is not a bad thing. Mandi thanks for always being there for me and never letting me give up on myself. Jess, thank you for being the best sounding board in the world. You will listen to me speak about mathematics at any time and actually

ask question until you understand. Thank you for actually being interested in what I do. I know how hard that is for other mathematicians, much less my sister with no formal math training. Thank you all for everything you have done for me.

April 11, 2012

ABSTRACT

NEW RESULTS IN FINITE GEOMETRIES PERTAINING TO ALBERT-LIKE SEMIFIELDS

Angela Michelle Brown, Ph.D.

The University of Texas at Arlington, 2012

Supervising Professor: Minerva Cordero

One of the most widely studied class of semifields are the generalized twisted fields defined by Albert in the 50s and 60s. The collineation groups of generalized twisted field planes have been completely described. In a series of papers Cordero and Figueroa studied semifields with an autotopism that acts transitively on one side of the autotopism triangle, equivalently the plane admits an autotopism which induces a permutation on a side of the autotopism triangle of order a p-primitive divisor of $p^r - 1$. They showed that with some minor exceptions the plane is a generalized twisted field plane. These planes π are coordinatized by pre-semifields $(K, +, \circ)$ where $x \circ y = \sum_{i=0}^{n-1} a_i x^{(i)} y^{(e_i)}$ for $x, y \in K = GF(p^n)$. Hence either π is a generalized twisted field plane or there exist at least two non-zero indices u, v such that $a_u \neq 0 \neq a_v$. In this case the pre-semifield has the product $x \circ y = xy + a_u x^{(u)} y^{(e_u)} + a_v x^{(v)} y^{(e_v)}$. In this work we study in depth the case in which there are precisely two nonzero indices. In this case the multiplication behaves much like a generalization of Albert's generalized twisted fields. For many of the cases, these semifields are generalized twisted fields. We provide a variety of examples in which these semifields are not generalized twisted

fields. For these we study the collineations of the semifield planes they coordinatize to help shed some light into the classification of the semifield planes of this type.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Semifields are algebraic structures that were first discovered by Dickson [17] in 1905. A literature review shows that the next known semifields were not discovered until 1951. Among these semifields were Albert's twisted fields, which are semifields over $GF(p^n)$ with the product $x*y = xy^{p^m} - cx^{p^m}y$ where $1 \leq m < n$ and $c \neq a^{p^m-1}$ for $a \in GF(p^n)$[1]. Albert computed the collineation groups of the corresponding semifield planes in 1958 [2]. He then generalized these results in 1960 to semifields over $GF(p^n)$ with product $x * y = xy - cx^{\alpha}y^{\beta}$ where $c \neq x^{\alpha-1}y^{\beta-1}$, α and $\beta \in \mathrm{Aut}(GF(p^n)$, and x and $y \in GF(p^n)$ [5]. Semifields of this type and the projective planes they coordinatize have been studied extensively in the work of Albert [4] and the full collineation group of these semifields was determined by Biliotti, Johnson, and Jha [7] in 1999.

Cordero and Figueroa, in a series of papers, [12]-[15] and [18], studied semifields of order p^n, p prime, with an autotopism that acts transitively on one side of the autotopism triangle. The plane also admits an autotopism which induces a permutation α on a side of the autotopism triangle of order a p-primitive divisor of $p^n - 1$, that is, $|\alpha| \mid p^n - 1$ but $|\alpha| \nmid p^i - 1$ for $0 \leq i \leq n-1$. They showed that in most cases these planes are generalized twisted field planes.

More specifically, let V denote the n-dimensional vector space over $GF(p^n)$ consisting of all the vectors of the form $(x) = (x^{(0)}, x^{(1)}, \cdots, x^{(n-1)})$ where $x \in GF(p^n)$ and $x^{(i)} = x^{p^i}$ for $i = 0, 1, \cdots, n-1$ and p is a prime number. The group of all automorphisms of V over $GF(p)$, $Aut(V)$, consists of the non-singular matrices of the form as shown in [26]

$$M = \begin{pmatrix} a_0 & a_{n-1}^{(1)} & \dots & a_1^{(n-1)} \\ a_1 & a_0^{(1)} & \dots & a_2^{(n-1)} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_{n-2}^{(1)} & \dots & a_0^{(n-1)} \end{pmatrix}$$

where $a_0, a_1, \cdots, a_{n-1} \in K$; we denote this matrix by $M = [a_0, a_1, \ldots, a_{n-1}]^t$.

For $0 \leq k \leq n-1$ and $k \in K$, let

$$T_k(c) = [0, \cdots, c, \cdots, 0]^t$$

where c is in the k-th position and the rest of the entries are zero. We will denote any matrix of the form $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ by $\mathrm{diag}(A, B)$.

Let π be a non-Desarguesian semifield plane of order $p^n \neq 2^6$ that admits an autotopism g_0 of order h where h is a prime p-primitive divisor of $p^n - 1$. We consider $V \oplus V$ as the vector space associated to the affine plane π and $V(\infty) = \{((0), (x)) | x \in K\}$ is a component of a spread of π in $V \oplus V$.

In [15] Cordero and Figueroa proved the following:

Theorem 1.1 (Result 1, [15]). *Let π be a non-Desarguesian semifield plane of order p^n. If π admits a collineation g_0 of order h, a p-primitive prime divisor of $p^n - 1$, then*

1. *There exists a spread set $\{V(0), V(\infty)\} \cup \{V(M(y)) | y \in K - \{0\}\}$ for π in $V \oplus V$ such that $V(\infty)$ is the shear axis and for $y \in K, y \neq 0$,*

$$M(y) = [a_0 y^{(e_0)}, a_1 y^{(e_1)}, \ldots, a_{n-1} y^{(e_{n-1})}]^t \in Aut(V).$$

2. *$g_0 = diag(T_0(\gamma), T_0(\delta))$, where γ and δ are two different elements in K, both of order h.*

3. $\left(\frac{\delta}{\gamma}\right)^{(e_i)} = \frac{\delta}{\gamma^{(i)}}$, *for each i such that $a_i \neq 0$.*

Notice that on Result 3.1 above the plane π is coordinatized by the pre-semifield $(K, +, \circ)$ where

$$x \circ y = \sum_{i=0}^{n-1} a_i x^{(i)} y^{(e_i)}$$

for $x, y \in K$. Hence either π is a generalized twisted field plane or there exist at least two non-zero indices u and v such that $a_u \neq 0 \neq a_v$. In this work we study the case in which there are precisely two nonzero coefficients, so the multiplication on the pre-semifield behaves like a generalization of the multiplication of a pre-semifield that defines the generalized twisted fields. Hence the product is of the form

$$x \circ y = xy + Ax^{(u)}y^{(e_u)} + Bx^{(v)}y^{(e_v)} \tag{1.1}$$

In [15] an example of such a product for $GF(3^6)$ was given:

Theorem 1.2 (Result 2, [15]). *Let π be a non-Desarguesian plane which is not a generalized twisted field plane of order 3^6. Suppose π admits an autotopism g_0 of order 7, a 3-primitive prime divisor of $3^6 - 1$. Then π can be coordinatized by the pre-semifield $GF(3^6, +, \circ)$, where*

$$x \circ y = xy + \gamma x^{(1)} y^{(3)} + \gamma^{13} x^{(3)} y^{(1)}$$

and γ is a primitive element in $GF(3^6)$ that satisfies $\gamma^2 + \gamma + 2 = 0$. Moreover, π has an autotopism of order 3 that normalizes g_0.

They also showed that all semifields defined on $GF(3^4)$ with this product are generalized twisted fields. In [13] they proved the following result.

Theorem 1.3 (Theorem 4.1, [13]). *Let π be a non-Desarguesian semifield plane of order p^n, where p is an odd prime number and $n \geq 3$. Let $\triangle$ be an autotopism triangle of π and let $\overline{G}$ be the group induced by the automorphism group G of π on a side ℓ of $\triangle$. If $\overline{G}$ has an element of order $\dfrac{p^n-1}{\mu}$ where μ is an integer dividing n, then π is a generalized twisted field plane.*

In Chapter 2 we introduce the terminology and theorems needed for understanding of the topic, including the terms given in the above description. Much of this information is introduced in [19], but can also be found in [16],[20], and [21].

In Chapter 3 we discuss the motivation for our research, as well as give the results and examples. Our goal is to provide information that will help in the classification problems of semifields with an autotopism as described above. These semifields are defined in $GF(p^n)$ by the following product;

$$x \circ y = xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha}$$

where $S(K, \alpha, \beta, A, B)$ denotes a semifield with the above product. For this semifield, $K = GF(p^n)$, $\alpha : x \mapsto x^{p^a}$ and $\beta : x \mapsto x^{p^b}$ are in $\mathrm{Aut}(K)$, and $A, B \in K$. The associated plane will be denoted $\pi(K, \alpha, \beta, A, B)$. First we discuss the autotopism homologies of $\pi(K, \alpha, \beta, A, B)$. We then discuss the order of the nuclei. With the aid of the computer we were able to find parameters that define semifields with the product as above. For the semifields over $GF(3^5)$ we compute the elements in the nuclei. For the ones defined over $GF(3^6)$ following the method of Cordero and Figueroa, we computed the normalizer of the group generated by the autotopism g_0 of order h, a $p-$primitive divisor of $3^6 - 1$. We show that for certain coefficients these semifields are not isomorphic to generalized twisted fields. The main motivation is to be able to classify the semifields that correspond to the new product.

CHAPTER 2

PRELIMINARIES

2.1 Semifields

Definition 1. *A **semifield** is a set S together with two binary operations $+$ and $\cdot$ such that*

- *S under addition is an abelian group.*
- *For $a, b \in S$ if $a \cdot b = 0$, then $a = 0$ or $b = 0$*
- *The distributive laws hold; that is:*

  $$a \cdot (b + c) = a \cdot b + a \cdot c.$$

  $$(a + b) \cdot c = a \cdot c + b \cdot c.$$

- *There exist $1 \in S$ such that $1 \cdot a = a \cdot 1 = a$.*

A semifield is **proper** if it is not a field; that is, if the multiplication is not associative. Actually, under multiplication $(S, \cdot)$ forms an algebraic system called a loop.

Definition 2. *A **loop** is a set L with a binary operation $\star$ satisfying:*

- *There exists an element $e \in L$ such that $a \star e = e \star a = a$ for all $a \in L$.*
- *Given two of the elements $a, b, c \in L$, the equation $a \star b = c$ uniquely determines the third.*

The element e is called the identity of L.

The set $\{e, a, b, c, d\}$ with operation $\star$ as shown in Table 2.1 is a loop with identity element e. Notice that $c \star (b \star a) = a$ while $(c \star b) \star a = c$, so the operation is not associative.

Definition 3. *The **order** of a semifield $\mathcal{S} = (S, +, \cdot)$ is the cardinality of the set S.*

Table 2.1. Example of a Loop

$\star$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

In this work we will be concerned exclusively with **finite** semifields, i.e. semifields with a finite number of elements.

Theorem 2.1 (Theorem 6.1, [22])**.** *Every proper finite semifield has order p^n, where p is prime, $n \geq 3$, and $p^n \geq 16$.*

If a semifield has prime order p then the semifield is actually isomorphic to the field $GF(p)$. Similarly a semifield of order p^2, p prime, is isomorphic to $GF(p^2)$.

Other algebraic structures closely related to semifields are the pre-semifields.

Definition 4. *A system $\mathcal{S} = (S, +, \cdot)$ is a **pre-semifield** if it satisfies all the axioms of a semifield except possibly having a multiplicative identity.*

By redefining the multiplication on a pre-semifield $(S, +, \cdot)$ we obtain a semifield $(S, +, *)$ as follows: choose an element $e \in S$. For $x, y \in S$ there exist $x', y' \in S$ such that $x = x' \cdot e$ and $y = e \cdot y'$. Define $x * y = (x' \cdot e) * (e \cdot y') = x' \cdot y'$. With this multiplication $(S, +, *)$ is a semifield with multiplicative identity $e \cdot e$. Notice $x * e = (x' \cdot e) * (e \cdot e) = x' \cdot e = x$ and $e * y = (e \cdot e) * (e \cdot y') = e \cdot y' = y$.

Since proper semifields are not associative and not necessarily commutative structures, we study the degree of associativity and commutativity they possess. These properties help distinguish between different semifields that have the same order. The nuclei of a semifield define degrees of associativity and the center defines the degree of commutativity. Each of the nuclei and the center are indeed fields and the semifield is a vector space over each of these.

Definition 5. *Let $(S, +, *)$ be a semifield. The left, middle, and right nuclei are defined as follows, respectively:*

- ***Left nucleus**: $\mathcal{N}_l = \{x \in S : (x * a) * b = x * (a * b), a, b \in S\}$.*
- ***Middle nucleus**: $\mathcal{N}_m = \{x \in S : (a * x) * b = a * (x * b), a, b \in S\}$.*
- ***Right nucleus**: $\mathcal{N}_r = \{x \in S : (a * b) * x = a * (b * x), a, b \in S\}$.*
- *The intersection of the three nuclei is called the **nucleus** and is denoted $\mathcal{N}$.*

Definition 6. *Let $(S, +, *)$ be a semifield. The **center** of $\mathcal{S}$ is the set $Z = \{x \in \mathcal{N} : x * y = y * x \text{ for all } y \in S\}$.*

In the finite case, by Wedderburn's Theorem (Result 1.3, [19]), associativity implies commutativity; hence the nucleus and the center coincide.

2.2 Planes

Finite geometries consist of a finite set of points and lines satisfying certain axioms. We define two finite geometries and in the next section we will use semifields to coordinatize these.

Definition 7. *A **finite affine plane** consists of a finite set of points together with a collection of its subsets, called lines, such that:*

- *Two distinct points are on only one line.*
- *For line ℓ and a point $p \notin \ell$ there is a unique line m containing p such that $m \cap \ell = \emptyset$.*
- *There are three points not all of which are collinear.*

Definition 8. *A **finite projective plane** is a set of elements, called points, together with a collection of certain subsets called lines such that:*

- *Any two distinct points lie on only one line.*
- *Any two lines intersect at only one point.*
- *There exist four points no three of which are collinear.*

Notice that in a finite projective plane parallel lines do not exist.

Regarding the number of points in a line and the number of lines through a point of a projective or affine plane we have the following result:

Theorem 2.2 (Theorem 3.5, [19]). *For a projective plane $\mathcal{P}$ there exists an integer n such that:*

- *Every line has exactly $n+1$ points.*
- *Every point is in $n+1$ lines.*
- *There are n^2+n+1 points and n^2+n+1 lines.*

Definition 9. *If $\mathcal{P}$ is a finite projective plane then the integer n is called the **order** of $\mathcal{P}$.*

Just as we can discuss relationships between algebraic structures, we have similar definitions for projective planes.

Definition 10. *Two projective planes $\mathcal{P}_1$ and $\mathcal{P}_2$ are **isomorphic** if there exists a bijection σ of the points of $\mathcal{P}_1$ onto the points of $\mathcal{P}_2$ mapping lines of $\mathcal{P}_1$ onto lines of $\mathcal{P}_2$ and satisfying $p \in \ell$ if and only if $\sigma(p) \in \sigma(\ell)$ for all points p of $\mathcal{P}_1$ and all lines ℓ of $\mathcal{P}_1$. An isomorphism of a plane onto itself is called a **collineation.***

The set of collineations of a projective plane $\mathcal{P}$ form a group under composition denoted $\mathrm{Aut}(\mathcal{P})$. Collineations of finite projective planes have the following property:

Theorem 2.3 (Theorem 4.9, [19]). *If $\mathcal{P}$ is a projective plane and $\alpha \neq 1$ is a collineation of $\mathcal{P}$ fixing a line ℓ pointwise then there is a point V in $\mathcal{P}$ that is fixed linewise by α. Furthermore α fixes no other line or point.*

In the above result the mapping α is said to fix a line ℓ *pointwise* if for every point A in the line, $\alpha(A) = A$. Similarly α is said to fix a point B *linewise* if for every line ℓ through B, $\alpha(\ell) = \ell$. Notice the image of a point A under a mapping α is usually denoted A^α.

Definition 11. *If a collineation α fixes a line ℓ pointwise and a point V linewise, then α is called a (V,ℓ)-**perspectivity**. The line ℓ is called the **axis** of α and the point V is called the **center** of α.*

Definition 12. *Let α be a (V,ℓ)-perspectivity. Then*

- *If $V \in \ell$, α is called an **elation**. See Figure 2.1.*

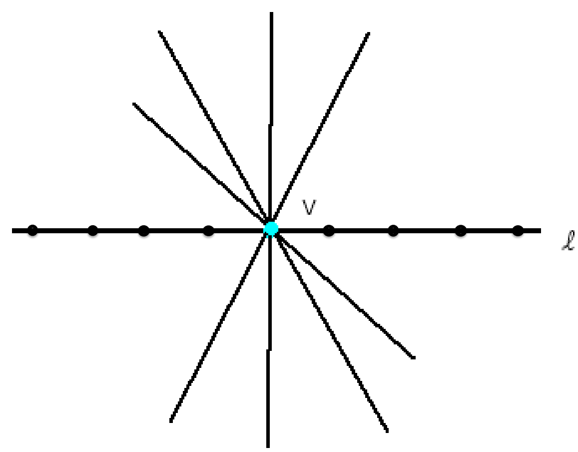

Figure 2.1. Elation.

- *If $V \notin \ell$, α is called a **homology**. See Figure 2.2.*

Let $\mathcal{P}(\mathcal{S})$ be a semifield plane coordinatized by the semifield $\mathcal{S} = (S,+,*)$ and let $\Pi = \mathrm{Aut}(\mathcal{P}(\mathcal{S}))$ be the collineation group of $\mathcal{P}(\mathcal{S})$. Under composition the following subsets form subgroups of $\Pi = \mathrm{Aut}(\mathcal{P}(\mathcal{S}))$.

Lemma 2.1 (Lemma 4.7, [21]). *Let $\mathcal{P}$ be a projective plane and let P be a point of $\mathcal{P}$ and ℓ be a line of $\mathcal{P}$. The following statements hold:*

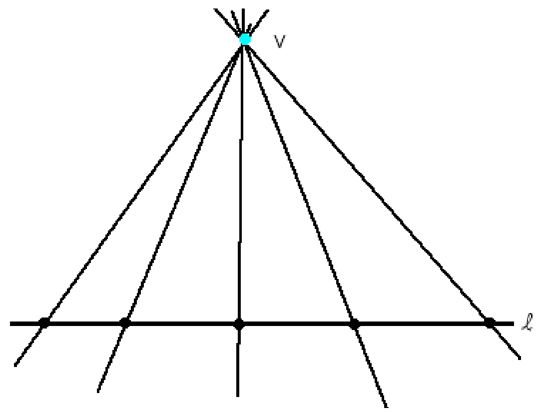

Figure 2.2. Homology.

(i) *The set of all perspectivities of $\mathcal{P}$ with axis ℓ forms a group under composition.*

(ii) *The set of all perspectivities of $\mathcal{P}$ with center P forms a group under composition.*

(iii) *The set of all perspectivities of $\mathcal{P}$ with center P and axis ℓ forms a group under composition.*

(iv) *The set of all elations of $\mathcal{P}$ with axis ℓ forms a group under composition.*

(v) *The set of all elations of $\mathcal{P}$ with center P forms a group under composition.*

2.3 Relationship between Semifields and Projective Planes

Finite fields are not the only algebraic structures that can be used to coordinatize a projective plane. In fact we can use any set R:

For a finite projective plane $\mathcal{P}$ of order n let $U, V, \mathcal{O}, I$ be four points of $\mathcal{P}$, no three of which are collinear. Take a set R of n elements such that: $0, 1 \in R$ and choose a point $\infty \notin R$. Fix a 1-1 correspondence α between R and the points in $\mathcal{O}I - (UV \cap \mathcal{O}I)$ where $\alpha(0) = \mathcal{O}$ and $\alpha(1) = I$.

To a point $P \in \mathcal{O}I - (UV \cap \mathcal{O}I)$ assign the coordinates (b, b) where $b \in R$ corresponds to P under the correspondence α.

If $P \notin \mathcal{O}I$, and $P \notin UV$, consider the lines PU and PV. To P assign the coordinates (a, b) where $PV \cap \mathcal{O}I = (a, a)$ and $PU \cap \mathcal{O}I = (b, b)$. For $P \in UV$ and $P \neq V$, assign to P the coordinate (m), where $\mathcal{O}P \cap IV = (1, m)$.

To point V assign the coordinate (∞) where $\infty \notin R$. The whole plane is coordinatized as shown in figure 2.3:

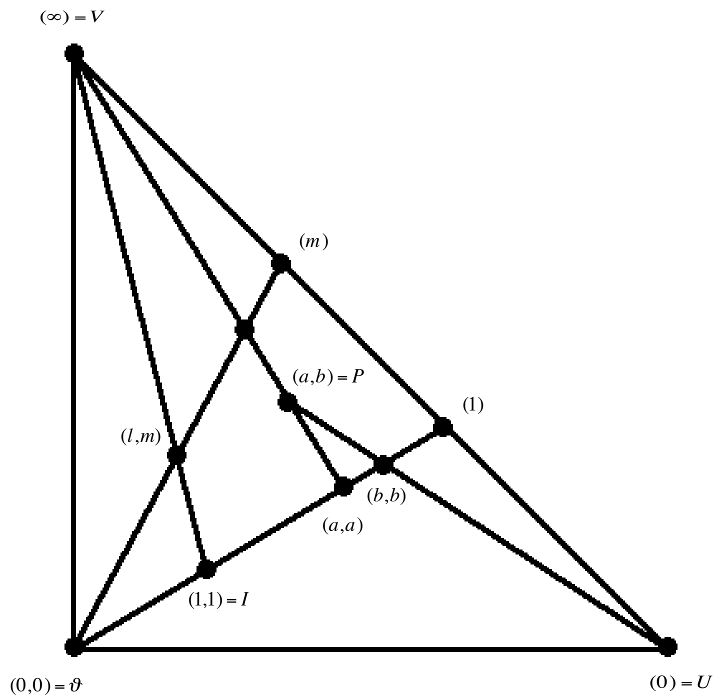

Figure 2.3. Coordinization of the Projective Plane.

The line through (m) and $(0, k)$ has coordinates $[m, k]$, where we say that $m =$ is the *slope* of the line and k is the $y-$ *intercept*. The line through (∞) and $(k, 0)$ has coordinates $[\infty, k]$; we say it has *slope* $\infty =$ and $x-$ *intercept* k. The line through the points U and V is called the **line at infinity** and is denoted by ℓ_∞ or $[\infty]$.

We can coordinatize a projective plane with elements from a semifield as we have shown above. We want to know what information we can obtain concerning the collineations of projective planes coordinatized by semifields.

The following result from [19] gives the relationship between the homologies of the plane and the nuclei of the semifield that coordinatizes the plane.

Theorem 2.4 (Theorem 8.2, [19])**.** *Let $\mathcal{P}(\mathcal{S})$ be a projective plane coordinatized by the semifield $\mathcal{S}$.*

(i) The group $\Pi_{(V,\mathcal{O}U)}$ of $(V,\mathcal{O}U)$- homologies of $\mathcal{P}(\mathcal{S})$ is isomorphic to ${\mathcal{N}_l}^{\times}$.

(ii) The group $\Pi_{(U,\mathcal{O}V)}$ of $(U,\mathcal{O}V)$- homologies of $\mathcal{P}(\mathcal{S})$ is isomorphic to ${\mathcal{N}_m}^{\times}$.

(iii) The group $\Pi_{(\mathcal{O},UV)}$ of $(\mathcal{O},UV)$- homologies of $\mathcal{P}(\mathcal{S})$ is isomorphic to ${\mathcal{N}_r}^{\times}$.

If we can find the structure of the different groups of homologies, we can then find the order of each of the nuclei. Conversely, if we know the order of the nuclei, then we can find the order of the group of homologies.

For the elations of a semifield plane, we have the following definitions and results:

Definition 13. *If $\mathcal{P}(\mathcal{S})$ is a semifield plane coordinatized by the semifield $\mathcal{S} = (S,+,*)$ and $\Pi = Aut(\mathcal{P}(\mathcal{S}))$ is the collineation group of $\mathcal{P}(\mathcal{S})$, then any elation with center (∞) and affine axis is called a **shear**. The group of shears with axis $\mathcal{O}V$ is denoted $\Pi_{((\infty),\mathcal{O}V)}$.*

Definition 14. *If $\mathcal{P}(\mathcal{S})$ is a proper semifield plane, then any elation with center any point on ℓ_∞ and axis ℓ_∞ is called a **translation**. The group of translations is denoted $\Pi_{([\infty],[\infty])}$.*

Lemma 2.2 (Lemma 7.10, [19])**.** *Let $\mathcal{P}(\mathcal{S})$ be a semifield plane coordinatized by the semifield $\mathcal{S} = (S,+,*)$ and let $\Pi = Aut(\mathcal{P}(\mathcal{S}))$ be the collineation group of $\mathcal{P}(\mathcal{S})$. Then $\Pi_{([\infty],[\infty])} \cong (\mathcal{S},+) \oplus (\mathcal{S},+)$.*

In Chapter VI of [19] the authors define the dual plane of a projective plane. For any projective plane $\mathcal{P}$ the **dual** of the plane, $\mathcal{P}^*$, is defined by taking the points of the new plane to be the lines of the given plane and the lines of the new plane to be the points of the given plane. Notice that a projective plane $\mathcal{P}$ can be coordinatized by a semifield if and only if $\mathcal{P}$ is a translation plane with respect to $[\infty]$ and the dual of a translation plane with respect to (∞). Planes coordinatized by fields, which are called **Desarguesian** planes, fall in this category. Since a proper semifield plane is not Desarguesian, we have the following lemma:

Lemma 2.3 (Lemma 8.3, [19]). *If $\mathcal{P}(\mathcal{S})$is a proper semifield plane, then $Aut(\mathcal{P}(\mathcal{S}))$ fixes (∞) and ℓ_∞.*

To proof the above lemma, if one assumes that either the point or the line at ∞ are not fixed by a collineation of the plane, then the plane is forced to be Desarguesian, which is then not a proper semifield plane. Since the point (∞) and the line ℓ_∞ are fixed, then the only types of elations in a semifield are the shears and elations as defined above.

If $\mathcal{P}(\mathcal{S})$ is a semifield plane coordinatized by the semifield $\mathcal{S} = (S, +, *)$ then $\Pi = \mathrm{Aut}(\mathcal{P}(\mathcal{S}))$, the full collineation group of $\mathcal{P}(\mathcal{S})$, has the following decomposition:

Lemma 2.4 (Lemma 8.4, [19]). *Let $\mathcal{P}(\mathcal{S})$ be a proper semifield plane and let $\Pi = Aut(\mathcal{P}(\mathcal{S}))$ be its collineation group. If $\Sigma = \Pi_{([\infty],[\infty])} \cdot \Pi_{((\infty),\mathcal{O}V)}$, then*

(i) Σ *is a group.*

(ii) $\Pi_{([\infty],[\infty])} \lhd \Sigma$

(iii) $\Pi_{([\infty],[\infty])} \cap \Pi_{((\infty),\mathcal{O}V)} = 1$.

Because Σ contains all the elations, it is generated by these elation and we have the following lemma:

Lemma 2.5 (Lemma 8.5, [19]). *If $\mathcal{S}$ is a proper semifield, then $\Sigma \lhd \Pi$ where $\Pi = Aut(\mathcal{P}(\mathcal{S}))$.*

Definition 15. *For a semifield plane $\mathcal{P}(\mathcal{S})$, the group of collineations fixing the points A, B, and C on a triangle where $A = (\infty)$, B is a point on ℓ_∞, and C is any point* *not on ℓ_∞ is called the **autotopism group of** $\mathcal{P}(\mathcal{S})$, denoted Λ. The fixed triangle is called the **autotopism triangle**.*

Notice that the set of collineations fixing a triangle form a group under composition as it is the stabilizer of the points that form the triangle.

Theorem 2.5 (Theorem 8.6, [19])**.** *Let $\mathcal{P}(\mathcal{S})$ be a proper semifield plane and let $\Pi = Aut(\mathcal{P}(\mathcal{S}))$. If $\Sigma = \Pi_{([\infty],[\infty])} \cdot \Pi_{((\infty),\mathcal{O}V)}$, and Λ is the autotopism group of $\mathcal{P}(\mathcal{S})$, then*

(i) $\Pi = \Sigma\Lambda$

(ii) $\Sigma \cap \Lambda = 1$.

From this theorem it follows that Σ and Λ have no elements in common except for the identity. Since they are distinct and Σ contains all the elations, then Λ does not contain any elations. To be able to find the autotopism group of a semifield plane, we need to first discuss what autotopisms look like for a semifield and what information autotopisms provide about the plane.

Since (∞) and $[\infty]$ are fixed by any collineation of a semifield plane, then this essentially determines the autotopism triangle. We already have (∞), another point on $[\infty]$, and since we want three points that are not collinear, the third point will not be in the line $[\infty]$. It is standard convention to use the points $\mathcal{O} = (0,0), U = (0)$, and $V = (\infty)$, and the lines that correspond to them, $\mathcal{O}U, UV$, and $[\infty]$. Now let $\alpha \in \Lambda$. The points and lines just given are fixed by α, so α acts as a permutation on the lines. Then α defines three permutations F, G, and H as follows: For $(m) \in [\infty]$, $(m)^\alpha = H(m)$; for $(a,0) \in [0,0]$ $(a,0)^\alpha = (F(a),0)$; and for $(0,b) \in [0]$, we have $(0,b)^\alpha = (0,G(b))$, where $F(0) = G(0) = H(0) = 0$. For any point (x,y) in the plane, $(x,y)^\alpha = (F(x),G(y))$ and for any line $[m,k]$ of the plane, $[m,k]^\alpha = [H(m),G(k)]$. It follows that F, G, and H are additive functions in $\mathcal{S}$. (See [19], page 175.) If the point $[x,y]$ is on the line $[m,k]$ then the point $(F(x),G(y))$ is on the line $[H(m),G(k)]$.

Therefore we have $x*m+y=k$ and $F(x)*H(m)+G(y)=G(x*m+y)$. Letting $y=0$ we get $H(m)*F(x)=G(xm)$. Conversely if we have a triple of nonsingular additive maps with $H(m)*F(x)=G(xm)$ we can define an autotopism by $(m)^\alpha=H(m)$ and $(x,y)^\alpha=(F(x),G(y))$. An analogous proof is given on [19] where right actions are used instead of left actions as above.

The autotopism group of a semifield plane $\mathcal{P}(\mathcal{S})$ is isomorphic to the autotopism group of its coordinatizing semifield $\mathcal{S}$ as the next result shows.

Lemma 2.6 (Lemma 8.8, [19])**.** *If $\mathcal{S}$ is a semifield, then the autotopism group of $\mathcal{S}$ is isomorphic to the autotopism group of $\mathcal{P}(\mathcal{S})$.*

Definition 16. *Two semifields $(S,+,\circ)$ and $(S',+,*)$ are* ***isotopic*** *if there is a set of bijective additive mappings (F,G,H) from S onto S' such that*

$$F(x)\circ H(n)=G(x*y) \text{ for all } x,y\in S.$$

The following theorem due to Albert ([4]) gives the relationship between two different semifields and the planes they coordinatize.

Theorem 2.6 (Theorem 6, [4])**.** *Two semifield planes are isomorphic if and only if the semifields that coordinatize them are isotopic.*

2.4 Some Known Semifields

In 1906 Dickson discovered the first semifields which are now referred to as *Dickson semifields*. These semifields are defined as follows: Let $K=GF(p^n)$ where p is an odd prime and $n>1$. Let f be any element of K that is not a square. Let S be a two-dimensional vector space over K with basis elements 1 and λ. If θ is the automorphism of K given by $x^\theta=x^{p^r}, 1\le r<n$, define a multiplication in K by

$(a + \lambda b)(c + \lambda d) = (ac + f(bd)^{\theta}) + \lambda(ad + bc)$. Then with this operation and field addition, S becomes a semifield. For more information see [17].

In 1958 Albert first discovered what he called *twisted fields*. For more information see [2]-[5]. Let $K = GF(p^n)$ where p is prime and define a new multiplication on K as follows:

$$x \circ y = xy^{p^m} - cx^{p^m}y$$

where $1 \leq m < n, c \neq a^{p^m-1}$ for $a \in GF(p^n)$ With the field addition and this multiplication K becomes a pre-semifield. In 1961 Albert further generalized this result by defining a new multiplication on K; the pre-semifields with this new product are called **generalized twisted fields**. The new multiplication in K was defined as follows:

$$x \circ y = xy - cx^{\alpha}y^{\beta}$$

where $\alpha, \beta \in$ Aut $(GF(p^n)), c \neq x^{\alpha-1}y^{\beta-1}$ and $x, y \in GF(p^n)$. Here $x^{\alpha-1}$ stands for $\dfrac{x^{\alpha}}{x}$. With the field addition and this multiplication K becomes a pre-semifield.

CHAPTER 3

RESULTS

3.1 Introduction

In this chapter we present the results of our study of semifield planes that are coordinatized by the pre-semifield with product

$$x \circ y = xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha}. \tag{3.1}$$

From this point on, we will name these semifields by their defining components. Namely we will call them $S(K, \alpha, \beta, A, B)$ where $K = GF(p^n)$, $\alpha : x \mapsto x^{p^a}$ and $\beta : x \mapsto x^{p^b} \in \mathrm{Aut}(K)$, and $A, B \in K$. The associated plane will be denoted $\pi(K, \alpha, \beta, A, B)$.

The product from 3.1 arose from a series of papers by Cordero and Figueroa[12]-[15] and [18]. Recall Albert's generalized twisted fields which have multiplication defined by

$$x \circ y = xy - cx^{\alpha}y^{\beta}$$

where $\alpha, \beta \in$ Aut $(GF(p^n)), c \neq x^{\alpha-1}y^{\beta-1}$ and $x, y \in GF(p^n)$. These are one of the most widely studied class of semifields. Albert began with a specific case which he called twisted fields as shown in [3] in 1959. He then further generalized these examples in [5] in 1961. The collineation groups of generalized twisted field planes were studied in [2] and [4] and were completely described in [7].

Cordero and Figueroa studied semifields with an autotopism that acts transitively on one side of the autotopism triangle. Equivalently the plane admits an autotopism which induces a permutation on a side of the autotopism triangle of order a p-primitive divisor of $p^r - 1$. They showed that with some minor exceptions the plane is a generalized twisted field plane.

More specifically, let V denote the n-dimensional vector space over $GF(p^n)$ consisting of all the vectors of the form $(x) = (x^{(0)}, x^{(1)}, \cdots, x^{(n-1)})$ where $x \in GF(p^n)$ and $x^{(i)} = x^{p^i}$ for $i = 0, 1, \cdots, n-1$ and p is a prime number. The group of all automorphisms of V over $GF(p), \mathrm{Aut}(V)$, consists of the non-singular matrices of the form as shown in [26]

$$M = \begin{pmatrix} a_0 & a_{n-1}^{(1)} & \dots & a_1^{(n-1)} \\ a_1 & a_0^{(1)} & \dots & a_2^{(n-1)} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_{n-2}^{(1)} & \dots & a_0^{(n-1)} \end{pmatrix}$$

where $a_0, a_1, \cdots, a_{n-1} \in K$; we denote this matrix by $M = [a_0, a_1, \ldots, a_{n-1}]^t$.

For $0 \leq k \leq n-1$ and $k \in K$, let

$$T_k(c) = [0, \cdots, c, \cdots, 0]^t$$

where c is in the k-th position and the rest of the entries are zero. We will denote any matrix of the form $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ by $\mathrm{diag}(A, B)$.

Let π be a non-Desarguesian semifield plane of order $p^n \neq 2^6$ that admits an autotopism g_0 of order h where h is a p-primitive divisor of $p^n - 1$, i.e. $h | p^n - 1$, but $h \nmid p^i - 1$ for $1 \leq i \leq n-1$. We consider $V \oplus V$ as the vector space associated to the affine plane π and $V(\infty) = \{((0), (x)) | x \in K\}$ is a component of a spread of π in $V \oplus V$.

In [15] Cordero and Figueroa proved the following:

Theorem 3.1 (Result 1, [15])**.** *Let π be a non-Desarguesian semifield plane of order p^n. If π admits a collineation g_0 of order h, a p-primitive prime divisor of p^n-1, then*

(i) There exists a spread set $\{V(0), V(\infty)\} \cup \{V(M(y)) | y \in K - \{0\}\}$ for π in $V \oplus V$ such that $V(\infty)$ is the shear axis and for $y \in K, y \neq 0$,

$$M(y) = [a_0 y^{(e_0)}, a_1 y^{(e_1)}, \ldots, a_{n-1} y^{(e_{n-1})}]^t \in \mathrm{Aut}(V).$$

(ii) $g_0 = diag(T_0(\gamma), T_0(\delta))$, where γ and δ are two different elements in K, both of order h.

(iii) $\left(\frac{\delta}{\gamma}\right)^{(e_i)} = \frac{\delta}{\gamma^{(i)}}$, for each i such that $a_i \neq 0$.

Notice that in Theorem 3.1 above the plane π is coordinatized by the pre-semifield $(K, +, \circ)$ where

$$x \circ y = \sum_{i=0}^{n-1} a_i x^{(i)} y^{(e_i)}$$

for $x, y \in K$. Hence either π is a generalized twisted field plane or there exist at least two non-zero indices u and v such that $a_u \neq 0 \neq a_v$. We study the case in which there are precisely two nonzero coefficients, so the multiplication on the pre-semifield behaves as a generalization of the multiplication of a pre-semifield that defines the generalized twisted fields. Hence the product is of the form

$$x \circ y = xy + Ax^{(u)} y^{(e_u)} + Bx^{(v)} y^{(e_v)}. \tag{3.2}$$

In [15] an example of such a product for $GF(3^6)$ was given:

Theorem 3.2. *(Result 2, [15]) Let π be a non-Desarguesian plane which is not a generalized twisted field plane of order 3^6. Suppose π admits an autotopism g_0 of order 7, a 3-primitive prime divisor of 3^6-1. Then π can be coordinatized by the pre-semifield $GF(3^6,+,\circ)$, where*

$$x \circ y = xy + \gamma x^{(1)} y^{(3)} + \gamma^{13} x^{(3)} y^{(1)}$$

and γ is a primitive element in $GF(3^6)$ that satisfies $\gamma^2+\gamma+2=0$. Moreover, π has an autotopism of order 3 that normalizes g_0.

In this work we study in general (pre)semifields with a product as in (3.2) above.

First, we show that $\mathcal{S}$ is indeed a pre-semifield with the product in equation 3.1.

Lemma 3.1. *$\mathcal{S}=(S,+,\circ)$ is a pre-semifield with product $x\circ y = xy + Ax^{\alpha}y^{\beta}+Bx^{\beta}y^{\alpha}$ for $\alpha,\beta \in Aut(GF(p^n))$ and $x,y,A,B \in GF(p^n)$ provided $Ax^{\alpha-1}y^{\beta-1}+Bx^{\beta-1}y^{\alpha-1} \neq -1$.*

Proof. Since addition is the field addition $(S,+)$ forms an abelian group. Now assume $x,y\neq 0$. Then $x\circ y = xy + Ax^{\alpha}y^{\beta}+Bx^{\beta}y^{\alpha}$, that is, $x\circ y = xy(1+Ax^{\alpha-1}y^{\beta-1}+Bx^{\beta-1}y^{\alpha-1})$ where $x^{\alpha-1}=\dfrac{x^{\alpha}}{x}$. Now $xy\neq 0$ because x and y are non-zero elements in the field. Thus if $x\circ y=0$ we must have $1+Ax^{\alpha-1}y^{\beta-1}+Bx^{\beta-1}y^{\alpha-1}=0$. Hence there are no zero divisors provided $Ax^{\alpha-1}y^{\beta-1}+Bx^{\beta-1}y^{\alpha-1}\neq -1$.

It remains to be shown that the distributive laws hold:

$$\begin{aligned} x\circ(y+z) &= x(y+z) + Ax^{\alpha}(y+z)^{\beta} + Bx^{\beta}(y+z)^{\alpha} \\ &= xy + xz + Ax^{\alpha}(y^{\beta}+z^{\beta}) + Bx^{\beta}(y^{\alpha}+z^{\alpha}) \end{aligned}$$

$$= xy + xz + Ax^{\alpha}y^{\beta} + Ax^{\alpha}z^{\beta} + Bx^{\beta}y^{\alpha} + Bx^{\beta}z^{\alpha}$$

$$= xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha} + xz + Ax^{\alpha}z^{\beta} + Bx^{\beta}z^{\alpha}$$

$$= x \circ y + x \circ z$$

and

$$\begin{aligned}(x+y)\circ z &= (x+y)z + A(x+y)^{\alpha}z^{\beta} + B(x+y)^{\beta}z^{\alpha}\\ &= xz + yz + A(x^{\alpha}+y^{\alpha})z^{\beta} + B(x^{\beta}+y^{\beta})z^{\alpha}\\ &= xz + yz + Ax^{\alpha}z^{\beta} + Ay^{\alpha}z^{\beta} + Bx^{\beta}z^{\alpha} + By^{\beta}z^{\alpha}\\ &= xz + Ax^{\alpha}z^{\beta} + Bx^{\beta}z^{\alpha} + xz + Ay^{\alpha}z^{\beta} + By^{\beta}z^{\alpha}\\ &= x \circ z + y \circ z.\end{aligned}$$

Therefore $(S, +, \circ)$ is a pre-semifield.

$\square$

3.2 General Results

Let $\mathcal{S} = S(K, \alpha, \beta, A, B)$ be a semifield with product given by $x \circ y = xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha}$ where $x, y \in K = GF(p^n)$, $\alpha : x \mapsto x^{p^a}$ and $\beta : x \mapsto x^{p^b}$. Assume $\alpha^3 \neq 1$ if $\alpha\beta = 1$. Let $\pi = \pi(K, \alpha, \beta, A, B)$ be the semifield plane coordinatized by $\mathcal{S}$.

From Hughes and Piper [19], all of the elations of π are either shears or translations and thus are in Σ. See Lemma 2.4 above. The full automorphism group, Π, is $\Pi = \Sigma \cdot \Lambda$ where Σ is the group generated by the shears and the translations and Λ is the autotopism group. We also know that $\Sigma \cap \Lambda = 1$, so there are no elations in the autotopism group. In the following discussion we expand on the ideas presented in [6].

First we discuss the autotopism collineations of $\pi(K, \alpha, \beta, A, B)$.

3.2.1 Autotopisms

Theorem 3.3. *Let* $\pi = \pi(K, \alpha, \beta, A, B)$ *be a semifield plane with product* $x \circ y = xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha}$*. Assume that* $\alpha^3 \neq 1$ *when* $\alpha\beta = 1$*. If* (F, G, H) *is an autotopism collineation of* π *with* $F(x) = cx^{\sigma}$ *and* $G(y) = dy^{\theta}$*, then* $\sigma = \theta, dc^{\beta}A^{\theta} = Ac^{\alpha}d^{\beta}, dc^{\alpha}B^{\theta} = Bc^{\beta}d^{\alpha}$*, and* $H(n) = \frac{d}{c}n^{\theta}$*.*

Proof. From $G(x \circ n) = F(x) \circ H(n)$ we get $d(x \circ n)^{\theta} = cx^{\sigma} \circ H(n)$. Expanding this equation we get: $d(xn + Ax^{\alpha}n^{\beta} + Bx^{\beta}n^{\alpha})^{\theta} = cx^{\sigma}H(n) + A(cx^{\sigma})^{\alpha}H(n)^{\beta} + B(cx^{\sigma})^{\beta}H(n)^{\alpha}$. Therefore,

$$dx^{\theta}n^{\theta} + dA^{\theta}x^{\alpha\theta}n^{\beta\theta} + dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = cx^{\sigma}H(n) + Ac^{\alpha}x^{\sigma\alpha}H(n)^{\beta} + Bc^{\beta}x^{\sigma\beta}H(n)^{\alpha}. \quad (3.3)$$

Let $E_1 = dx^{\theta}n^{\theta}, E_2 = dA^{\theta}x^{\alpha\theta}n^{\beta\theta}, E_3 = dB^{\theta}x^{\beta\theta}n^{\alpha\theta}, E_4 = cx^{\sigma}H(n), E_5 = Ac^{\alpha}x^{\sigma\alpha}H(n)^{\beta}$, and $E_6 = Bc^{\beta}x^{\sigma\beta}H(n)^{\alpha}$. We analyze the possibilities for equality in (3.3):

Suppose $E_1 = E_4, E_2 = E_5$ and $E_3 = E_6$. From $dx^{\theta}n^{\theta} = cx^{\sigma}H(n)$ we get $x^{\theta} = x^{\sigma}$, hence $\theta = \sigma$. From $dn^{\theta} = cH(n)$, we get $H(n) = \frac{d}{c}n^{\theta}$.

By substituting into $E_2 = E_5$ we get: $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} = Ac^{\alpha}x^{\sigma\alpha}\left(\frac{d}{c}n^{\theta}\right)^{\beta}$, that is, $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} = Ac^{\alpha}x^{\sigma\alpha}\left(\frac{d^{\beta}}{c^{\beta}}n^{\theta\beta}\right)$. From here we get $dA^{\theta} = Ad^{\beta}\frac{c^{\alpha}}{c^{\beta}}$.

By substituting into $E_3 = E_6$ we get: $dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = Bc^{\beta}x^{\sigma\beta}\left(\frac{d}{c}n^{\theta}\right)^{\alpha}$, that is, $dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = Bc^{\beta}x^{\sigma\beta}\left(\frac{d^{\alpha}}{c^{\alpha}}n^{\theta\alpha}\right)$. This implies $dB^{\theta} = Bd^{\alpha}\left(\frac{c^{\beta}}{c^{\alpha}}\right)$.

Similarly, if $E_1 = E_4, E_2 = E_6$, and $E_3 = E_5$, as in the previous case, we get $\theta = \sigma$ and $H(n) = \frac{d}{c}n^{\theta}$. Replacing H(n) with the above we get: $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} =$

$Bc^{\beta}x^{\sigma\beta}\left(\frac{d}{c}n^{\theta}\right)^{\alpha}$, that is, $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} = Bc^{\beta}x^{\sigma\beta}\left(\frac{d^{\alpha}}{c^{\alpha}}n^{\theta\alpha}\right)$. This implies $x^{\alpha\theta} = x^{\sigma\beta}$, hence $\alpha = \beta$. However, this is not possible because $\alpha \neq \beta$.

Now if $E_1 = E_5, E_2 = E_4$, and $E_3 = E_6$ from $E_2 = E_4$, we have $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} = cx^{\sigma}H(n)$. This implies $x^{\alpha\theta} = x^{\sigma}$ and therefore $\alpha\theta = \sigma$. Thus

$$H(n) = \frac{dA^{\theta}n^{\beta\theta}}{cx} \tag{3.4}$$

In $E_1 = E_5$ substituting for $H(n)$ from (3.4) we get $dx^{\theta}n^{\theta} = Ac^{\alpha}x^{\sigma\alpha}\left(\frac{dA^{\theta}n^{\beta\theta}}{c}\right)^{\beta}$, that is, $dx^{\theta}n^{\theta} = Ac^{\alpha}x^{\sigma\alpha}\left(\frac{d^{\beta}A^{\theta\beta}n^{\beta^2\theta}}{c^{\beta}}\right)$. This implies $x^{\theta} = x^{\sigma\alpha}$, hence

$$\theta = \sigma\alpha. \tag{3.5}$$

Using (3.4) and (3.5), we get from $E_3 = E_6$ that $dB^{\theta}x^{\beta\theta}n^{\alpha\theta}=Bc^{\beta}x^{\sigma\beta}\left(\frac{dA^{\theta}n^{\beta\theta}}{c}\right)^{\alpha}$. That is, $dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = Bc^{\beta}x^{\sigma\beta}\left(\frac{d^{\alpha}A^{\theta\alpha}n^{\beta\theta\alpha}}{c^{\alpha}}\right)$. This implies $x^{\beta\theta} = x^{\beta\sigma,}$ hence $\theta = \sigma$. Also $n^{\alpha\theta} = n^{\beta\theta\alpha}$. This implies $\beta = 1$, which is not possible since β is a nontrivial automorphism.

If $E_1 = E_5, E_3 = E_4$, and $E_2 = E_6$ from $E_3 = E_4$ we get $dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = cx^{\sigma}H(n)$, hence $x^{\beta\theta} = x^{\sigma}$. This implies $\beta\theta = \sigma$ and

$$H(n) = \frac{dB^{\theta}n^{\alpha\theta}}{c} \tag{3.6}$$

From $E_1 = E_5$ and using equation 3.6, we get $dx^\theta n^\theta = Ac^\alpha x^{\sigma\alpha}\left(\frac{dB^\theta n^{\alpha\theta}}{c}\right)^\beta$, that is, $dx^\theta n^\theta = Ac^\alpha x^{\sigma\alpha}\left(\frac{d^\beta B^{\theta\beta} n^{\alpha\theta\beta}}{c^\beta}\right)$. Hence $dx^\theta n^\theta = Ac^\alpha x^{\beta\theta\alpha}\left(\frac{d^\beta B^{\theta\beta} n^{\alpha\theta\beta}}{c^\beta}\right)$. This implies $x^\theta = x^\beta\theta\alpha$; therefore

$$1 = \beta\alpha. \tag{3.7}$$

From $E_2 = E_6$ and using equation (3.6) and (3.7) we get $dA^\theta x^{\alpha\theta} n^{\beta\theta} = Bc^\beta x^{\sigma\beta}\left(\frac{dB^\theta n^{\alpha\theta}}{c}\right)^\alpha$, that is, $dA^\theta x^{\alpha\theta} n^{\beta\theta} = Bc^\beta x^{\sigma\beta}\left(\frac{d^\alpha B^{\theta\alpha} n^{\alpha^2\theta}}{c^\alpha}\right)$. Hence $dA^\theta x^{\alpha\theta} n^{\beta\theta} = Bc^\beta x^{\beta\theta\beta}\left(\frac{d^\alpha B^{\theta\alpha} n^{\alpha^2\theta}}{c^\alpha}\right)$. This implies $x^{\alpha\theta} = x^{\beta^2\theta}$; hence

$$\alpha = \beta^2 \tag{3.8}$$

and from $n^{\beta\theta} = n^{\alpha^2\theta}$ we get

$$\beta = \alpha^2. \tag{3.9}$$

From equations (3.8) and (3.9) we get $\alpha^3 = 1$, which can not happen since $\alpha\beta = 1$.

If $E_1 = E_6, E_2 = E_4$, and $E_3 = E_5$ beginning with $E_2 = E_4$, we have $dA^\theta x^{\alpha\theta} n^{\beta\theta} = cx^\sigma H(n)$. Hence $x^{\alpha\theta} = x^\sigma$; therefore $\alpha\theta = \sigma$. Also,

$$H(n) = \frac{dA^\theta n^{\beta\theta}}{c} \tag{3.10}$$

Using equation (3.10), from $E_1 = E_6$ we get $dx^\theta n^\theta = Bc^\beta x^{\sigma\beta}\left(\frac{d^\alpha A^{\theta\alpha} n^{\beta\theta\alpha}}{c^\alpha}\right)$. This implies $x^\theta = x^{\sigma\beta}$; hence

$$\theta = \sigma\beta \tag{3.11}$$

and $n^\theta = n^{\beta\theta\alpha}$ which implies

$$\beta\alpha = 1. \tag{3.12}$$

Now using (3.10) and (3.11), from $E_3 = E_5$ we get $dB^\theta x^{\beta\theta} n^{\alpha\theta} = Ac^\alpha x^{\sigma\alpha} \left(\frac{dA^\theta n^{\beta\theta}}{c}\right)^\beta$, that is, $dB^\theta x^{\beta\theta} n^{\alpha\theta} = Ac^\alpha x^{\sigma\alpha} \left(\frac{d^\beta A^\theta \beta n^{\beta^2\theta}}{c^\beta}\right)$. This implies $n^{\alpha\theta} = n^{\beta^2\theta}$, hence

$$\alpha = \beta^2. \tag{3.13}$$

From (3.12) and (3.13) we get $\beta^3 = 1$, which can't happen, since $\beta^3 = 1$ implies $1 = \alpha^3$.

If $E_1 = E_6, E_2 = E_5$, and $E_3 = E_4$, using $E_2 = E_5$, we get $dA^\theta x^{\alpha\theta} n^{\beta\theta} = Ac^\alpha x^{\sigma\alpha} H(n)^\beta$ which implies $x^{\alpha\theta} = x^{\sigma\alpha}$; hence $\theta = \sigma$.

Using this fact in $E_3 = E_4$, we get $x^{\beta\theta} = x^\sigma$; this is equivalent to $x^{\beta\theta} = x^\theta$. This implies $\beta = 1$ which cannot happen since β cannot be a trivial automorphism.

The cases considered above are the only possibilities to get equality in (3.3).

□

We now look at the homologies of π. In the following results we let $\mathcal{O} = (0,0)$, $I = (1,1)$, $U = (0)$, and $V = (\infty)$.

Theorem 3.4. *Let $\mathcal{S} = S(K, \alpha, \beta, A, B)$ be a semifield with product given by $x \circ y = xy + Ax^\alpha y^\beta + Bx^\beta y^\alpha$ where $x, y \in K = GF(p^n)$, $\alpha : x \mapsto x^{p^a}$ and $\beta : x \mapsto x^{p^b}$. Assume $\alpha^3 \neq 1$ if $\alpha\beta = 1$. Let $\pi = \pi(K, \alpha, \beta, A, B)$ be the semifield plane coordinatized by $\mathcal{S}$. Let (F, G, H) be an autotopism collineation of π. Then (F,G,H) is a homology with center U and axis $\mathcal{O}V$ if and only if $F(x) = cx; G(y) = y;$ and $H(n) = c^{-1}n$, where $c \in K, c \neq 0,$ and $c^\alpha = c^\beta$.*

Proof. Let (F, G, H) be a homology with center U and axis $\mathcal{O}V$. Then $G(y) = y$ since $(x, y) \mapsto (F(x), G(y))$ and $G(y)$ acts on the points of $\mathcal{O}V$, the line from $(0,0)$ to (∞), which is fixed pointwise.

Now, $G(x \circ n) = F(x) \circ H(n)$ by definition, so let $m = H(n)$. Thus we have $G(x \circ n) = F(x) \circ m$. From here we get $G(xn + Ax^{\alpha}n^{\beta} + Bx^{\beta}n^{\alpha}) = F(x)y + AF(x)^{\alpha}m^{\beta} + BF(x)^{\beta}m^{\alpha}$. This yields $xn + Ax^{\alpha}n^{\beta} + Bx^{\beta}n^{\alpha} = F(x)y + AF(x)^{\alpha}m^{\beta} + BF(x)^{\beta}m^{\alpha}$, since $G(y) = y$.

Since $F(x)$ is additive, it can be written as

$$F(x) = \sum_{i=1}^{r-1} f_i x^{p^i}.$$

So, $AF(x)^{\alpha}m^{\beta} = Am^{\beta}\sum_{i=0}^{r-1} f_i^{\alpha}x^{p^i}x^{p^a} = Am^{\beta}\sum_{i=0}^{r-1} f_i^{\alpha}x^{p^{i+a}} = Am^{\beta}\sum_{t=0}^{r-1} f_{t-a}^{\alpha}x^{p^t}$, where $t = a + i$.

Thus $AF(x)^{\alpha}m^{\beta} = \sum_{t=0}^{r-1} Am^{\beta}f_{t-a}^{\alpha}x^{p^t}$.

Similarly, $BF(x)^{\beta}m^{\alpha} = Bm^{\alpha}\sum_{i=0}^{r-1} f_i^{\beta}x^{p^i}x^{p^b} = Bm^{\alpha}\sum_{i=0}^{r-1} f_i^{\beta}x^{p^{i+b}} = Bm^{\alpha}\sum_{t=0}^{r-1} f_{t-b}^{\beta}x^{p^t}$, where $t = i + b$. Thus $BF(x)^{\beta}m^{\alpha} = \sum_{t=0}^{r-1} Bm^{\alpha}f_{t-b}^{\beta}x^{p^t}$.

We then have

$$\begin{aligned} xn + Ax^{\alpha}n^{\beta} + Bx^{\beta}n^{\alpha} &= \sum_{t=0}^{r-1} mf_t x^{p^t} + \sum_{t=0}^{r-1} Am^{\beta}f_{t-a}^{\alpha}x^{p^t} + \sum_{t=0}^{r-1} Bm^{\alpha}f_{t-b}^{\beta}x^{p^t} \\ &= \sum_{t=0}^{r-1}(mf_t + Am^{\beta}f_{t-a}^{\alpha} + Bm^{\alpha}f_{t-b}^{\beta})x^{p^t} \end{aligned}$$

For $t = 0$ on the left hand side of the above equation, there is no x^{p^t} term, so the coefficient of this term will be 0. Thus $mf_t + Am^{\beta}f_{t-a}^{\alpha} + Bm^{\alpha}f_{t-b}^{\beta} = 0$. Hence $f_t = 0, f_{t-a} = 0,$ and $f_{t-b} = 0$ since $xn + Ax^{\alpha}n^{\beta} + Bx^{\beta}n^{\alpha} = \sum_{t=0}^{r-1}(mf_t + Am^{\beta}f_{t-a}^{\alpha} + Bm^{\alpha}f_{t-b}^{\beta})x^{p^t}$ holds for all n and $m = H(n)$ is bijective. If $a + b \neq r$ then $t = a + b \neq 0$ mod r, so $f_{t-a} = f_b = 0$ and $f_{t-b} = f_a = 0$. For $a + b = r$, if $2a = r$ then $2b = r$

because $a = b$, but $a < b$, so $2a \neq 0 \mod r$ and $2b \neq 0 \mod r$. If $2a = b \mod r$ or $2b = a \mod r$ then $3a = r$ but $\alpha^3 \neq 1$ when $\alpha\beta = 1$. So from $t = 2a \mod r$ we get $0 = f_{t-a} = f_{2a-a} = f_a$ and $0 = f_{t-b} = f_{2b-b} = f_b$ if $t = 2b \mod r$.

Therefore $F(x) = f_0 x^{p^0} + \underbrace{f_1 x^{p^1} + f_2 x^{p^2} + \cdots + f_{r-1} x^{p^{r-1}}}_{\text{all zero since } f_t = 0 \text{ for all } t \neq 0}$, which implies $F(x) = f_0 x$.

Now $xn + Ax^\alpha n^\beta + Bx^\beta n^\alpha = f_0 x \circ m = f_0 xm + A(f_0 x)^\alpha m^\beta + B(f_0 x)^\beta m^\alpha$.

From $n = f_0 m = f_0 H(n)$ we get $f_0^{-1} n = H(n)$. From $n^\beta = f_0^\alpha m^\beta$ and $n^\alpha = f_0^\beta m^\alpha$ we get $f_0^\alpha = f_0^\beta$. Letting $c = f_0$, we get $F(x) = cx, G(y) = y$, $c^{-1}n = H(n)$, and $c^\alpha = c^\beta$.

Conversely, suppose (F, G, H) is an autotopism collineation of π with $F(x) = cx$, $G(y) = y$, and $H(n) = c^{-1}n$. Then, since $G(y) = y$, $\mathcal{O}V$ is fixed pointwise. Also $U = (0)$ is the only point fixed linewise. Moreover $G(x \circ n) = F(x) \circ H(n)$. Thus (F, G, H) is a homology with center U and axis $\mathcal{O}V$.

$\square$

In the next theorem we discuss the homologies with center $\mathcal{O}$ and axis UV.

Theorem 3.5. *Let $\pi = \pi(K, \alpha, \beta, A, B)$ be a semifield plane with the product $x \circ y = xy + Ax^\alpha y^\beta + Bx^\beta y^\alpha$ where $\alpha : x \mapsto x^{p^a}$ and $\beta : x \mapsto x^{p^b}$. Assume $\alpha^3 \neq 1$ if $\alpha\beta = 1$. Let (F, G, H) be an autotopism collineation. Then (F, G, H) is a homology with center $\mathcal{O}$ and axis UV if and only if $F(x) = cx, G(y) = cy$, and $H(n) = n$, where $c \in K, c \neq 0$ and $c^\alpha = c = c^\beta$, except when $\alpha^4 = 1$ and $\alpha\beta = 1$. If $\alpha^4 = 1$ and $\alpha\beta = 1$, then (F, G, H) is a homology if and only if $G(y) = g_0 y + g_a y^\alpha + g_b y^\beta, F(x) = g_0 x + \frac{C g_a}{A^\beta} x^{\alpha^2}$, and $H(n) = n$, where $C = A^\alpha A^\beta - B^\alpha B^\beta$, and $g_0, g_a, g_b \in K$ are such that $g_0^\alpha = g_0 = g_0^\beta, g_b = \frac{B^\alpha}{A^\beta} g_a, g_a B^\alpha = -C^\alpha A^\beta g_a^\alpha$, and if $g_a \neq 0$ then $CC^\alpha = -1$.*

Proof. The point (x, y) maps into the point $(F(x), G(y))$, and for $n \in UV$, $H(n) = n$ since the "slopes" are fixed. We also have $G(x \circ n) = F(x) \circ n$, for all $x, n \in K$.

Since G is additive, then

$$G(y) = \sum_{i=0}^{r-1} g_i x^{p^i}.$$

Thus, $G(x \circ n) = F(x) \circ n$, so we have

$$\sum_{i=0}^{r-1} g_i(xn + Ax^\alpha n^\beta + Bx^\beta n^\alpha)^{p^i} = F(x)n + AF(x)^\alpha n^\beta + BF(x)^\beta n^\alpha.$$

$$\sum_{i=0}^{r-1}(g_i x^{p^i} n^{p^i} + g_i A^{p^i} x^{\alpha p^i} n^{\beta p^i} + g_i B^{p^i} x^{\beta p^i} n^{\alpha p^i}) = F(x)n + AF(x)^\alpha n^\beta + BF(x)^\beta n^\alpha. \tag{3.14}$$

For $t = b + i$ and $t = a + i$, we get, repsectively,

$$\sum_{t=0}^{r-1}(g_t x^{p^t} n^{p^t} + g_{t-b} A^{p^{t-b}} x^{p^{a+t-b}} n^{p^t} + g_{t-a} B^{p^{t-a}} x^{p^{b+t-a}} n^{p^t}) = F(x)n + AF(x)^\alpha n^\beta + BF(x)^\beta n^\alpha.$$

$$\sum_{t=0}^{r-1}(g_t x^{p^t} + g_{t-b} A^{p^{t-b}} x^{p^{a+t-b}} + g_{t-a} B^{p^{t-a}} x^{p^{b+t-a}}) n^{p^t} = F(x)n + AF(x)^\alpha n^\beta + BF(x)^\beta n^\alpha.$$

Equation (3.14) holds for all n, so for $t \notin \{0, a, b\}$, we have

$$g_t x^{p^t} + g_{t-b} A^{p^{t-b}} x^{p^{a+t-b}} + g_{t-a} B^{p^{t-a}} x^{p^{b+t-a}} = 0. \tag{3.15}$$

If $2a \neq 2b \mod r$, that is $a - b \neq b - a$ then the individual terms have different degrees and thus $g_t = 0, g_{t-b} = 0$, and $g_{t-a} = 0$ for $t > 0$ and $G(y) = g_0 y$.

Now assume $2a = 2b \mod r$. That is $\alpha^2 = \beta^2$. Then $g_t = 0$ for $t \neq 0, a,$ or b. Since $b - a \neq 0, a,$ or $b \mod r$, then $g_{b-a} = 0$ and $g_{a-b} = 0$.

Comparing the coefficients of n, n^{β}, and n^{α} and using the fact that $2a = 2b$ we get $a - b = b - a \mod r$,. Therefore

$$\begin{aligned} F(x) &= g_0 x + g_{0-b} A^{p^{0-b}} x^{p^{a+0-b}} + g_{0-a} B^{p^{0-a}} x^{p^{b+0-a}} \\ &= g_0 x + g_{-b} A^{p^{-b}} x^{p^{a-b}} + g_{-a} B^{p^{-a}} x^{p^{b-a}} \\ &= g_0 x + (g_{-b} A^{p^{-b}} + g_{-a} B^{p^{-a}}) x^{p^{a-b}}, \end{aligned} \tag{3.16}$$

$$\begin{aligned} AF(x)^{\alpha} &= g_b x p^b + g_{b-b} A^{p^{b-b}} x^{p^{a+b-b}} + g_{b-a} B^{p^{b-a}} x^{p^{b+b-a}} \\ &= g_b x^{p^b} + g_0 A^{p^0} x^{p^a} + g_{b-a} B^{p^{b-a}} x^{p^{b+b-a}} \\ &= g_b x^{p^b} + g_0 A x^{p^a} + g_{b-a} B^{p^{b-a}} x^{p^{-a}} \\ &= g_b x^{p^b} + g_0 A x^{p^a}, \text{ since } g_{b-a} = 0, \end{aligned} \tag{3.17}$$

and

$$\begin{aligned} BF(x)^{\beta} &= g_a x p^a + g_{a-b} A^{p^{a-b}} x^{p^{a+a-b}} + g_{a-a} B^{p^{a-a}} x^{p^{b+a-a}} \\ &= g_a x p^a + g_{a-b} A^{p^{a-b}} x^{p^{2a-b}} + g_0 B^{p^0} x^{p^b} \\ &= g_a x p^a + g_0 B x^{p^b}, \text{ since } g_{a-b} = 0. \end{aligned} \tag{3.18}$$

If $-b \neq a \mod r$, then $-b \neq 0, a,$ or $b \mod r$ and $g_{-b} = 0$. This implies that $b \neq -a \mod r$ so $g_{-a} = 0$ and hence $F(x) = g_0 x$.

Thus $AF(x)^{\alpha} = A(g_0 x)^{\alpha} = A g_0^{\alpha} x^{\alpha} = g_b x^{p^b} + g_0 A x^{p^a}$; hence, $g_0^{\alpha} = g_0$ and $g_b = 0$. Also, $BF(x)^{\beta} = B(g_0 x)^{\beta} = B g_0^{\beta} x^{\beta} = g_a x^{p^a} + g_0 B x^{p^b}$. Therefore, $g_0^{\beta} = g_0$ and $g_a = 0$.

If $2a = 2b$, and $-b = a \mod r$ we get $\alpha\beta = p^a p^b = p^{a+b} = p^{a-a} = p^0 = 1$ and $\alpha^4 = p^a p^a p^a p^a = p^a p^a p^{-b} p^{-b} = p^{2a-2b} = p^{2a-2a} = p^0 = 1$. In this case, equation (3.16) becomes $F(x) = g_0 x + (g_a A^\alpha + g_b B^\beta)x^{\alpha^2}$. Then from equation (3.17) above we get,

$$\begin{aligned}
AF(x)^\alpha = A[g_0 x + (g_a A^\alpha + g_b B^\beta)x^{\alpha^2}]^\alpha &= g_b x^\beta + g_0 A x^\alpha \\
&= A[g_0^\alpha x^\alpha + (g_a^\alpha A^{\alpha^2} + g_b^\alpha B^{\beta\alpha})x^{\alpha^3}] \\
&= A[g_0^\alpha x^\alpha + g_a^\alpha A^{\alpha^2} x^{\alpha^3} + g_b^\alpha B^{\beta\alpha} x^{\alpha^3}] \\
&= A[g_0^\alpha x^\alpha + g_a^\alpha A^{\alpha^2} x^{\alpha^3} + g_b^\alpha B^{\beta\alpha} x^{\alpha^3}] \\
&= A[g_0^\alpha x^\alpha + g_a^\alpha A^{\alpha^2} x^{\beta} + g_b^\alpha B^{\beta\alpha} x^{\beta}]
\end{aligned}$$

This implies

$$g_0^\alpha = g_a \text{ and } A[(g_a A^\alpha + g_b B^\beta)^\alpha] = g_b \tag{3.19}$$

From equation (3.18) above we get,

$$\begin{aligned}
BF(x)^\beta = B[g_0 x + (g_a A^\alpha + g_b B^\beta)x^{\alpha^2}]^\beta &= g_a x^\alpha + g_0 B x^\beta \\
&= B[g_0^\beta x^\beta + (g_a^\beta A^{\alpha\beta} + g_b^\beta B^{\beta^2})x^{\alpha^2\beta}] \\
&= B[g_0^\beta x^\beta + g_a^\beta A^{\alpha\beta} x^\alpha + g_b^\beta B^{\beta^2} x^\alpha] \\
&= B[g_0^\beta x^\beta + g_a^\beta A^{\alpha\beta} x^\alpha + g_b^\beta B^{\beta^2} x^\alpha]
\end{aligned}$$

This implies

$$g_a = B(g_a^\beta A\alpha + g_b B^\beta)^\beta \text{ and } g_0^\beta = g_0. \tag{3.20}$$

Since $2a \neq 0, a,$ or $b \mod r$, taking $t = 2a$, from equation (3.15) we have

$$g_{2a}x^{p^{2a}} + g_{2a-b}A^{p^{2a-b}}x^{p^{a+2a-b}} + g_{2a-a}B^{p^{2a-a}}x^{p^{b+2a-a}} = 0.$$

$$g_{a-b}x^{p^{a-b}} + g_{3a}A^{p^{3a}}x^{p^{4}a} + g_{a}B^{p^{a}}x^{p^{b+a}} = 0.$$

$$g_{a-b}x^{p^{a-b}} + g_{3a}A^{p^{3a}}x^{p^{4}a} + g_{a}B^{p^{a}}x^{p^{b-b}} = 0.$$

$$g_{a-b}x^{p^{a-b}} + g_{3a}A^{p^{3a}}x^{p^{0}} + g_{a}B^{p^{a}}x^{p^{0}} = 0.$$

$$g_{a-b}x^{p^{a-b}} + g_{b}A^{p^{b}}x + g_{a}B^{p^{a}}x = 0.$$

$$g_{a-b}x^{p^{a-b}} + g_{b}A^{\beta}x + g_{a}B^{\alpha}x = 0.$$

So $g_bA^\beta + g_aB^\alpha = 0$ and hence $g_b = -\dfrac{g_aB^\alpha}{A^\beta}$. Also, $g_aB^\alpha + g_bB^\alpha = 0$, which implies $g_b = -g_a\dfrac{B^\alpha}{A^\beta}$.

From (3.19) we get

$$\begin{aligned}
A\left(g_aA^\alpha + g_bB^\beta\right)^\alpha &= g_b \\
A\left(g_aA^\alpha - g_a\frac{B^\alpha}{A^\beta}B^\beta\right)^\alpha &= -g_a\frac{B^\alpha}{A^\beta} \\
-\frac{AA^\beta}{B^\alpha}\left(A^{\alpha^2} - \frac{B^{\alpha^2}B^{\beta\alpha}}{A^{\beta\alpha}}\right)g_a^\alpha &= g_a \\
-\frac{A^\beta}{B^\alpha}\left(\frac{AA^{\alpha^2}A^{\beta\alpha} - AB^{\alpha^2}B^{\beta\alpha}}{A^{\beta\alpha}}\right)g_a^\alpha &= g_a \\
-\frac{A^\beta}{B^\alpha}\left(\frac{AA^{\alpha^2}A - AB^{\alpha^2}B}{A}\right)g_a^\alpha &= g_a \text{ since } \beta\alpha = 1 \\
-\frac{A^\beta}{B^\alpha}\left(A^{\alpha^2}A - B^{\alpha^2}B\right)g_a^\alpha &= g_a \\
-\frac{A^\beta}{B^\alpha}\left(A^{\alpha^2(-\beta)}A^{-\beta} - B^{\alpha^2(-\beta)}B^{-\beta}\right)^\beta g_a^\alpha &= g_a \\
-\frac{A^\beta}{B^\alpha}\left(A^{\alpha^3}A^{\alpha} - B^{\alpha^3}B^{\alpha}\right)^\beta g_a^\alpha &= g_a \\
-\frac{A^\beta}{B^\alpha}\left(A^{\beta}A^{\alpha} - B^{\beta}B^{\alpha}\right)^\beta g_a^\alpha &= g_a \qquad (3.21)
\end{aligned}$$

and from (3.20) we get

$$\begin{aligned}
B\left(g_aA^\alpha + g_bB^\beta\right)^\beta &= g_a\\
B\left(g_aA^\alpha - \frac{g_aB^\alpha}{A^\beta}B^\beta\right)^\beta &= g_a\\
B\left(\frac{A^\alpha A^\beta - B^\alpha B^\beta}{A^\beta}\right)^\beta g_a^\beta &= g_a\\
\frac{B}{A^{\beta^2}}\left(A^\alpha A^\beta - B^\alpha B^\beta\right)^\beta g_a^\beta &= g_a\\
\frac{B}{A^{\alpha^2}}\left(A^\alpha A^\beta - B^\alpha B^\beta\right)^\beta g_a^\beta &= g_a,\ \text{since } \alpha^2 = \beta^2. \qquad (3.22)
\end{aligned}$$

Let $C = A^\alpha A^\beta - B^\alpha B^\beta$ in equations (3.21) and (3.22). Then we have

$$V = -\frac{A^\beta C^\beta}{B^\alpha} \text{ and } W = \frac{BC^\beta}{A^{\alpha^2}}.$$

Equation (3.21) yields $g_a = vg_a^\alpha$ and equation (3.22) gives $g_a = wg_a^\beta$. Thus $g_a^\beta = v^\beta g_a^{\alpha\beta} = v^\beta g_a$. This implies $g_a = wv^\beta g_a$; hence $1 = wv^\beta$.

Now, $1 = wv^\beta = \left(\frac{BC^\beta}{A^{\alpha^2}}\right)\left(-\frac{A^\beta C^\beta}{B^\alpha}\right)^\beta = \left(\frac{BC^\beta}{A^{\alpha^2}}\right)\left(-\frac{A^{\beta^2}C^{\beta^2}}{B^{\alpha\beta}}\right) = -C^\beta C^{\beta^2}$ if $g_a \neq 0$.

Since $-C^\beta C^{\beta^2} = 1$, we get $-C^\beta C^{\beta^2} = 1$. By direct computation we get $1 = -CC^\alpha$

Conversely, since $H(n) = n$, then UV is fixed pointwise. Since UV is fixed pointwise, then $\mathcal{O}U$ and $\mathcal{O}V$ are fixed linewise. Also $\mathcal{O}$ is the center.

□

In the next theorem we discuss the homologies with center V and axis $\mathcal{O}U$.

Theorem 3.6. *Let $\pi = \pi(K, \alpha, \beta, A, B)$ be a semifield plane with the product $x \circ y = xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha}$ where $\alpha : x \mapsto x^{p^a}$ and $\beta : x \mapsto x^{p^b}$. Assume $\alpha^3 \neq 1$ if $\alpha\beta = 1$. Let (F, G, H) be an autotopism collineation. Then (F, G, H) is a homology with center V and axis $\mathcal{O}U$ if and only if $F(x) = x$, $G(y) = cy$ and $H(n) = cn$, $c \in K, c \neq 0, c^{\alpha} = c = c^{\beta}$ except when $\alpha^4 = 1$ and $\alpha\beta = 1$. If $\alpha^4 = 1$ and $\alpha\beta = 1, (F, G, H)$ is a homology if and only if $F(x) = x, G(y) = g_0 y + g_a x^{\alpha} + g_b x^{\beta}, H(n) = g_0 n - \dfrac{C g_a}{b^{\beta}} n^{\alpha^2}$ where $C = A^{\alpha}A^{\beta} - B^{\alpha}B^{\beta}$ and $g_0, g_a, g_b \in K$ such that $g_0^{\beta} = g_0 = g_0^{\alpha}, g_b = -\dfrac{a^{\alpha}}{B^{\beta}} = -A^{\alpha}C g_a$, and if $g_a \neq 0$, then $CC^{\alpha} = -1$.*

Proof. Let (F, G, H) be an autotopism collineation that maps (x, y) into $(F(x), G(y))$ and fixes each line through V. Then $F(x) = x$. So $G(x \circ n) = x \circ H(n)$. Assume first that $G(y) = g_0 y$ for some $g_0 \in K, g_0 \neq 0$. Then $g_0(xn + Ax^{\alpha}n^{\beta} + Bx^{\beta}n^{\alpha}) = xH(n) + Ax^{\alpha}H(n)^{\beta} + Bx^{\beta}H(n)^{\alpha}$. This implies $g_0 n = H(n)$. Since G is additive we have $G(y) = \sum_{i=0}^{r-1} g_i x^{p^i}$, for some $g_i \in K$. From $G(x \circ n) = x \circ H(n)$ we have

$$\sum_{i=0}^{r-1} g_i(xn + Ax^{\alpha}n^{\beta} + Bx^{\beta}n^{\alpha})^{p^i} = xH(n) + Ax^{\alpha}H(n)^{\beta} + Bx^{\beta}H(n)^{\alpha}. \tag{3.23}$$

That is,

$$\sum_{i=0}^{r-1}(g_i x^{p^i} n^{p^i} + g_i A^{p^i} x^{p^{a+i}} n^{p^{b+i}} + g_i B^{p^i} x^{p^{b+i}} n^{p^{a+i}}) = xH(n) + Ax^{\alpha}H(n)^{\beta} + Bx^{\beta}H(n)^{\alpha}.$$

For $t = i, t = a + i,$ and $t = b + i$,

$$\sum_{t=0}^{r-1}(g_t x^{p^t} n^{p^t} + g_{t-a} A^{p^{t-a}} x^{p^t} n^{p^{b+t-a}} + g_{t-b} B^{p^{t-b}} x^{p^t} n^{p^{a+t-b}}) = xH(n) + Ax^{\alpha}H(n)^{\beta} + Bx^{\beta}H(n)^{\alpha}$$

$$\sum_{t=0}^{r-1}(g_t n^{p^t} + g_{t-a} A^{p^{t-a}} n^{p^{b+t-a}} + g_{t-b} B^{p^{t-b}} n^{p^{a+t-b}}) x^{p^t} = xH(n) + Ax^{\alpha}H(n)^{\beta} + Bx^{\beta}H(n)^{\alpha} \tag{3.24}$$

Equation (3.23) holds for all x, so for $t \neq a, b,$ or 0

$$g_t n^{p^t} + g_{t-a} A^{p^{t-a}} n^{p^{b+t-a}} + g_{t-b} B^{p^{t-b}} n^{p^{a+t-b}} = 0 \tag{3.25}$$

If $2a \neq 2b \mod r$ then the terms in equation (3.25) have different degrees. Therefore $g_t = 0, g_{t-b} = 0,$ and $g_{t-a} = 0$ for $t \neq 0, a, b$. Therefore, $g_t = 0$ for $t > 0$ and $G(y) = g_0 y$.

From $G(x \circ n) = F(x) \circ H(n)$, we get $g_0 xn + g_0 A x^\alpha n^\beta + g_0 B x^\beta n^\alpha = xH(n) + Ax^\alpha H(n)^\beta + Bx^\beta H(n)^\alpha$.

This implies $H(n) = g_0 n, g_0 n^\beta = H(n)^\beta$ and $g_0 n^\alpha = H(n)^\alpha$.

Assume now $2a = 2b \mod r$ and $g_t = 0$ for $t \neq 0, a,$ or b. Since $b - a \neq 0, a,$ or $b \mod r$, then $g_{b-a} = 0$ and $g_{a-b} = 0$. So from (3.23) and (3.24) we get

$$H(n) = g_0 n + g_{-a} A^{p^{-a}} n^{p^{b-a}} + g_{-b} B^{p^{-b}} n^{p^{a-b}} \tag{3.26}$$

Therefore,

$$AH(n)^\beta = g_a n^{p^a} + g_0 A n^{p^b} + g_{a-b} B^{p^{a-b}} n^{p^b} = g_a n^{p^a} + g_0 A n^{p^b} \text{ since } g_{a-b} = 0. \tag{3.27}$$

and

$$BH(n)^\alpha = g_b n^{p^b} + g_{b-a} A^{p^{b-a}} n^{p^a} + g_0 B n^{p^a} = g_b n^{p^b} + g_0 B n^{p^a} \text{ since } g_{b-a} = 0. \tag{3.28}$$

Now assume $2a = 2b$ and $-b = a \mod r$ (*i.e.* $\alpha\beta = 1$ and $\alpha^4 = 1$).

From equation (3.26) we get

$$H(n) = g_0 n + g_{-a} A^{p^{-a}} n^{p^{b-a}} + g_{-b} B^{p^{-b}} n^{p^{a-b}}$$
$$= g_0 n + g_b A^{p^b} n^{p^{2b}} + g_a B^{p^a} n^{p^{2a}}. \tag{3.29}$$

From equation (3.27)

$$\begin{aligned} AH(n)^\beta &= g_a n^\alpha + g_0 A n^\beta \\ &= A(g_0 n + g_b A^{p^b} n^{p^{2b}} + g_a B^{p^a} n^{p^{2a}})^\beta \text{ from (3.29)} \qquad (3.30) \\ &= A g_0^\beta n^\beta + A(g_b A^\beta n^{\beta^2} + g_a B^\alpha n^{\alpha^2})^\beta \\ &= A g_0^\beta n^\beta + A(g_b A^\beta)^\beta n^\alpha + A(g_a B^\alpha)^\beta n^\alpha \end{aligned}$$

This implies

$$g_a = A(g_b A^\beta + g_a B^\alpha)^\beta \text{ and } g_0 = g_0^\beta. \tag{3.31}$$

From (3.28)

$$\begin{aligned} BH(n)^\alpha &= g_b n^\beta + g_0 B n^\alpha \\ &= B(g_0 n + g_b A^{p^b} n^{p^{2b}} + g_a B^{p^a} n^{p^{2a}})^\alpha \text{ from (3.29)} \end{aligned}$$

$$\begin{aligned} &= B g_0^\alpha n^\alpha + B(g_b A^\beta n^{\beta^2} + g_a B^\alpha n^{\alpha^2})^\alpha \\ &= B g_0^\alpha n^\alpha + B(g_b A^\beta + g_a B^\alpha)^\alpha n^\beta \end{aligned}$$

This implies

$$g_b = B(g_b A^\beta + g_a B^\alpha)^\alpha \text{ and } g_0 = g_0^\alpha. \tag{3.32}$$

Since $2a \neq 0, a,$ or $b \mod r$ by taking $t = 2a$ in (3.25) we get

$$g_{2a}n^{p^{2a}} + g_a A^{p^a} n^{p^{b+a}} + g_{2a-b}B^{p^{2a-b}} n^{p^{3a-b}} = 0.$$

Hence $g_{2a}n^{p^{2a}} + g_a A^{p^a} n^{p^{-a+a}} + g_{2a+a}B^{p^{2a+a}} n^{p^{3a+a}} = 0,$ since -b=a.

Therefore $g_{2a}n^{p^{2a}} + g_a A^{p^a} n + g_b B^{p^b} n = 0,$ since $3a = b$ and $4a = 0$.

Thus $g_{2a}n^{\alpha^2} + g_a A^{\alpha} n + g_b B^{\beta} n = 0.$

The coefficient of n^{α^2} has to be 0; hence,

$$g_a A^{\alpha} + g_b B^{\beta} = 0.$$

Solving for g_b we get

$$g_b = -\frac{g_a A^{\alpha}}{B^{\beta}}.$$

Now substituting this on equation (3.31) we get

$$\begin{aligned} g_a &= A(g_b A^{\beta} + g_a B^{\alpha})^{\beta} \\ &= A(-\frac{g_a A^{\alpha}}{B^{\beta}} A^{\beta} + g + aB^{\alpha})^{\beta}; g_0 = g_0^{\beta} \end{aligned}$$

$$\begin{aligned} &= A\left(\frac{B^{\alpha}B^{\beta} - A^{\alpha}A\beta}{B^{\beta}}\right)^{\beta} g_a^{\beta} \\ &= -A\left(\frac{C}{B^{\beta}}\right) g_a^{\beta};\ \text{where } C = A^{\alpha}A^{\beta} - B^{\alpha}B^{\beta}. \\ &= v g_a^{\beta};\ \text{where } v = -A\left(\frac{C}{B^{\beta}}\right)^{\beta} \end{aligned}$$

and equation (3.32) becomes:

$$
\begin{aligned}
-\frac{g_a A^\alpha}{B^\beta} &= B\left(-\frac{g_a A^\alpha}{B^\beta}A^\beta + g_a B^\alpha\right)^\alpha ; g_0 = g_0^\alpha \\
&= -Bg_a^\alpha\left(\frac{A^\alpha A^\beta - B^\alpha B^\beta}{B^\beta}\right)^\alpha \\
&= -Bg_a^\alpha\left(\frac{C}{B^\beta}\right)^\alpha, \text{ where } C = A^\alpha A^\beta - B^\alpha B^\beta.
\end{aligned}
$$

Rearranging this equation we get:

$$
\begin{aligned}
g_a &= \frac{B^\beta}{A^\alpha}Bg_a^\alpha\left(\frac{C}{B^\beta}\right)^\alpha \\
&= \frac{B^\beta}{A^\alpha}Bg_a^\alpha\left(\frac{C^\alpha}{B^\beta\alpha}\right) \\
&= \frac{B^\beta}{A^\alpha}Bg_a^\alpha\left(\frac{C^\alpha}{B}\right); \text{ since } \alpha\beta = 1 \\
&= \frac{B^\beta}{A^\alpha}g_a^\alpha C^\alpha \\
&= wg_a^\alpha; \text{ where } w = B^\beta\left(\frac{C}{A}\right)^\alpha.
\end{aligned}
$$

From here we get $g_a^\beta = w^\beta g_a^{\alpha\beta} = w^\beta g_a$ and $g_a = vw^\beta g_a$.

Now,

$$
\begin{aligned}
1 &= vw^\beta \\
&= -A\left(\frac{C}{B^\beta}\right)^\beta\left(B^\beta\left(\frac{C}{A}\right)^\alpha\right)^\beta \\
&= -A\left(\frac{C}{B^\beta}\right)^\beta B^{\beta^2}\left(\frac{C^{\alpha\beta}}{A^{\alpha\beta}}\right) \\
&= -A\left(\frac{C^\beta}{B^{\beta^2}}\right)B^{\beta^2}\left(\frac{C}{A}\right); \text{ since } \alpha\beta = 1 \\
&= -C^\beta C, \text{ if } g_a \neq 0.
\end{aligned}
$$

This implies

$$CC^{\alpha} = -1.$$

Conversely, since $F(x) = x$, the line $\mathcal{O}U$ is fixed pointwise. Thus UV and $\mathcal{O}V$ are fixed lines and the only point they have in common is $V = (\infty)$. Thus we have a homology with center V and axis $\mathcal{O}U$. □

3.2.2 The Nuclei of $\mathcal{S}$

Recall that the nuclei of a semifield measure degrees of associativity. In the next theorem we give the order of the nuclei of the semifields under consideration.

Theorem 3.7. *Let $\pi = \pi(K, \alpha, \beta, A, B)$ be a semifield plane. Assume that $\alpha^3 \neq 1$ if $\alpha\beta = 1$. Let $\mathcal{S}$ be a semifield that coordinatizes π. Then the order of the middle nucleus of $\mathcal{S}$ is $p^{(r,b-a)}$. The left and right nuclei have the same order $p^{(r,a,b)}$ where $(n, m) = \gcd(n, m)$, except when $a^4 = 1, \alpha\beta = 1$, and $g_a \neq 0$ in the above theorems.*

Proof. By Theorem 8.2 in [19] $\mathcal{N}_m^{\times}$ is isomorphic to $\Pi_{(U,\mathcal{O}V)}$, the group of homologies with axis $\mathcal{O}V$ and center U. By Theorem(3.4), the coefficients of the mappings F, G, H are the $c \in K$ where $c \neq 0, c^{\alpha} = c^{\beta}$. Thus $c^{p^a} = c^{p^b}$. From this we get $1 = c^{p^a(p^{b-a}-1)}$. So the order of $\Pi_{(U,\mathcal{O}V)}$ must divide $p^{b-a} - 1$. Now, since K^* is cyclic and is of order $p^r - 1$, then the order of $\Pi_{(U,\mathcal{O}V)}$ must also divide $p^r - 1$, since $\Pi_{(U,\mathcal{O}V)}$ is isomorphic to the multiplicative group of the middle nucleus and this is a subgroup of the whole multiplicative group. Thus the order of $\Pi_{(U,\mathcal{O}V)}$ is $p^s - 1$, where $s = \gcd(r, b - a)$.

The arguments for the left and right nuclei are similar. For each of these, the order of the corresponding isomorphic homology group is equal to the number of c's in K, where $c \neq 0$, such that $c^{\alpha} = c^{\beta} = c$. From this relationship we get, $c^{p^a} = c^{p^b} = c$, therefore $c^{p^a-1} = 1$ and similarly $c^{p^b-1} = 1$. Thus the order of the corresponding homology groups divide both $p^a - 1$ and $p^b - 1$. Now since the group of homologies with center $\mathcal{O}$ and axis UV (respectively, center V and axis $\mathcal{O}U$) is isomorphic to the multiplicative group of the right(left) nucleus and the multiplicative group of the right(left) nucleus is a subgroup of the multiplicative group K^*, then the order of the corresponding homology group will divide the order of K^*. Therefore the order is $p^s - 1$, where $s = \gcd(r, a, b)$.

$\square$

Now we apply these results to some specific examples.

3.3 Examples

Examples of semifields $S(K, \alpha, \beta, A, B)$ for different fields $K = GF(p^n)$ were found using a computer program. In Table 3.1, we list the parameters that yield semifields with the product under study. In the table γ is a primitive element in K, that is, γ is a generator of the multiplicative group $K^{\times}$. For all the orders under study this is not a complete listing, but for $3^4, 3^5$, and 3^6, with the exception of a change in primitive elements, this is an exhaustive list. Of the fields of small order we investigated no parameters were found to yield semifields over $GF(3^7), GF(3^9), GF(3^{10}), GF(5^7)$, $GF(5^9), GF(5^{10})$, $GF(7^7), GF(11^5), GF(13^5)$.

Note that for any pre-semifield with the product $x \circ y = xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha}$, if $\alpha^3 = 1$ when $\alpha\beta = 1$, then the corresponding semifield is a generalized twisted field. Since the semifields corresponding to rows #14, 18, 20 and 22 in Table 3.1 have $\alpha^3 = 1$ when $\alpha\beta = 1$ they are generalized twisted fields.

The semifields corresponding to rows #1, 2, 3, 4, 9, 10, 11, 15, 16, 17, 19, 21, and 23 have $\alpha^3 = 1$ when $\alpha\beta = 1$. Of these, the semifields corresponding to rows #1, 2, 3, 4, 11, 16, and 23 have $CC^{\alpha} = -1$, so $g_a \neq 0$ for these. For the semifields

Table 3.1. Parameters for the Semifields Under Study

#	*Prime*	*Power*	a	b	u	v	*Irreducible Polynomial for* γ
1	3	4	1	3	0	10	x^4+2x+2
2	3	4	1	3	0	14	x^4+2x+2
3	3	4	1	3	0	2	x^4+2x^3+2
4	3	4	1	3	0	6	x^4+2x^3+2
5	3	5	2	4	0	11	x^5+2x+1
6	3	5	2	4	1	10	x^5+2x+1
7	3	5	2	4	1	21	x^5+2x+1
8	3	6	1	3	1	13	x^6+x+2
9	3	8	2	6	0	28	x^8+2x^3+2
10	3	12	3	9	0	82	$x^{12}+2x^4+2x^3+2x^2+x+2$
11	5	4	1	3	2	6	x^4+4x^2+4x+3
12	5	5	3	4	2	20	x^5+4x+3
13	5	6	3	5	1	97	x^6+3x+3
14	5	6	2	4	0	24	x^6+3x+3
15	5	8	2	6	0	0	x^8+4x^2+4x+3
16	7	4	1	3	0	6	x^4+6x^2+4x+5
17	7	4	1	3	2	18	x^4+6x^2+4x+5
18	7	6	2	4	0	48	x^6+6x^2+4x+5
19	11	4	1	3	0	54	x^4+6x+8
20	11	6	2	4	0	120	x^6+4x^2+7x+8
21	13	4	1	3	0	56	$x^4+12x^2+9x+11$
22	13	6	2	4	0	168	$x^6+11x^2+9x+11$
23	17	4	1	3	0	16	$x^4+16x^2+11x+14$

corresponding to rows # 9, 10, 15, 17, 19, and 21, $CC^{\alpha} \neq -1$ which implies $g_a = 0$. In these cases the homologies are of the first forms given in Theorems 3.4, 3.5, and 3.6. So the order of the middle nucleus is $p^{(r,b-a)} = p^{(4a,3a-a)} = p^{2a}$. The left and right nuclei are of order $p^{(r,a,b)} = p^{(4a,a,3a)} = p^{a}$. Thus the semifield as a vector space over its nuclei has dimension 4 over its left and right nuclei and dimension 2 over its middle nucleus. It should be noted that all of the p-primitive semifields of order p^4 with right nucleus isomorphic to the left nucleus have been characterized by Cordero in [8]-[11]. However, for the semifields of order p^4 in Table 3.1 the left and right nucleus are not isomorphic. In [13] Cordero and Figueroa proved explicitly that all of the semifields of order 3^4 with the product under study are generalized twisted fields.

It remains to look at the semifields corresponding to rows # 5, 6, 7, 8, 12, and 13. For these we show that they are not generalized twisted fields. All of the autotopisms of these semifields are of the form found in Theorem 3.3. First let $G(y) = dy^\theta$ and $F(x) = cx^\theta$. Recall $H(n) = \dfrac{d}{c}n^\theta$. Since c and d are in K, and γ generates the multiplicative group $K^\times$, there exist positive integers k and j such that $c = \gamma^k$ and $d = \gamma^j$. Using the equations from Theorem 3.3, that is, $dc^\beta A^\theta = Ac^\alpha d^\beta$ and $dc^\alpha B^\theta = Bc^\beta d^\alpha$, we have the values for k and j given in Table 3.2. In this table, the first column gives the corresponding row in Table 3.1. For the first four rows in Table 3.2 , t can be 0 or 1 and for the remaining rows $0 \le t \le 3$. When $\theta = 1$ and $t = 0$, s_0 gives the values of c and d that define an autotopism of order a $p-$primitive divisor of $p^n - 1$.

Table 3.2. Values for powers of γ

#	k	j	range of s	s_0
5	$\frac{7(\theta-1)}{2} + 11s$	$\frac{\theta-1}{8} + 143s + 121t$	$1 \le s \le 22$	12
6	$18(\theta-1) + 11s$	$\frac{83(\theta-1)}{4} + 143s + 121t$	$1 \le s \le 22$	12
7	$5(\theta-1) + 11s$	$\frac{113(\theta-1)}{78} + 143s + 121t$	$1 \le s \le 22$	12
8	$\frac{\theta-1}{2} + 13s$	$\frac{\theta-1}{2} + 572s + 364t$	$1 \le s \le 56$	8
12	$\frac{29(\theta-1)}{2} + 71s$	$\frac{2176(\theta-1)}{2} + 1704s + 781t$	$1 \le s \le 44$	24
13	$\frac{42(\theta-1)}{4} + 93s$	$\frac{2641(\theta-1)}{4} + 2790s + 3906t$	$1 \le s \le 168$	24

Theorem 3.8. *The semifields corresponding to the parameters in Table 3.2 are not generalized twisted fields.*

Proof. Assume that $\pi(K, \alpha, \beta, A, B)$ is a semifield plane coordinatized by a generalized twisted field. The left and right nuclei of π have the same order. From [7], $\mathcal{A}(\pi)$, the full autotopism group of π , admits a cyclic group that acts transitively on the non vertex points on the line $\mathcal{O}U$. Also from [7], $\mathcal{A}(\pi)$ is a subgroup of $\Gamma L(1, K) \times \Gamma L(1, K)$. Now each pre-semifield under consideration admits an autotopism (F_0, G_0, H_0) with $F_0(x) = cx$ and $G_0(y) = dy$ where $c, d \in K$ have order a $p-$primitive prime divisor of $p^r - 1$. Since the subgroup generated by this autotopism is normal in $\mathcal{A}(\pi)$, and for a generalized twisted field, Liebler [23] showed the normalizer is all of $\mathcal{A}(\pi)$, then every element in $\mathcal{A}(\pi)$ is of the form given in Theorem 3.3 and is transitive. However, from the table above, we see that none of the elements have order $p^r - 1$.

$\square$

By Albert's Isomorphism Theorem in [4], two semifield planes are isomorphic if and only if the semifields that coordinatize them are isotopic. The following theorem gives the conditions for the semifields under study to be isotopic.

Theorem 3.9. *Let (F, G, H) be an isotopism of $S(K, \alpha, \beta, A, B)$ onto $S(K, \alpha', \beta', A', B')$ where $\alpha^3 \neq 1$ when $\alpha\beta = 1$with $F(x) = cx^\sigma, G(y) = dy^\theta$ and $H(n) = hn^\tau$. Then one of the following must occur:*

(i) $\alpha = \alpha', \beta = \beta'$, $A' = d^{1-\beta}c^{\beta-\alpha}A^\theta$, *and* $B' = d^{\alpha-1}c^{\alpha-\beta}B^\theta$.

(ii) $\beta = \alpha', \alpha = \beta'$, $A' = d^{1-\alpha}c^{\alpha-\beta}B^\theta$, *and* $B' = d^{1-\beta}c^{\beta-\alpha}A^\theta$

Proof. Suppose that $S(K, \alpha, \beta, A, B)$ and $S(K, \alpha', \beta', A', B')$ are isotopic; let (F, G, H) where $F(x) = cx^{\sigma}, G(y) = dy^{\theta}$, and $H(n) = hn^{\tau}$ be an isotopism between them. Then

$$G(x \circ n) = F(x) \circ' H(n)$$

Therefore, $G(xn+Ax^{\alpha}n^{\beta}+Bx^{\beta}n^{\alpha})=F(x)H(n)+A'F^{\alpha'}(x)H^{\beta'}(n) + B'F^{\beta'}(x)H^{\alpha'}(n)$

and $dx^{\theta}n^{\theta} + dA^{\theta}x^{\alpha\theta}n^{\beta\theta} + dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = cx^{\sigma}hn^{\tau} + A'(cx^{\sigma})^{\alpha'}(hn^{\tau})^{\beta'} + B'(cx^{\sigma})^{\beta'}(hn^{\tau})^{\alpha'}$

$$dx^{\theta}n^{\theta} + dA^{\theta}x^{\alpha\theta}n^{\beta\theta} + dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = cx^{\sigma}hn^{\tau} + A'c^{\alpha'}x^{\sigma\alpha'}h^{\beta'}n^{\tau\beta'} + B'c^{\beta'}x^{\sigma\beta'}h^{\alpha'}n^{\tau\alpha'}$$

$$dx^{\theta}n^{\theta} + dA^{\theta}x^{\alpha\theta}n^{\beta\theta} + dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = chx^{\sigma}n^{\tau} + A'c^{\alpha'}h^{\beta'}x^{\sigma\alpha'}n^{\tau\beta'} + B'c^{\beta'}h^{\alpha'}x^{\sigma\beta'}n^{\tau\alpha'}$$

$$E_1 \quad + \quad E_2 \quad + \quad E_3 \quad = \quad E_4 \quad + \quad E_5 \quad + \quad E_6 \qquad (3.33)$$

We now check the different possibilities for this to be true.

$\underline{E_1 = E_4, E_2 = E_5, E_3 = E_6}$

For this case we have $dx^{\theta}n^{\theta} = chx^{\sigma}n^{\tau}$, $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} = A'c^{\alpha'}h^{\beta'}x^{\sigma\alpha'}n^{\tau\beta'}$, and $dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = B'c^{\beta'}h^{\alpha'}x^{\sigma\beta'}n^{\tau\alpha'}$. So $\theta = \sigma$ and $\theta = \tau$. From the first equation we have $d = ch$ which implies $h = \dfrac{d}{c}$. By replacing τ and σ with θ, we get $x^{\alpha\theta} = x^{\alpha'\theta}$ which implies that $\alpha\theta = \alpha'\theta$; hence $\alpha = \alpha'$. Similarly $n^{\beta\theta} = n^{\beta'\theta}$ implies $\beta = \beta'$.

From the coefficients of the second and third equations, we get:

$$dA^{\theta} = A'c^{\alpha'}h^{\beta'}$$

$$\frac{dA^{\theta}}{c^{\alpha'}h^{\beta'}} = A'$$

$$\frac{dA^{\theta}}{c^{\alpha}h^{\beta}} = A'$$

$$\frac{dA^{\theta}}{c^{\alpha}h^{\beta}} = A'$$

$$\frac{dA^\theta}{c^\alpha(\frac{d}{c})^\beta} = A'$$
$$d^{1-\beta}c^{\beta-\alpha}A^\theta = A'$$

and

$$dB^\theta = B'c^{\beta'}h^{\alpha'}$$
$$\frac{dB^\theta}{c^{\beta'}h^{\alpha'}} = B'$$
$$\frac{dB^\theta}{c^\beta h^\alpha} = B'$$
$$\frac{dB^\theta}{c^\beta(\frac{d}{c})^\alpha} = B'$$
$$d^{1-\alpha}c^{\alpha-\beta}B^\theta = B'$$

$\underline{E_1 = E_4, E_2 = E_6, E_3 = E_5}$

For this case we have $dx^\theta n^\theta = chx^\sigma n^\tau$, $dA^\theta x^{\alpha\theta}n^{\beta\theta} = B'c^{\beta'}h^{\alpha'}x^{\sigma\beta'}n^{\tau\alpha'}$, and $dB^\theta x^{\beta\theta}n^{\alpha\theta} = A'c^{\alpha'}h^{\beta'}x^{\sigma\alpha'}n^{\tau\beta'}$. Thus $\theta = \sigma$ and $\theta = \tau$. From the first equation we have $d = ch$ which implies $h = \dfrac{d}{c}$. By replacing τ and σ with θ, we get $x^{\alpha\theta} = x^{\beta'\theta}$ which implies that $\alpha\theta = \beta'\theta$; hence $\alpha = \beta'$. Similarly $n^{\beta\theta} = n^{\alpha'\theta}$ implies $\beta = \alpha'$.

From the coefficients of the second and third equations, we have

$$dB^\theta = A'c^{\alpha'}h^{\beta'}$$
$$\frac{dB^\theta}{c^{\alpha'}h^{\beta'}} = A'$$
$$\frac{dB^\theta}{c^\beta h^\alpha} = A'$$
$$\frac{dB^\theta}{c^\beta h^\alpha} = A'$$
$$\frac{dB^\theta}{c^\beta(\frac{d}{c})^\alpha} = A'$$
$$d^{1-\alpha}c^{\alpha-\beta}B^\theta = A'$$

and

$$dA^{\theta} = B'c^{\beta'}h^{\alpha'}$$
$$\frac{dA^{\theta}}{c^{\beta'}h^{\alpha'}} = B'$$
$$\frac{dA^{\theta}}{c^{\alpha}h^{\beta}} = B'$$
$$\frac{dA^{\theta}}{c^{\alpha}(\frac{d}{c})^{\beta}} = B'$$
$$d^{1-\beta}c^{\beta-\alpha}A^{\theta} = B'$$

$\underline{E_1 = E_5, E_2 = E_4, E_3 = E_6}$

In this case we have $dx^{\theta}n^{\theta} = A'c^{\alpha'}h^{\beta'}x^{\sigma\alpha'}n^{\tau\beta'}$, $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} = chx^{\sigma}n^{\tau}$, and $dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = B'c^{\beta'}h^{\alpha'}x^{\sigma\beta'}n^{\tau\alpha'}$. From these equations we get: $\theta = \sigma\alpha'$, $\theta = \tau\beta'$, $\alpha\theta = \sigma$, $\beta\theta = \tau$, $\beta\theta = \sigma\beta'$, and $\alpha\theta = \tau\alpha'$. From these we get $\theta = \alpha\theta\alpha'$ which implies $1 = \alpha\alpha'$. Hence $\alpha^{-1} = \alpha'$. Similarly we get $\beta^{-1} = \beta'$. Now $\alpha\theta = \tau\alpha^{-1}$, so $\alpha^2 = \tau\theta^{-1}$. This gives $\alpha^2 = \beta\theta\theta^{-1}$ so, $\alpha^2 = \beta$. Also, $\beta\theta = \sigma\beta^{-1}$, so $\beta^2 = \sigma\theta^{-1}$. This gives $\beta^2 = \alpha\theta\theta^{-1}$ so, $\beta^2 = \alpha$. Since $\alpha^2 = \beta$ and $\beta^2 = \alpha$, we get $\alpha^3 = 1$ when $\alpha\beta = 1$. By the stated assumption this cannot happen.

$\underline{E_1 = E_5, E_2 = E_6, E_3 = E_4}$

In this case $dx^{\theta}n^{\theta} = A'c^{\alpha'}h^{\beta'}x^{\sigma\alpha'}n^{\tau\beta'}$, $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} = B'c^{\beta'}h^{\alpha'}x^{\sigma\beta'}n^{\tau\alpha'}$, and $dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = chx^{\sigma}n^{\tau}$. From the powers on the variables, we get $\theta = \sigma\alpha'$, $\theta = \tau\beta'$, $\alpha\theta = \sigma\beta'$, $\beta\theta = \tau\alpha'$, $\beta\theta = \sigma$, and $\alpha\theta = \tau$. From here we get $\theta = \beta\theta\alpha'$ and thus $\beta^{-1} = \alpha'$. Also $\theta = \alpha\theta\beta'$ so $\alpha^{-1} = \beta'$. Moreover, $\alpha\theta = \beta\theta\beta'$; hence $\alpha\beta^{-1} = \beta'$. and $\beta\theta = \alpha\theta\alpha'$ so $\beta\alpha^{-1} = \alpha'$. From here we get $\alpha = \beta^2$ and $\beta^2 = \alpha$. These last two relationships lead to $\alpha^3 = 1$ when $\alpha\beta = 1$. Therefore this case is not possible.

$\underline{E_1 = E_6, E_2 = E_4, E_3 = E_5}$

In this case $dx^{\theta}n^{\theta} = B'c^{\beta'}h^{\alpha'}x^{\sigma\beta'}n^{\tau\alpha'}$, $dA^{\theta}x^{\alpha\theta}n^{\beta\theta} = chx^{\sigma}n^{\tau}$, and $dB^{\theta}x^{\beta\theta}n^{\alpha\theta} = A'c^{\alpha'}h^{\beta'}x^{\sigma\alpha'}n^{\tau\beta'}$. From the powers on the variables, we get $\theta = \sigma\beta'$, $\theta = \tau\alpha'$, $\alpha\theta = \sigma$,

$\beta\theta = \tau$, $\beta\theta = \sigma\alpha'$, and $\alpha\theta = \tau\beta'$. From these we get $\theta = \beta\theta\alpha'$ and thus $\beta^{-1} = \alpha'$. Moreover $\theta = \alpha\theta\beta'$; hence $\alpha^{-1} = \beta'$. Also $\alpha\theta = \beta\theta\beta'$ which implies $\alpha\beta^{-1} = \beta'$. Therefore $\beta\theta = \alpha\theta\alpha'$; hence $\beta\alpha^{-1} = \alpha'$. From these we get $\alpha = \beta^2$ and $\beta^2 = \alpha$. These last two relationships lead to $\alpha^3 = 1$ when $\alpha\beta = 1$. Therefore this case is not possible.

$\underline{E_1 = E_6, E_2 = E_5, E_3 = E_4}$

In this case $dx^\theta n^\theta = B'c^{\beta'}h^{\alpha'}x^{\sigma\beta'}n^{\tau\alpha'}$, $dA^\theta x^{\alpha\theta}n^{\beta\theta} = A'c^{\alpha'}h^{\beta'}x^{\sigma\alpha'}n^{\tau\beta'}$, and $dB^\theta x^{\beta\theta}n^{\alpha\theta} = chx^\sigma n^\tau$. From the powers on the variables, we get $\theta = \sigma\beta'$, $\theta = \tau\alpha'$, $\alpha\theta = \sigma\alpha'$, $\beta\theta = \tau\beta'$, $\beta\theta = \sigma$, and $\alpha\theta = \tau$. From these we get $\theta = \beta\theta\beta'$ and thus $\beta^{-1} = \beta'$. Now, $\theta = \alpha\theta\alpha'$ so $\alpha^{-1} = \alpha'$. Also $\alpha\theta = \beta\theta\alpha'$ so $\alpha\beta^{-1} = \alpha'$ and $\beta\theta = \alpha\theta\beta'$; hence $\beta\alpha^{-1} = \beta'$. From these we get $\alpha = \beta^2$ and $\beta^2 = \alpha$. These last two relationships lead to $\alpha^3 = 1$ when $\alpha\beta = 1$. Therefore this case is not possible either.

The cases considered above are the only possibilities to obtain equality in equation (3.33). Hence the result follows. $\square$

As evident from Table 3.1 for $GF(3^4)$,$GF(3^5)$, and $GF(7^4)$, we have multiple values of A and B that yield a semifield. This will happen in other cases as well. By using the isotopism theorem, Theorem 3.9, since the values of α and β are the same, we can explicitly see which values of A and B give isotopic semifields which would then coordinatize isomorphic planes. For this case, $A' = d^{1-\beta}c^{\beta-\alpha}A^\theta$, and $B' = d^{\alpha-1}c^{\alpha-\beta}B^\theta$, so for $GF(3^4)$, $A' = d^{1-\beta}c^{\beta-\alpha}A^\theta = d^{1-3^2}c^{3^2-3^1}(\gamma^0)^\theta = \dfrac{(\gamma^k)^6}{(\gamma^j)^2}$.

By letting k and j be 0, we get $A' = \gamma^2$. Now using $c = d = \gamma^6$, we get $B' = d^{\alpha-1}c^{\alpha-\beta}B^\theta = B^\theta$. By choosing $\theta = 3$ we get $B' = B^\theta = (\gamma^2)^3 = \gamma^6$. Therefore in Table 3.1 #3 and #4 are isotopic.

Notice that the semifield corresponding to the parameters listed in #15 is the only semifield that coordinatizes a self dual plane. For a semifield with the product $\circ$, the multiplication of the semifield that coordinatizes the dual plane is $x \circ' y = y \circ x$.

Thus a plane will be self dual if $x \circ y = y \circ x$. For the semifields under study we have the following result.

Lemma 3.2. *A semifield plane $\pi(K, \alpha, \beta, A, B)$ coordinatized by a semifield with product $x \circ y = xy + Ax^\alpha y^\beta + Bx^\alpha y^\beta$ is self dual if and only if $A = B$. The only self-dual planes $\pi(K, \alpha, \beta, A, B)$ are the generalized twisted field planes.*

Proof. A plane is self-dual if $x \circ y = y \circ x$. Therefore we must have $xy + Ax^\alpha y^\beta + Bx^\beta y^\alpha = yx + Ay^\alpha x^\beta + By^\beta x^\alpha$. That is, $Ax^\alpha y^\beta + Bx^\beta y^\alpha = Ay^\alpha x^\beta + By^\beta x^\alpha$.

Thus either $Ax^\alpha y^\beta = Ay^\alpha x^\beta$ and $Bx^\beta y^\alpha = By^\beta x^\alpha$ in which case $\alpha = \beta$, which cannot occur, or $Ax^\alpha y^\beta = By^\beta x^\alpha$ and $Bx^\beta y^\alpha = Ay^\alpha x^\beta$ in which case $A = B$. If $A = B$, we get from [7] that $\pi(K, \alpha, \beta, A, B)$ is a generalized twisted field. □

3.3.1 Semifields from $GF(3^5)$

To begin we find an irreducible polynomial in $GF(3^5)$ over $GF(3)$ and use the polynomial to generate the elements of the pre-semifield. We chose $f(x) = x^5 + 2x + 1$ where $\gamma \in GF(3^5) - GF(3)$ is a root of f. Using a computer program it was found that the values for $A, B, a,$ and b that give a pre-semifield with product $x \circ y = xy + Ax^\alpha y^\beta + Bx^\beta y^\alpha$ are $A = 1, B = \gamma^{11}, a = 2,$ and $b = 4$. For the same irreducible polynomial and the same α and β, $A = \gamma$ with $B = \gamma^{10}$ or $A = \gamma$ with $B = \gamma^{21}$ also determine a pre-semifield. For any irreducible polynomial used to generate $GF(3^5)$, these are the only possibilities for pre-semifields. Since $\alpha : x \mapsto x^{p^a} = x^{3^2}$ and $\beta : x \mapsto x^{p^b} = x^{3^4}$, then the middle nucleus has order $p^{(r,b-a)} = 3^{(5,4-2)} = 3^1$ by Theorem 3.7. To determine the group of homologies with center U and axis $\mathcal{O}V$, which is isomorphic to the middle nucleus, we find the values of $c \in GF(3^5)$ for which $c^\alpha = c^\beta, c \neq 0$. These elements are $\gamma^0 = 1$ and γ^{121}. The right and left nucleus have order $p^{(r,a,b)} = 3^{(5,2,4)} = 3^1$ by Theorem 3.7.

Since all the nuclei are isomorphic to the field $GF(3)$, the center is also $GF(3)$. For the different semifields, the elements of the nuclei and the center are:

For $A = \gamma^0, B = \gamma^{11} : 0, \gamma^{216}$, and γ^{95} are the elements of the nuclei and center.

For $A = \gamma^1, B = \gamma^{10} : 0, \gamma^{131}$, and γ^{10} are the elements of the nuclei and center.

For $A = \gamma^1, B = \gamma^{21} : 0, \gamma^{107}$, and γ^{228} are the elements of the nuclei and center.

For every semifield of order $GF(3^5)$, regardless of the irreducible polynomial used, these are the only choices.

3.3.2 Semifields from $GF(3^6)$

To begin we find an irreducible polynomial in $GF(3^6)$ to generate the elements; we chose $f(x) = x^6 + x + 2$. Again a computer program was used to obtain the parameters that define a pre-semifield with the product $x \circ y = xy + Ax^{\alpha}y^{\beta} + Bx^{\beta}y^{\alpha}$. These values are $A = \gamma, B = \gamma^{13}, a = 1,$ and $b = 3$ and for this particular irreducible polynomial, these are the only values possible.

Since $\alpha : x \mapsto x^{p^a} = x^{3^1}$ and $\beta : x \mapsto x^{p^b} = x^{3^3}$, then the middle nucleus has order $p^{(r,b-a)} = 3^{(6,3-1)} = 3^2$. To determine the group of homologies with center U and axis $\mathcal{O}V$, which is isomorphic to the middle nucleus, we find all of the values of $c \in GF(3^6)$ with $c^{\alpha} = c^{\beta}, c \neq 0$. These elements are $\gamma^0 = 1, \gamma^{91}, \gamma^{182}, \gamma^{273}, \gamma^{364}, \gamma^{455}, \gamma^{546}$, γ^{637}. Together with 0 they form a field isomorphic to $GF(3^2)$. Doing the calculations for the middle nucleus we get that the elements of the middle nucleus are $0, \gamma^{545}, \gamma^{181}, \gamma^{113}, \gamma^{91}, \gamma^{662}, \gamma^{298}, \gamma^{282}, \gamma^{477}$. The multiplication table is given in Table 3.3.

Since $\alpha : x \mapsto x^{p^a} = x^{3^1}$ and $\beta : x \mapsto x^{p^b} = x^{3^3}$ the right and left nucleus have order $p^{(r,a,b)} = 3^{(6,1,3)} = 3^1$. To determine the group of homologies with center $\mathcal{O}$ and axis UV, which is isomorphic to the right nucleus, we find all the values of $c \in GF(3^6)$ where $c^{\alpha} = c^{\beta} = c, c \neq 0$. These elements are $\gamma^0 = 1, \gamma^{364}$. Along with 0, they form

Table 3.3. Multiplication Table for Elements of the Middle Nucleus

$*$	γ^{545}	γ^{646}	γ^{662}	γ^{477}	γ^{181}	γ^{282}	γ^{298}	γ^{113}
γ^{545}	γ^{545}	γ^{646}	γ^{662}	γ^{477}	γ^{181}	γ^{282}	γ^{298}	γ^{113}
γ^{646}	γ^{646}	γ^{662}	γ^{477}	γ^{181}	γ^{282}	γ^{298}	γ^{113}	γ^{545}
γ^{662}	γ^{662}	γ^{477}	γ^{181}	γ^{282}	γ^{298}	γ^{113}	γ^{545}	γ^{646}
γ^{477}	γ^{477}	γ^{181}	γ^{282}	γ^{298}	γ^{113}	γ^{545}	γ^{646}	γ^{662}
γ^{181}	γ^{181}	γ^{282}	γ^{298}	γ^{113}	γ^{545}	γ^{646}	γ^{662}	γ^{477}
γ^{282}	γ^{282}	γ^{298}	γ^{113}	γ^{545}	γ^{646}	γ^{662}	γ^{477}	γ^{181}
γ^{298}	γ^{298}	γ^{113}	γ^{545}	γ^{646}	γ^{662}	γ^{477}	γ^{181}	γ^{282}
γ^{113}	γ^{113}	γ^{545}	γ^{646}	γ^{662}	γ^{477}	γ^{181}	γ^{282}	γ^{298}

a field isomorphic to $GF(3)$. Doing the calculations for the right nucleus we get the elements $0, \gamma^{181}, \gamma^{545}$. To determine the group of homologies with center V and axis $\mathcal{O}U$, which is isomorphic to the left nucleus, we find all the values of $c \in GF(3^6)$ where $c^\alpha = c^\beta = c, c \neq 0$. These elements are $\gamma^0 = 1, \gamma^{364}$. Along with 0 they form a field isomorphic to $GF(3)$. Doing the calculations for the left nucleus we get the elements $0, \gamma^{181}, \gamma^{545}$. Thus the nucleus is $GF(3)$. Based on the order of the nuclei, we conclude that this semifield is not a generalized twisted field because the middle nucleus of a generalized twisted field is of order 3, not 9.

The center, which is isomorphic to $GF(3)$, consists of the elements 0, γ^{181}, and γ^{545}. For every semifield of order 3^6, regardless of the irreducible polynomial used to construct the field $GF(3^6)$, the parameters are $A = \gamma, B = \gamma^{13}, a = 1,$ and $b = 3$.

3.4 Autotopism Collineations

Let $\pi = \pi(K, \alpha, \beta, A, B)$ where $K = GF(p^n), p$ prime. We will consider the autotopisms of π that fix $V(\infty)$ and $V(0)$. Each autotopism will then have a matrix of the form $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ with $A, B \in \mathcal{G}$. Notice that as indicated before, π admits an autotopism g_0 of order h where h is a p-primitive prime divisor of $p^n - 1$.

By the choice of g_0 and by a basis change in $V \oplus V$ we can assume that

$$g_0 = \begin{pmatrix} T_0(\xi) & 0 \\ 0 & T_0(\eta) \end{pmatrix}$$

where ξ and $\eta \in K$ and $\xi^h = 1 = \eta^h$. Since π is not Desarguesian we have $\xi \neq \eta$ and $|\xi| = h = |\eta|$. Cordero and Figueroa [15] showed that since g_0 is an autotopism of π then there exist $a_0 = 1, a_1, a_2, \ldots, a_{n-1} \in K$ and nonnegative integers $e_0 = 0, e_1, \ldots, e_{n-1}$ such that

(i) $M(y) = [a_0 y^{(e_0)}, a_1 y^{(e_1)}, \ldots, a_{n-1} y^{(e_{n-1})}]^t \in \mathcal{G}$ for $y \neq 0$.

(ii) $\Sigma = \{V(0), V(\infty)\} \cup \{V(y) | y \in K^*\}$ is a spread for π where
$V(y) = \{((x), (x)M(y)) | x \in K\}$.

(iii) $\left(\dfrac{\eta}{\xi}\right)^{(e_\ell)} = \dfrac{\eta}{\xi^{(\ell)}}$, for each ℓ, $0 \leq \ell \leq n-1$ such that $a_\ell \neq 0$. .

From (iii) above we have if $i \neq j$ and $a_i \neq 0 \neq a_j$, then $e_i \neq e_j$, otherwise we would have $\dfrac{\eta}{\xi^{(i)}} = \dfrac{\eta}{\xi^{(j)}}$ which implies $\xi^{(i)} = \xi^{(j)}$ and since $|\alpha| = h$ and h is a p-primitive prime divisor of $p^n - 1$, then $i = j$.

Let $\mathcal{A}$ the the autotopism group of π. In [23] Liebler showed that if π is a generalized twisted field plane, then the subgroup generated by g_0 is normal in $\mathcal{A}$. We now look at the normalizer of $< g_0 >$ in $\mathcal{A}$.

Theorem 3.10. *Let* $H = \left\{ g = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} : g \in \mathcal{A} \text{ and } g \text{ normalizes } < g_0 > \right\}$ *and let* $g \in H$. *Then there exist* $a, b \in K$ *such that* $g = \begin{pmatrix} T_k(a) & 0 \\ 0 & T_k(b) \end{pmatrix}$.

For the proof we need the following lemma.

Lemma 3.3.

(i) $(T_k(a))^i = T_{ik}(a_i)$ *where* $a_i = aa^{(k)}a^{(2k)} \cdots a^{((i-1)k)}$ *and* ik *is taken modulo* n.

(ii) $T_k(a)^{-1} = T_{n-k}\left(\frac{1}{a^{(n-k)}}\right)$

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

Proof.

(i) Label the columns and rows of $T_k(a)$ by $0, 1, 2, \ldots n-1$. Consider $T_k(a)T_k(a) = C$. Since every row and column of $T_k(a)$ has only one non-zero element, then the value of the non-zero position in the first column of C is determined by the product of the element in the $s \times k$ position of $T_k(a)$ times the element in the $k \times 0$ position of $T_k(a)$. The element in the first column of the $T_k(a)$ matrix on the left is in row k, so the element in the k^{th} column of matrix C will be in row $k + k = 2k$. The power of the non-zero element corresponds to the column number, so this element in the matrix $T_k(a)$ on the left is $a^{(k)}$ in column k. Therefore in matrix C, the nonzero element is in row $2k$ and column 0 and will be $a^{(k)}a$. Thus $(T_k(a))^2 = T_{2k}(a_2)$ where $a_2 = aa^{(k)}$.
Suppose this holds for m, that is, $T_k(a)^m = T_{mk}(a_m)$ where $a_m = aa^{(k)}a^{(2k)} \cdots a^{((m-1)k)}$. Then $T_k(a)^{m+1} = T_k(a)^m T_k(a) = T_{mk}(a_m)T_k(a) = T_t(c)$. Therefore since $T_k(a)$ is again the second matrix, the element in the $t \times k$ position of the first matrix times the element in the $k \times 0$ position of the second matrix will give the element in the first column of the new matrix. The element in the first column of the first matrix is in the mk^{th} row, so the element in the k^{th} column will be in row $mk + k = k(m+1)$. The non-zero element from the first matrix in the k^{th} column is $a_m^{(k)}$ and the non-zero element from row k in the second matrix is a, so the non-zero element in the first column of the new matrix will be $a_m^{(k)} \cdot a$.

Thus the new matrix will be $T_{mk+k}(a_m^{(k)}a) = T_{m(k+1)}((aa^{(k)}a^{(2k)}\cdots a^{((m-1)k)})^{(k)}a)$
$= T_{m(k+1)}(a^{(k)}a^{(2k)}a^{(3k)}\cdots a^{((m-1)k+k)}a) = T_{m(k+1)}(aa^{(k)}a^{(2k)}a^{(3k)}\cdots a^{(m)})$
$= T_{m(k+1)}(a_{m+1})$.

(ii) Let $T_k(a)T_l(b) = T_0(1)$ where $T_0(1)$ is the identity matrix. We need to find the values of l and b that make this true. Since $T_k(a)$ matrices are named for the row k of the non-zero element, a, of the first column, we need to determine the element from row 0 and column l of $T_k(a)$ and the element from row l and column 0 of $T_l(b)$. Then, the element in the first row of $T_k(a)$ is $a^{(n-k)}$ and is in column number $n-k$. Thus $l = n-k$. Also, $a^{(n-k)}b = 1$, so $b = \dfrac{1}{a^{(n-k)}}$. Therefore, $T_k(a)^{-1} = T_l(b) = T_{n-k}\left(\dfrac{1}{a^{(n-k)}}\right)$.

(iii) Consider the product $T_k\,(a)\,T_l\,(b)$. Clearly this is of the form $T_s\,(c)$ for some $s \in \mathbb{Z}_n$ and some $c \in K$. Then the non-zero element, c, will come from the row s and column l of the first matrix $T_k(a)$ and row l and column 0 of matrix $T_l(b)$. The element in the row l of $T_k(a)$ is $a^{(l)}$, so $c = a^{(l)}b$. We then have $s = k+l$ since $a^{(l)}$ is in column l and row $k+l$. This row position from $T_k(a)$ defines the row position for $T_s(c)$. Therefore, $T_k\,(a)\,T_l\,(b) = T_{l+k}\left(a^{(l)}b\right)$.

□

We now provide a proof of Theorem 3.10:

Proof. Let $g = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ normalize $< g_0 >$. Then $A^{-1}T_0(\xi)A = T_0(\xi)^i = T_0(\xi^i)$ and $B^{-1}T_0(\eta)B = T_0(\eta)^j = T_0(\eta^j)$for some i, j.

Using the fact that $A^{-1}T_0(\xi)A = T_0(\xi^i)$ we get $A = T_k(a)$ for some k and a. Similarly since $B^{-1}T_0(\eta)B = T_0(\eta^j)$ we get $B = T_\ell(b)$ for some ℓ and b. If $g \in H \cap \mathcal{A}$ where $\mathcal{A}$ is the autotopism group of π, then $g^{-1}g_0g = \begin{pmatrix} T_0(\xi^{(k)}) & 0 \\ 0 & T_0(\eta^{(l)}) \end{pmatrix} \in \mathcal{A}$

and since $g_0^{-p^k} = \begin{pmatrix} T_0(\xi^{-p^k}) & 0 \\ 0 & T_0(\eta^{-p^k}) \end{pmatrix}$ we will have $g^{-1}g_0 g g_0^{-p^k}$ is an autotopism of the form $\begin{pmatrix} I & 0 \\ 0 & T_0(\eta^{p^\ell - p^k}) \end{pmatrix}$ where I is the identity. Since π is non-Desarguesian, π does not admit an autotopism of the form $\begin{pmatrix} I & 0 \\ 0 & T_0(\zeta) \end{pmatrix}$ with $|\zeta| = h$. Therefore $\eta^{p^l - p^k} = 1$ and together with $|\eta| = h$ imply $\ell = k$. Therefore the autotopisms of π that normalize $< g_0 >$ are of the form $\begin{pmatrix} T_k(a) & 0 \\ 0 & T_k(b) \end{pmatrix}$.

$\square$

Notice that if $g = \begin{pmatrix} T_k(a) & 0 \\ 0 & T_k(b) \end{pmatrix}$ is an autotopism of π, then

$$V(y)^g = g^{-1}V(y)g = \{((x), (x)T_k(a)^{-1}M(y)T_k(b))|x \in K\}$$

is also contained in Σ. Since

$$T_k(a)^{-1}[x_0, x_1, \ldots, x_{n-1}]^t T_k(a) = \left[x_0^{(k)}, \frac{a}{a^{(1)}}x_1^{(k)}, \ldots, \frac{a}{a^{(n-1)}}x_{n-1}^{(k)}\right]^t$$

and

$$T_k(a)^{-1}M(y)T_k(b) = T_k(a)^{-1}M(y)T_k(a)T_k(a)^{-1}T_k(b)$$

we get that g is an autotopism if and only if

$$a_\ell \left(\frac{b}{a}\right)^{(e_\ell)} = a_\ell^{(k)} \frac{b}{a^{(\ell)}} \quad \text{for all } \ell. \tag{3.34}$$

3.4.1 Example of order 3^6

We study the autotopisms of the semifield $\mathcal{S} = S(K, \alpha, \beta, A, B)$ where $K = GF(3^6) = GF(3)[\gamma]$ with $\gamma^6 + \gamma + 2 = 0$. The element γ has order $3^6 - 1 = 728 = 2^3 \cdot 7 \cdot 13$. The product in $\mathcal{S}$ is given by $x \circ y = xy + \gamma x^3 y^{27} + \gamma^{13} x^{27} y^3$. The corresponding semifield plane admits an autotopism, g_0 of order 7, the only 3-primitive prime divisor of $3^6 - 1$.

First we will look at autotopisms of the form $\begin{pmatrix} T_0(a) & 0 \\ 0 & T_0(b) \end{pmatrix}$. By equation 3.34, we have $\left(\frac{b}{a}\right)^{27} = \frac{b}{a^3}$. Thus $b^{26} = a^{24}$ and $b^2 = a^{-24}$. Therefore $\left(\frac{b}{a^{-12}}\right)^2 = 1$ and $b = \pm a^{-12}$. With $a = \gamma^r$ we have $\gamma^{-12 \cdot 26r} = \gamma^{24r}$, and $-12 \cdot 26r \equiv 24r \bmod (2^3 \cdot 7 \cdot 13)$ and therefore $13|r$.

Hence $\begin{pmatrix} T_0(a) & 0 \\ 0 & T_0(b) \end{pmatrix} = \begin{pmatrix} T_0(\gamma^{13s}) & 0 \\ 0 & \pm T_0(\gamma^{-12 \cdot 13s}) \end{pmatrix}$ with $s \in \mathbb{Z}$.

Now we look at the autotopisms of the form $\begin{pmatrix} T_k(c) & 0 \\ 0 & T_k(d) \end{pmatrix}$. From equation 3.34 using $k = 1$ we get $\gamma \left(\frac{d}{c}\right)^{27} = \gamma^3 \frac{d}{c^3}$ and $\gamma^{13} \left(\frac{d}{c}\right)^3 = \gamma^{13 \cdot 3} \frac{d}{c^{27}}$. From this we get $\begin{pmatrix} T_k(c) & 0 \\ 0 & T_k(d) \end{pmatrix} = \begin{pmatrix} T_1(\gamma\gamma^{-13s}) & 0 \\ 0 & \pm T_1(\gamma\gamma^{12 \cdot 13s}) \end{pmatrix}$ for some $s \in \mathbb{Z}$.

Now let $f_0 = \begin{pmatrix} T_0(1) & 0 \\ 0 & -T_0(1) \end{pmatrix}$, $f_1 = \begin{pmatrix} T_0(\gamma^{13}) & 0 \\ 0 & T_0(\gamma^{-12 \cdot 13}) \end{pmatrix}$, and $f_2 = \begin{pmatrix} T_1(\gamma) & 0 \\ 0 & T_1(\gamma) \end{pmatrix}$.

As above let H be the subgroup of $\mathcal{A}$ of all autotopisms that normalize $< g_0 >$

with $|g_0| = 7$. Let $H_0 = \left\{ \begin{pmatrix} T_0(a) & 0 \\ 0 & T_0(b) \end{pmatrix} \in H \right\}$. If $\begin{pmatrix} T_k(c) & 0 \\ 0 & T_k(d) \end{pmatrix} \in H$ and $k \neq 0$, then $\begin{pmatrix} T_k(c) & 0 \\ 0 & T_k(d) \end{pmatrix} f_2^{-k} \in H_0$, so H is generated by H_0 and f_2. Moreover, $\begin{pmatrix} T_0(a) & 0 \\ 0 & T_0(b) \end{pmatrix} = \begin{pmatrix} T_0(\gamma^{13s}) & 0 \\ 0 & \pm T_0(\gamma^{-12 \cdot 13s}) \end{pmatrix} = f_0^i f_1^s$ with $i = 0$ or $i = 1$. Therefore H_0 is generated by f_0 and f_1. The order of $f_1 = 8 \cdot 7 = 56$. If $f_0 \notin < f_1 >$, then $|H_0| = 2 \cdot 8 \cdot 7$. If $f_0 \in < f_1 >$, then $|H_0| = 8 \cdot 7$. In either case, $|H_0| \leq 2 \cdot 8 \cdot 7$. On the other hand, $f_2^6 \in H_0$ and since H_0 is normal in $H, |H| = 6|H_0| \leq 6 \cdot 2 \cdot 8 \cdot 7 \leq 8 \cdot 7 \cdot 13 = 3^6 - 1$.

From here it follows that H is not transitive in $\mathcal{O}V$, $\mathcal{O}U$, or UV. Notice that $g_0 = f_1^8$ is of order 7 and corresponds to the values of k and j that we found for $GF(3^6)$ in Table 3.2.

We have proven the following result:

Theorem 3.11. *Let $K = GF(3^6) = GF(3)[\gamma]$ where $\gamma^6 + \gamma + 2 = 0$. Let $\mathcal{S} = (K, \alpha, \beta, A, B) = (GF(3^6), \alpha, \beta, \gamma, \gamma^{13})$ be the semifield of order 3^6 with product $x \circ y = xy + \gamma x^3 y^{27} + \gamma^{13} x^{27} y^3$ where $x, y \in K$ and let $\mathcal{A}$ be its autotopism group. Let $g_0 = \begin{pmatrix} T_0(\xi) & 0 \\ 0 & T_0(\eta) \end{pmatrix}$ where ξ and $\eta \in K$ and $\xi^7 = 1 = \eta^7$ and let $H = \mathcal{N}_{\mathcal{A}}(< g_0 >)$. Then $|H| < 3^6 - 1$.*

REFERENCES

[1] Albert, A.A., *On non associative division algebras*, Trans. Amer. Math Soc. 72 (1952), pp. 296-309.

[2] Albert, A.A., *On the collineation groups associated with twisted fields*, Calcutta Math. Soc., Golden Jubilee Commem. Vol. (1958-1959), Part 2, (1959), pp. 485-497.

[3] Albert, A.A., *Finite noncommutative division algebras*, Proc. Amer. Math. Soc. 9 (1959), pp. 928-932.

[4] Albert, A.A., *Finite Division Algebras and Finite Planes*, Proceedings of Symposia in Applied Mathematics 10 (1960),pp. 53-70.

[5] Albert, A.A., *Generalized twisted fields*, Pacific. J. Math. 11 (1961), pp. 1-8

[6] Aponte, C. and Figueroa, R., *Semifields with a 3-term product*, Private communication.

[7] Biliotti, M., Jha, V., and Johnson, N.L., *The collineation groups of generalized twisted fields planes*, Geom. Dedicata 76 (1999), pp. 97-126.

[8] Cordero, M., *p-primitive semifield planes*, Dissertation under Professor Norman Johnson, The University of Iowa, Iowa City, May 1989, published with UMI.

[9] Cordero, M., *Semifield planes of order p^4 that admit a p-primitive Baer collineation,* Osaka Journal of Mathematics, 28(1991), pp. 305-321.

[10] Cordero, M., *The autotopism group of p-primitive semifield planes,* ARS Combinatoria, 32(1991), pp. 57-64.

[11] Cordero, M., *The nuclei and other properties of p-primitive semifield planes,* International Journal of Mathematics and Mathematical Sciences, Vol 15 No. 2 (1992), pp. 367-370.

[12] Cordero, M. and Figueroa, R., *Semifield Planes admitting a transitive autotopism group,* Congressus Numerantum, 102 (1994), pp. 91-95.

[13] Cordero, M. and Figueroa, R., *Semifield planes with a transitive autotopism group,* Archiv der Mathematik, 63 (1994), pp. 17-22.

[14] Cordero, M. and Figueroa, R.,*Towards a characterization of generalized twisted field planes*. J. Geom. 52 (1995), pp. 54-63.

[15] Cordero, M. and Figueroa, R.,*Transitive autotopism groups and the generalized twisted field planes*, Mostly Finite Geometries, Lecture Notes in Pure Appl. Math. 190, Dekker, New York, (1996), pp. 191-196.

[16] Dembowski, P. *Finite Geometries*, Springer-Verlag, NewYork-Berlin, (1968).

[17] Dickson,L.E., *On finite algebras*, Nachr. Ges. Wiss. Göttingen (1905), pp. 358-393.

[18] Figueroa, R., *A characterization of the generalized twisted field planes of characteristic* ≥ 5. Geom. Dedicata 50 (1994), pp 205-216.

[19] Hughes, D.R. and Piper, F.C., *Projective Planes*, Graduate Texts in Mathematics, Vol. 6. Springer-Verlag, New York-Berlin, (1973).

[20] Johnson, N.L., Jha, V., Billoti, M., *Handbook of Finite Translation Planes*, Chapman & Hall/CRC, Boca Raton, F, (2007).

[21] Kallaher, M.J., *Affine Planes with Transitive Collineation Groups*, Elsevier, New York, (1982).

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

[23] Liebler,R. A., *On nonsingular tensors and related projective planes*, Geom. Dedicata 11, pp. 455-464 (1981).

[24] Menichetti,G. *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra 47 , pp. 400-410 (1977).

[25] Menichetti, G.,*n-dimensional algebras over a field with a cyclic extension of degree n* Geom. Dedicata, 63 (1996), pp. 69-94.

[26] Oyama, T., *On quasifields.* Osaka J. Math. 22, pp. 35-54 (1985).

BIOGRAPHICAL STATEMENT

Angela M. Brown was born in Houston, TX, in 1980. She received her B.S. and M.S. degrees from Sam Houston State University, Huntsville,TX, in 2003 and 2006 respectively and her Ph.D. degree from The University of Texas at Arlington in 2012, all in Mathematics. From 2003 to 2006 she was a graduate teaching assistant at Sam Houston State University as a lab assistant and instructor. From 2006-2009 and 2011-2012 she was an instructor in the mathematics department as a graduate teaching assistant at UT-Arlington. For 2009-2011 she was a NSF GK-12 fellow at the University of Texas at Arlington.