On Nonassociative Division Rings and Projective Planes

Eric J. Landquist

Thesis submitted to the Faculty of the

Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

Dr. Daniel Farkas, Advisor

Dr. Ezra Brown

Dr. Edward Green

May 18, 2000

Blacksburg, VA

Keywords: Nonassociative, Division Rings, Semifields, Projective Planes

On Nonassociative Division Rings and Projective Planes

Eric Landquist

(ABSTRACT)

An interesting thing happens when one begins with the axioms of a field, but does not require the associative and commutative properties. The resulting nonassociative division ring is referred to as a "semifield" in this paper. Semifields have intimate ties to finite projective planes. In short, a finite projective plane with certain restrictions gives rise to a semifield, and, in turn, a finite semifield can be used via a coordinate construction, to build a special finite projective plane. It is also shown that two finite semifields provide a coordinate system for isomorphic projective planes if and only if the semifields are isotopic, where isotopy is a relationship similar to but weaker than isomorphism.

Before we prove those results, we explore the nature of isotopy to get a little better feel for the concept. For example, we look at isotopy for associative algebras. We will also examine a particular family of semifields and gather concrete information about solutions to linear equations and isomorphisms.

Contents

1 Introduction

The purpose of this paper is to combine an introduction to the theory of finite nonassociative division rings and projective planes with a little exploration of some specific examples. The hope is to obtain some idea of the structure for these objects and to produce some new observations about them. Recall that the associative property states that if a, b, and c are elements of some set with a binary operation such as multiplication, then $a(bc) = (ab)c$. That is, one can associate the multiplication of any number of elements and be guaranteed to have the same result. From this point on, we cannot assume that this property holds for multiplication, unless we are dealing with a field. The objects we will be focused on for the majority of the paper are called *semifields*, and more specifically, finite semifields. We will give a definition at the beginning of the next section, but an equivalent description of a semifield is that it is a nonassociative division ring, a ring such that linear equations in one variable can be solved. This implies that nonzero elements have multiplicative inverses but, in the absence of associativity, is much stronger.

Once we have discussed finite semifields, we will show some relationships to what are called finite *projective planes*. A projective plane is a like a graph in that it contains points, but unlike a graph, it possesses lines that contain a given number of points instead of edges which only connect two points. Projective planes possess more axioms in their definition, which will be given in the next section, but for now the hope is to give a little taste of what to expect. The two main relationships between finite semifields and finite projective planes is that they can be used to construct each other and that two isomorphic projective planes are constructed by semifields that possess a certain property called *isotopy*. So if we are given a finite semifield, then we can build a finite projective plane. Conversely, if we are given a finite projective plane with restrictions, we can construct a finite semifield. Understanding isotopy is the goal of the third section. We will begin that section by defining isotopy, which is a concept similar to isomorphism, but much weaker. From the definition, we will flesh out the concept some more to get a little better understanding of what it is that isotopy does, and then will show how isotopy relates finite semifields and finite projective planes.

In the fourth and last section of this paper, we will examine a family of semifields discovered by L.E. Dickson in 1906. Specifically, we find isomorphisms of these semifields and also compute solutions to linear equations explicitly.

This subject was first studied by both Dickson and Wedderburn in the early 1900's at the same time they analyzed associative fields. Dickson's main contribution was the construction of the first semifields that were not fields themselves. Then one of Dickson's students, A. Adrian Albert made further contributions to the subject, determining conditions under which semifields are Galois fields and discovering a large class of finite semifields. At some point in the middle of the 1900's, the connection between finite projective planes and semifields was finalized, providing a new motivation for study of the subject. In this context, Albert invented the notion of isotopy and proved the theorem that two semifields *coordinatize* isomorphic projective planes if and only if they are isotopic. Since then, efforts have been made to classify semifields and also to find out how many isomorphism and isotopism classes of semifields exist for given orders. The first results on enumerating semifields of order 16 were done on computer by Erwin Kleinfeld in 1960. In 1977 Kaplansky and Menichetti confirmed the number of semifields which are algebras of degree three over finite fields. As of now, it is not known if all semifields of a given order have been found, or if we are anywhere close to a classification of finite semifields.

We will see that semifields are difficult to work with, but are fascinating. Semifields are a relatively unresearched topic; it does not appear that much has been done in recent years, so new discoveries in this area may be just on the horizon. One reason for reviving the topic today links to another hot research area altogether. Finite semifields are similar to finite fields in many ways, so it is likely that cryptography is an application of finite semifields. It is well known that finite fields play a very significant role in modern cryptography, so by throwing in the added complexity of nonassociativity, resulting cryptosystems may be more difficult to break. While this paper is not focused on developing nonassociative cryptography, it is a motivating factor.

The body of this essay contains three types of contributions. We verify comments in the literature by providing more complete arguments. We also present theorems which are new to us although there is some evidence that similar results are in papers which are not accessible. Finally, some of the mathematics presented here is original.

With that introduction and motivation into this topic, we begin with semifields.

2 Semifields and Projective Planes

An interesting thing happens when one begins with the axioms of a field, but leaves out the associative and commutative properties. Such an object we will call a $semifield$.

Definition 2.1 *A finite* **semifield** *is a finite set containing at least two elements with two binary operations, multiplication, and addition satisfying the following four axioms:*

1. *The semifield is a group under addition, with identity 0.*
2. *0 is the only zero divisor.*
3. *The distributive properties hold.*
4. *There exists a multiplicative identity, 1.*

An observation from this definition is that any finite field is a semifield. We will mostly be concerned with finite semifields that are not fields, so-called *proper semifields*. A semifield is also a special case of what we call an *algebra*, as we shall see in Theorem 1.2.

Definition 2.2 *An* **algebra** *A is both a (not necessarily associative) ring and a vector space over a field F so that for all $a, b \in A$ and $\alpha \in F$:*

$$(\alpha a)b = \alpha(ab) = a(\alpha b).$$

Therefore we are guaranteed some associativity when multiplying three elements of an algebra if one of the three is in the base field. However, we will be working in the case where general associativity is not guaranteed. We call such algebras *nonassociative algebras*.

We will only be concerned with finite semifields in this paper. Axiom 2 must be replaced for an infinite semifield with the stronger condition that if $a, c \neq 0$ are elements of a semifield, then $ax = b$ and $yc = d$ are uniquely solvable for x and y. To quickly see why these two definitions are equivalent in the finite case, we show that in any finite semifield these equations can be solved. Let R be such a ring, suppose $a \in R$ is nonzero, and let $\theta : R \to R$ be the function defined by $\theta(x) = ax$. θ is one-to-one because if there were $x, y \in R$ such that $ax = ay$, then $a(x - y) = 0$. Since R has no zero divisors, then either $a = 0$ or $x = y$. Since R is finite, θ is onto, making θ a bijection. Therefore if $b \in R$, then there must be a unique $t \in R$ such that $\theta(t) = b$. Thus t is the unique solution to $ax = b$. Similarly, we let $\phi : R \to R$ be the function defined by $\phi(y) = yc$. We see that, like θ, ϕ is one-to-one and onto. Therefore if $d \in R$ then there exists a unique $u \in R$ such that $uc = d$. Thus we see that u is the unique solution to $yc = d$.

Example 2.1 *A finite proper semifield.*

The following is one example of a proper semifield with 16 elements. The addition is familiar, but the definition of multiplication is quite strange. This case is typical of most constructions of semifields in that it begins with a finite field, but a different multiplication is defined on the semifield to make it nonassociative. Let $V = \{(a,b)|a,b \in GF(4)\}$, where $GF(4)$ is the unique field with four elements: $\{0, 1, \omega, \omega^2 = \omega + 1\}$. As a side note, V is an algebra over $GF(4)$ with basis $\{(0,1),(1,0)\}$. Define addition coordinate-wise:

$$(u,v) + (x,y) = (u + x, v + y),$$

but define multiplication by:

$$(u,v)(x,y) = (ux + v^2y, vx + u^2y + v^2y^2).$$

If $v, y = 0$, then we are simply multiplying elements u and x of the field $GF(4)$, so

$$(u,0)(x,0) = (ux,0).$$

Knuth [9] notes that V is indeed a proper semifield, with additive identity $(0,0)$, multiplicative identity $(1,0)$, the distributive property, and no zero divisors. It is not commutative but does have a great deal of associativity since $(ab)c = a(bc)$ if any two of a, b, c are elements of $GF(4)$.

We provide a quick proof of these claims.

Theorem 2.1 *V as described above is a proper semifield.*

Proof: The first axiom holds because V is any ordinary vector space with scalar field $GF(4)$. Now to show that the second axiom is true suppose that $(u,v)(x,y) = 0$. Then $(ux + v^2y, vx + u^2y + v^2y^2) = 0$. Thus

$$ux + v^2y = 0$$

and

$$vx + u^2y + v^2y^2 = 0.$$

Suppose that $(x,y) \neq (0,0)$. If $x = 0$ and $y \neq 0$, then

$$v^2y = 0$$

and

$$u^2y + v^2y^2 = 0,$$

so $v^2 = 0$ and thus $v = 0$. From this it is true that $u^2y = 0$ so $u = 0$. Therefore $(u,v) = (0,0)$.

Now suppose that $x \neq 0$. Then

$$u = -v^2yx^{-1}$$

and

$$vx + v^4y^3x^{-2} + v^2y^2 = 0$$

$$\Rightarrow vx^3 + v^4y^3 + v^2y^2x^2 = 0.$$

It is immediately clear that if $v = 0$, then $u = 0$, and we would have $(u, v) = (0, 0)$ as a factor, so let $v \neq 0$. Then:

$$x^3 + v^3y^3 + vy^2x = 0.$$

To simplify things, note that the cube of any nonzero element of $GF(4)$ is 1, so

$$1 + 1 + vy^2x = vy^2x = 0.$$

We have assumed that $v, x \neq 0$, so the only possibility is that $y = 0$. However, we just saw that $x^3 + v^3y^3 + vy^2x = 0$, so if $y = 0$, then $x^3 = 0$. Therefore $x = 0$, a contradiction. So we must have $(u, v) = (0, 0)$ as a factor. Therefore this construction does not have any nonzero zero divisors.

Now we show that the distributive property holds. We evaluate $(u, v)((w, x) + (y, z))$.

$$\begin{aligned}(u, v)(w + y, x + z) &= (u(w + y) + v^2(x + z), v(w + y) + u^2(x + z) + v^2(x + z)^2)\\ &= (uw + v^2x + uy + v^2z, vw + u^2x + v^2x^2 + vy + u^2z + v^2z^2)\\ &= (u, v)(w, x) + (u, v)(y, z).\end{aligned}$$

Similarly, the right distributive property holds.

To complete the proof that the construction is a semifield, we see by inspection that (1, 0) is the multiplicative identity.

Lastly, we show that the construction is proper with an example.

$$(\omega, 0)((1, \omega)(\omega, 1)) = (\omega, 0)(1, 1) = (\omega, \omega + 1)$$

$$((\omega, 0)(1, \omega))(\omega, 1) = (\omega, 1)(\omega, 1) = (\omega, 0).$$

We have proved that V is a proper semifield. *QED*.

Now we also made the claim that associativity holds if two of the three elements being multiplied together are elements of the base field, $GF(4)$. We saw in the example given in the proof that if one of the three elements is in the base field, then associativity does not hold in general. Clearly, if all three were in the field, then multiplication would be associative. So what if we have two elements of the field? $(u, 0)((v, 0)(x, y)) = (u, 0)(vx, v^2y) = (uvx, u^2v^2y)$. And on the other end we have $((u, 0)(v, 0))(x, y) = (uv, 0)(x, y) = (uvx, u^2v^2y)$. So the two are equal. Similar checks will show that the other two cases: $(u, 0)((x, y)(v, 0)) = ((u, 0)(x, y))(v, 0)$ and $(x, y)((u, 0)(v, 0)) = ((x, y)(u, 0))(v, 0)$ hold. Therefore multiplication of three elements is associative if at least two of the elements are elements of the base field.

There are several other interesting questions to pursue with regard to there being a lack of associativity in general. For example, if x is an element of a proper semifield, can we define x^n? Clearly x^2 is well defined, but when we move on to x^3, there are two ways of grouping the terms, and for x^4 there are five. But do all these groupings yield the same value, a small set of values, or every nonzero element of the semifield? It turns out that we cannot guarantee associativity even in the case x^3.

Example 2.2 *Powers need not be associative in a proper semifield.*

If $(\omega, 1) \in V$, the proper semifield defined above, is $(\omega, 1)^2(\omega, 1) = (\omega, 1)(\omega, 1)^2$?

$$((\omega, 1)(\omega, 1))(\omega, 1) = (\omega, 0)(\omega, 1) = (\omega + 1, \omega + 1)$$

$$(\omega,1)((\omega,1)(\omega,1)) = (\omega,1)(\omega,0) = (\omega+1,\omega)$$

The answer is "no."

If we define x^i recursively by $x^1 = x$ and $x^{i+1} = xx^i$, then we say that a semifield S is *power associative* when $x^i x^j = x^{i+j}$ for all $x \in S$. Albert [1] showed that finite power associative semifields are always fields. Another question for consideration following from the existence of x^n is the existence of a primitive element for the semifield. By this we mean an element of the semifield that generates all nonzero elements of the semifield. Wene [12] has conjectured that there exists such a left (and right) primitive element for every semifield, and has proven that left primitive elements exist for all semifields of dimension $2n$, with $n \geq 3$, over $GF(p^m)$. A left primitive element would be one such that the nonzero elements of a semifield are powers of a generator with powers defined above. A right primitive element, then, has its powers constructed by $x^{i+1} = x^i x$. Such questions are intriguing, and important if we are to apply such systems to cryptography.

Getting back to our example, we had a proper semifield of order $16 = 2^4$. We know that all fields must have order p^m for some prime p and integer m. It turns out the same is true for semifields.

Theorem 2.2 *All finite semifields have order p^m, for some prime p and integer m. Indeed, a finite semifield S is an algebra over some field $GF(p)$.*

Proof: Let R be the finite additive cyclic group generated by 1 in the semifield S:

$$R = \{1, 1+1, ..., 1+1+...+1\}.$$

Since $R \subseteq S$, R has no nonzero zero divisors. It is also clear from its additive structure that R is commutative. We show that $\lambda(\mu s) = (\lambda\mu)s$ for all $\lambda, \mu \in R$ and $s \in S$. We proceed first by induction on λ then by induction on μ. First $1(1 \cdot s) = s = (1 \cdot 1)s$. Now suppose that for some number k that $(1+...+1)(1 \cdot s) = ((1+...+1) \cdot 1)s$, where we have a sum of k 1's in the parentheses. We add s to both sides and see that $(1+...+1+1)(1 \cdot s) = ((1+...+1+1 \cdot 1)s$ because of the distributive properties of S and because $1 \cdot s = s$. This yields $k+1$ 1's grouped in the parentheses. Now with that being the base case for induction on μ, suppose that $(1+...+1)((1+...+1) \cdot s) = ((1+...+1) \cdot (1+...+1)) \cdot s$, where there are l 1's in the second grouping of parentheses, and k in the first. Now if we add $s + ... + s$ to both sides, where there are k s's being added we get:

$$(1+...+1)((1+...+1) \cdot s) + s + ... + s = (((1+...+1) \cdot (1+...+1)) \cdot s) + s + ... + s$$

$$(1+...+1)((1+...+1) \cdot s) + (1+...+1) \cdot s = (((1+...+1) \cdot (1+...+1)) \cdot s) + (1+...+1) \cdot s$$

$$(1+...+1)((1+...+1) \cdot s + s) = (((1+...+1) \cdot (1+...+1)) + (1+...+1)) \cdot s$$

$$(1+...+1)((1+...+1+1) \cdot s) = (((1+...+1) \cdot (1+...+1+1)) \cdot s).$$

So the condition holds for $l+1$ 1's in the second set of parentheses. Since R is a finite domain, it is a field, so it follows that S is a vector space over R. A similar argument shows that S is an algebra over R. It is clear that R has prime order; otherwise there would exist nonzero elements of R such that $(1+...+1)(1+...+1) = 0$, contradicting the fact that R is a field. So R has prime order p and S has order p^m, where m is the cardinality of the basis of S over R, *QED*.

So what is the reason for working with semifields? It turns out that there is a nice link between semifields and *projective planes*.

Definition 2.3 *A* **projective plane** *is a set of points and lines and a relation "incident to" satisfying the following axioms:*

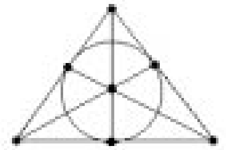
1. *Every pair of distinct lines intersects at a unique point, that is, they are incident to a unique point.*

2. *Every pair of distinct points is incident to a unique line.*

3. *There exist four points such that no three are incident to the same line.*

The most basic of all projective planes is the Fano Plane.

Example 2.3 *The Fano Plane*



The Fano Plane has seven distinct points, represented by "·", and seven distinct lines, including the circle inscribed in the plane. Notice that each line contains three distinct points and each point is incident to three distinct lines.

It turns out that the Fano Plane can be *coordinatized* by the simplest of all semifields, the field of two elements: $\{0,\ 1\}$. That is one of the links between semifields and projective planes. Semifields give rise to projective planes. This observation will be the subject of the remainder of this section, and will lead to another connection to be studied in the next section. However, a more general construction, called a *ternary ring* must be used to coordinatize a projective plane.

Definition 2.4 *A* **loop** *is a set L with a binary operation satisfying two conditions. First, if $a, b, c \in L$ and $ab = c$, then any two of a, b, c will determine the third uniquely. The second condition is that L has a two-sided identity element for the operation.*

Definition 2.5 *A* **ternary ring** *is a set S and a ternary operation $x \cdot m \circ b : (S, S, S) \to S$ such that the following six axioms hold:*

1. *There is a unique element $1 \in S$ such that the system consisting of the set S and the binary operation "addition" defined by $a + b = 1 \cdot a \circ b$ is a loop with identity $0 \neq 1$.*

2. $0 \cdot m \circ b = x \cdot 0 \circ b = b$ *for every $m, x, b \in S$.*

3. *$S \setminus \{0\}$ under the binary operation "multiplication" defined by $xm = x \cdot m \circ 0$ is a loop with identity 1.*

4. *Given $a, m, c \in S$, there exists exactly one $z \in S$ such that $a \cdot m \circ z = c$.*

5. *If $m_1 \neq m_2$, the equation $x \cdot m_1 \circ a = x \cdot m_2 \circ b$ has a unique solution $x \in S$ for every $a, b \in S$.*

6. *If $x_1 \neq x_2$ and $y_1 \neq y_2$, then the equations $y_1 = x_1 \cdot m \circ b, y_2 = x_2 \cdot m \circ b$ are uniquely solvable for $m, b \in S$.*

By this definition, any semifield is a ternary ring by setting $x \cdot m \circ b = xm + b$.

One introduces a coordinate system for projective planes called *homogeneous coordinates*; we shall follow Knuth [9] for our notation. Each point is denoted $(0, 0, 1), (0, 1, a)$, or $(1, a, b)$, where a and b are elements of some set S, and each line is similarly denoted $[0, 0, 1], [0, 1, a]$, or $[1, a, b]$. It is very important to note that $(0, 0, 0)$ is not a legal point and $[0, 0, 0]$ is not a legal line. The idea is to define a ternary operation so that a point (x_1, x_2, x_3) is incident to a line $[y_1, y_2, y_3]$ if and only if

$$y_1 x_3 = x_2 \cdot y_2 \circ x_1 y_3.$$

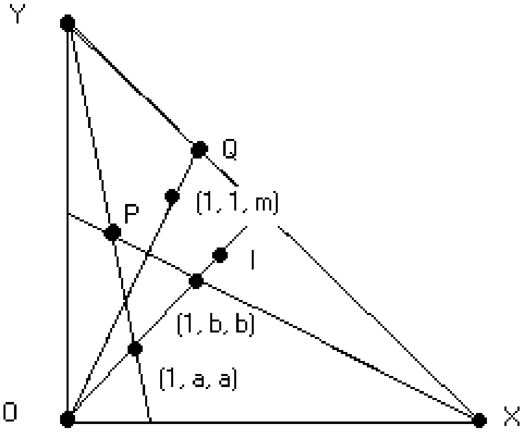
We explain this notation. Recall that x_1 and y_1 are either 0 or 1. Here the juxtaposition $0x_3$ or $0y_3$ is to be interpreted as 0 and $1x_3$ (respectively $1y_3$) means x_3 (respectively y_3). In the case that the ternary ring is a semifield, we will write $y_1 x_3 = x_2 y_2 + x_1 y_3$. We will refer to this relation as the "Knuth equation" or "incidence equation."

Here is some useful notation. If P and Q are two distinct points, then $P : Q$ denotes the unique line incident to both points, and if L and M are two distinct lines, then $L \cap M$ denotes the unique point incident to both of the two lines. Similarly, if a point P is incident to a line L, then we write $P \in L$.

We now have three goals for the remainder of this section. First, given a finite projective plane, we will assign coordinates from a set S to the points and lines. Next, we will show that the set S is endowed with a ternary operation thus making it a ternary ring. That is, the ternary ring will assign coordinates to the projective plane and will possess an algebraic structure to mirror the geometric structure of the projective plane. Extra conditions on the plane will imply that S is a semifield. Our final goal of the section will be to show that semifields give rise to projective planes via homogenous coordinates and Knuth's incidence equation. We show that ternary rings can be constructed out of a projective plane. The result is classical.

Theorem 2.3 *Suppose we have a finite projective plane. Then we can assign each point an ordered triple and each line an ordered triple, with the elements of each triple arising from a ternary ring. In this case geometric incidence coincides with equational incidence under the ternary operation described above.*

Proof: We will show that from the axioms of a projective plane, we can construct a ternary ring with elements in S. To get a clearer idea of exactly what will be going on, we provide the following general picture of a projective plane.



We begin with points, assigning unique coordinates to each point. First choose four distinct points, which we call $X = (0,1,0), Y = (0,0,1), O = (1,0,0)$, and $I = (1,1,1)$ such that no three are collinear. Let (0, 1, 1) be the point at the intersection of OI and XY. For other points on OI assign the coordinates $(1,b,b)$. Let P be a point on the projective plane, but not on the line XY. The line YP will intersect OI at a point $(1,a,a)$, and XP will intersect OI at some point $(1,b,b)$. Assign the coordinate $(1,a,b)$ to P. This gives the coordinate for all points of the form $(1,x_2,x_3)$. Now we will assign all points on XY the form $(0,x_2,x_3)$. Suppose XY intersects $O:(1,1,m)$ at a point Q. Assign the value $(0,1,m)$ to Q. We have now completed assigning coordinates to the points.

We now assign coordinates to the lines. Each line will have homogeneous coordinates and we will define an equation to describe the line in the form $y = m \cdot x \circ b$, which is similar to that seen in Euclidean geometry, with the exception of a *line at infinity.* The equation form of lines will help to give insight into the feel of projective planes, but on a mathematical level, will bridge the gap from the geometry of a projective plane to the algebra of a ternary ring. Let $XY = [0,0,1]$ be the line at infinity and $OI = [1,1,0]$ be the line $y = x$. Let $[1,1,b]$ be the line joining $(0,1,1)$ and $(1,0,b)$. If $(1,x,y)$ is a point on this line, then we define the binary operation of addition by $y = x + b$. If $a \in S$, then the line joining $(0,1,1)$ and $(1,0,a)$ is $[1,1,a]$. If $(1,a',0)$ is a point on this line for some $a' \in S$, then $0 = a' + a$ by our definition of addition. Think of a' as the additive inverse of a, and write $a' = -a$. A line distinct from XY through Y and $(1,a,1)$ will be assigned $[0,1,-a]$, and is also described $x = a$. The line joining $O = (1,0,0)$ and $(0,1,m)$ will be $[1,m,0]$. If $(1,x,y)$ is a point on this line, then we define the binary operation of multiplication by $y = xm$. Lastly, every line that intersects XY in some point $(0,1,m)$ and intersects OY in some point $(1,0,b)$ will have the coordinate $[1,m,b]$. If $(1,x,y)$ is a point on this line, then we define the ternary operation via $y = x \cdot m \circ b$. So now we have assigned every line a unique coordinate and produced a ternary operation.

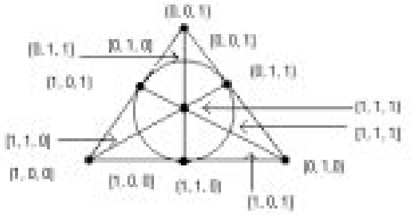
We now show that the operation we gave satisfies the axioms for a ternary ring. First observe that $x + b = x \cdot 1 \circ b$ and $xm = x \cdot m \circ 0$. So from this, it is clear that we have an additive identity 0 and multiplicative identity 1, so axioms 2 and 3 follow immediately. The fourth axiom says that the lines joining $(0,1,m)$ and $(1,a,c)$ intersect in a unique point $(1,0,z)$. The fifth says that two lines $[1,m_1,b_1]$ and $[1,m_2,b_2]$ with $m_1 \neq m_2$ intersect in a unique finite point. The last says that if $(1,x_1,y_1)$ and $(1,x_2,y_2)$ are two points such that $x_1 \neq x_2$, then there is a unique line of the form

$y = x \cdot m \circ b$ to which they are incident. The first axiom is the condition that addition is a loop with 0 as the identity. We have established that 0 is the identity and is different than the multiplicative identity. The fact that addition is a loop then follows from the definition of addition: $y = x + b$ if $(1, x, y) \in [1, 1, b]$, so if any two of y, x, and b are chosen, then the third is uniquely determined. Therefore we have constructed a ternary ring.

To show that geometric incidence coincides with equational incidence, we will look at all the possible incidences. First, the line $[0, 0, 1]$ was said to contain the points $(0, 0, 1)$ and $(0, 1, m)$, and were defined to be on the line. According to the Knuth equation, $(0, 0, 1), (0, 1, m) \in [0, 0, 1]$ if and only if $(0)(1) = 0 \cdot 0 \circ (0)(1)$ and $(0)(1) = 0 \cdot 0 \circ (0)(m)$, respectively. It is obvious that both equations reduce to $0 = 0$. Lines of the form $[0, 1, -a]$ were said to contain $(0, 0, 1)$ and all points of the form $(1, a, b)$. The line $[0, 1, -a]$ is also described $x = a$ and includees the point $(0, 0, 1)$ by definition. Points of the form $(1, a, b)$ can be thought of as having "x-coordinate" a and "y-coordinate" b. Therefore $(1, a, b)$ is certainly on the line $x = a$. By Knuth's equation, $(0, 0, 1) \in [0, 1, -a]$ if and only if $(0)(1) = 0 \cdot 1 \circ (0)(-a)$, which clearly reduces to $0 = 0$. Now we also see that $(1, a, b) \in [0, 1, -a]$ if and only if $(0)(b) = a \cdot 1 \circ 1(-a)$ which reduces to $0 = a + (-a)$ by the ternary operation. Lastly lines of the form $[1, m, b]$ contain points of the form $(0, 1, m)$ and $(1, x, x \cdot m \circ b)$, with the point $(0, 1, m)$ being defined to be on the line $[1, m, b]$. The equation form of the line $[1, m, b]$ is $y = x \cdot m \circ b$, so if we think of the point $(1, x, x \cdot m \circ b)$ as having the "x-coordinate" x and "y-coordinate" $x \cdot m \circ b$, then it makes sense to see why $(1, x, x \cdot m \circ b) \in [1, m, b]$. In this latter case, Knuth's equation is identical. First $(0, 1, m) \in [1, m, b]$ if and only if $(1)(m) = 1 \cdot m \circ (0)(b)$, which is equivalent to $m = m$ under the ternary operation. Lastly, For $(1, x, x \cdot m \circ b) \in [1, m, b]$, the ternary operation says that $x \cdot m \circ b = x \cdot m \circ b$, mirroring the earlier equation we gave. So $(1, x, x \cdot m \circ b) \in [1, m, b]$. Therefore all possible incidences hold and the coordinate system the projective plane determines satisfies all equational and geometric incidence properties, *QED*.

To give an example of how a semifield coordinatizes a projective plane, this is how one would coordinatize the Fano Plane with the semifield {0, 1}.

Example 2.4 *Coordinatization of the Fano Plane*



To see how we arrive at this coordinatization we will follow the steps outlined in the proof above. We first choose four noncollinear points as O, X, Y, and I. $Y = (0, 0, 1)$ is the top vertex, $X = (0, 1, 0)$ is the bottom right vertex, $O = (1, 0, 0)$ is the bottom left vertex, and $I = (1, 1, 1)$ is the vertex in the center. We assign $(0, 1, 1)$ to the point at the intersection of OI and XY. Two more points are left to be assigned, and the coordinates for these are $(1, 0, 1)$ and $(1, 1, 0)$. We will assign a coordinate for the middle point on the line OY. The line $YP = OY$ intersects OI at the point $O = (1, 0, 0)$, and the line XP intersects OI at the point $I = (1, 1, 1)$, so by the algorithm given in the proof, we assign the value $(1, 0, 1)$ to the point in question. Therefore the last point must have the coordinate $(1, 1, 0)$.

To assign coordinates to the lines, we first assign $XY = [0, 0, 1]$ and $OI = [1, 1, 0]$. In the proof above, the next line we assign a coordinate to is $[1, 1, 1]$, the circular line connecting $(0, 1, 1)$ to $(1, 0, 1)$. Since we are dealing with a characteristic 2 field for the coordinatization, the vertical line through $(0, 0, 1)$ and $(1, 1, 1)$ is assigned $[0, 1, 1]$. Likewise, the line OY is assigned the coordinate $[0, 1, 0]$. In the next step, we can assign $[1, 0, 0]$ to the line connecting $(1, 0, 0)$ and $(0, 1, 0)$. The last line intersects XY at $(0, 1, 0)$ and intersects OY at $(1, 0, 1)$, and is thus given the coordinate $[1, 0, 1]$. This completes the assignment of coordinates for the entire Fano Plane.

Ternary rings are the most general objects that coordinatize projective planes. So we ask what sort of conditions must a ternary ring meet in order to be a semifield and what conditions must a projective plane meet in order to be coordinatized by a semifield? We answer these questions and then prove a partial converse of Theorem 2.3, that semifields can be used to construct a projective plane.

Note that the additive structue of a semifield is a group, whereas in a ternary ring it is just a loop. Also both distributive properties must hold in a semifield. These two extra conditions on a ternary ring will make it a semifield.

To find out which projective planes are coordinatized by a semifield, we must first define some terms. We first note that as for mathematical structure, we can create maps and isomorphisms from one projective plane to another.

Definition 2.6 *If π and π' are projective planes and if $\alpha : \pi \longrightarrow \pi'$ is a pair of one-to-one correspondences on points and lines, then α is called an* **isomorphism** *when it preserves incidence. In the case that $\pi = \pi'$, we say α is a* **collineation**.

For example, the map that rotates the Fano Plane is a collineation. This collineation fixes the point $(1, 1, 1)$ and the line $[1, 1, 1]$, and maps the points $(0, 0, 1)$ to $(1, 0, 0)$ and $(1, 0, 0)$ to $(0, 1, 0)$.

The set of collineations of a projective plane forms a group under the operation of composition. We single out some special collineations.

Definition 2.7 *A collineation α is a P-L* **central collineation** *provided α fixes every point on the line L and stabilizes all lines through the point P. (Notice that α fixes the point P.)*

The collineation of the Fano Plane we just gave does not fit this definition. Any identity collineation is a P-L central collineation for all points P and lines L. In the Fano Plane, if we map the lines $[1, 1, 0]$ to $[1, 0, 0]$ and $[1, 0, 0]$ to $[1, 1, 0]$ and the points $(1, 1, 1)$ to $(1, 1, 0)$ to $(1, 1, 1)$ and $(0, 1, 1)$ to $(0, 1, 0)$ to $(0, 1, 1)$, then every line through $(0, 0, 1)$ is stabilized, even though not every point on those lines are fixed, and every point on the line $[1, 0, 1]$ is fixed. Therefore the collineation we have described is a $(0, 0, 1)$-$[1, 0, 1]$ central collineation.

Definition 2.8 *A projective plane is C-L-***transitive** *provided that for every point P other than C and not on L, and for every point Q on the line CP, also distinct from C and not on L, there is a C-L central collineation sending P to Q.*

In other words, if π is a P-L-transitive projective plane, then there exists a P-L central collineation, α, of π such that for distinct points P and Q of π where $P, Q \neq C$, $P, Q \notin L$, and $Q \in CP$ we have $\alpha(P) = Q$. For example, the Fano Plane is $(0, 0, 1)$-$[1, 0, 1]$-transitive by the construction of the central collineation. That is, the $(0, 0, 1)$-$[1, 0, 1]$ central collineation we defined is the only such collineation on the Fano Plane, and for any choice of P as given in the definition, there is exactly one possible Q to choose, and this collineation is defined to map P to Q and Q to P.

We note that if α is a P-L central collineation and P is given, then $\alpha(P)$ must lie on CP because α stabilizes all lines through P. If all points on CP arise this way, then the plane is P-L-transitive.

We will state the necessary and sufficient conditions for a projective plane to be coordinatized by a semifield in two steps. The reader is referred to Hall [5] for the proofs.

Theorem 2.4 *A projective plane π is P-L-transitive for a choice of a line L and a point $P \in L$ if and only if in the coordinatizing ternary ring S satisfies $a \cdot m \circ b = am + b$ and S is a group under addition.*

Theorem 2.5 *A plane is coordinatized by a semifield if and only if there are distinct points E and F such that the plane is P-L-transitive for $L = E : F$ and all points $P \in E : F$, and for $P = F$ and all lines L through F.*

This completes the determination of all projective planes that are coordinatized by a semifield. We will use this result again in Chapter 3 when we discuss isotopies of semifields and how they relate to isomorphisms of projective planes. Now we find a condition that shows when a plane is coordinatized by a nonassociative division ring. The following theorem is due to Albert [1].

Theorem 2.6 *Assume that the plane satisfies those conditions which make its coordinatizing ternary ring a semifield. There exists a line L and a point P not on L such that the plane is P-L-transitive if and only if the ternary ring is an associative division ring.*

Recall that we showed that the Fano Plane, which is coordinatized by $GF(2)$, is $(0, 0, 1)$-$[1, 0, 1]$-transitive. $(0, 0, 1) \notin [1, 0, 1]$ and $GF(2)$ is certainly an associative field.

Now we can prove a partial converse to Theorem 2.3.

Theorem 2.7 *Let S be a semifield and consider ordered triples (x_1, x_2, x_3) and $[y_1, y_2, y_3]$ with the first nonzero coordinate equal to 1. If "incident to" is determined by the Knuth equation, then "point" (x_1, x_2, x_3) and "line" $[y_1, y_2, y_3]$ describe a projective plane.*

Proof: There are three axioms in the definition of a projective plane: any two lines intersect in exactly one point, any two points determine exactly one line, and there exist four noncollinear points. We know the third axiom is met by the points (0, 0, 1), (0, 1, 0), (1, 0, 0), and (1, 1, 1), since 0 and 1 are elements of every semifield and the incidence relations above tell us that no three of these are collinear. Now we prove the first axiom, that a pair of distinct lines determines a unique point. Suppose that there exist two lines $[y_1, y_2, y_3]$ and $[y_4, y_5, y_6]$ that intersect in two points (x_1, x_2, x_3) and (x_4, x_5, x_6). Then both of those points must be on both lines, so the following four equations hold:

$$y_1x_3 = x_2y_2 + x_1y_3$$

$$y_4x_3 = x_2y_5 + x_1y_6$$

$$y_1x_6 = x_5y_2 + x_4y_3$$

$$y_4x_6 = x_5y_5 + x_4y_6.$$

From here on, we will consider several cases.

Case 1: $y_1 = y_4 = 0$

Then each of y_2, y_5 must either be 0 or 1, but both cannot be 0, otherwise both will be the line [0, 0, 1]. So if one line is [0, 0, 1], then, without loss of generality, we have the equations:

$$0 = x_2 + x_1y_3$$
$$0 = x_5 + x_4y_3$$
$$0 = x_1 = x_4.$$

Since $x_1 = x_4 = 0$ then $x_2 = x_5 = 0$, so $x_3 = x_6 = 1$, and both points are the same, a contradiction. Now if neither line is [0, 0, 1], then we have the following equations:

$$0 = x_2 + x_1y_3$$
$$0 = x_5 + x_4y_3$$
$$0 = x_2 + x_1y_6$$
$$0 = x_5 + x_4y_6.$$

Since both lines are distinct, $y_3 \neq y_6$, and $0 = x_2 + x_1y_3 = x_2 + x_1y_6$, which means that $x_1 = x_2 = 0$ and $x_4 = x_5 = 0$, thus requiring $x_3 = x_6 = 1$, which is a contradiction.

Case 2: $y_1 = 0, y_4 = 1$ (or vice versa, without loss of generality)

Since $y_1 = 0$, $y_2 = 0, 1$. Suppose $y_2 = 0$. This situation gives the equations:

$$0 = x_1y_3$$
$$0 = x_4y_3$$
$$x_3 = x_2y_5 + x_1y_6$$
$$x_6 = x_5y_5 + x_4y_6.$$

Since there are no zero divisors in a semifield, and since we cannot have the point (0, 0, 0), $x_1 = x_4 = 0$, so the bottom two equations are now

$$x_3 = x_2y_5$$
$$x_6 = x_5y_5.$$

Since $x_1 = x_4 = 0$, $x_2, x_5 = 0, 1$. Neither can be 0, since it would force a point to be (0, 0, 0), so $x_2 = x_5 = 1$, which now forces $x_3 = x_6 = y_5$, so both points are the same, a contradiction.

Case 3: $y_1 = y_4 = 1$

The final case gives the following equations:

$$x_3 = x_2y_2 + x_1y_3$$
$$x_3 = x_2y_5 + x_1y_6$$
$$x_6 = x_5y_2 + x_4y_3$$
$$x_6 = x_5y_5 + x_4y_6.$$

There are several cases for this, since $x_1, x_4 = 0, 1$.

Case 3a: $x_1 = x_4 = 0$

If both x_1 and x_4 are 0, then $x_2, x_5 = 0, 1$. However, neither can be 0, otherwise the corresponding point will be (0, 0, 0), so $x_2 = x_5 = 1$. Therefore:

$$x_3 = y_2 = y_5 = x_6.$$

So both points will have to be the same.

Case 3b: $x_1 = 0, x_4 = 1$ (or vice versa)

Again, $x_2 \neq 0$, so for our four equations, we have:

$$x_3 = y_2$$

$$x_3 = y_5$$

$$x_6 = x_5y_2 + y_3$$

$$x_6 = x_5y_5 + y_6.$$

So we see that this forces $y_2 = y_5$, and subsequently for $y_3 = y_6$, so both lines are the same, which is a contradiction. Now finally the last case of the last case.

Case 3c: $x_1 = x_4 = 1$

Now we have:

$$x_3 = x_2y_2 + y_3$$

$$x_3 = x_2y_5 + y_6$$

$$x_6 = x_5y_2 + y_3$$

$$x_6 = x_5y_5 + y_6.$$

If $x_2 = x_5$, then the top two equations tell us that $x_3 = x_6$, so $x_2 \neq x_5$. We also can see from either the left two or the right two equations that if $y_2 = y_5$, then $y_3 = y_6$, so we also know that $y_2 \neq y_5$. If we solve for y_3 and y_6 in one equation and plug into another we obtain:

$$\begin{aligned} x_6 &= x_5y_2 + x_3 - x_2y_2 \\ &= x_5y_5 + x_3 - x_2y_5 \\ &\Rightarrow (x_5 - x_2)y_2 = (x_5 - x_2)y_5. \end{aligned}$$

So either $x_2 = x_5$ or $y_2 = y_5$, which is a contradiction.

This completes all the cases. We know that there is a unique point anytime two lines intersect from this, and in every case we had, there did exist a point at the intersection of any two lines, so this has proven that homogeneous coordinates do satisfy the first axiom of projective planes.

For the second axiom, consider the case if two distinct points do not determine a unique line, that is, they determine more than one line. Then two distinct lines would intersect in more than one point, a contradiction of the first axiom. Now suppose that two distinct points did not determine a line, then there would be no solution $[y_1, y_2, y_3]$ to the equations:

$$y_1x_3 = x_2y_2 + x_1y_3$$

$$y_6x_3 = x_5y_2 + x_4y_3.$$

If $y_1 = 0$, then clearly we can find a trivial solution [0, 0, 0], but we find a nontrivial solution by solving the system

$$\begin{cases} 0 = x_2y_2 + x_1y_3 \\ 0 = x_5y_2 + x_4y_3 \end{cases}.$$

If $y_1 = 1$, then we can again solve a system of two equations and find a unique solution for the line. Thus the second axiom for a projective plane is met. All the axioms for a projective plane have been met, which tells us that if we are given a semifield, we can construct a projective plane, *QED*.

Since the projective plane we just constructed is coordinatized by a semifield, it has the properties we mentioned in Theorem 2.5, that the plane is P-L-transitive for a given line L and all points $P \in L$ and for some fixed point P and all lines L through P. To demonstrate part of the theorem, we show that π is $(0, 0, 1)$-$[0, 0, 1]$ transitive. Consider the collineation α that maps the points

$$(x_1, x_2, x_3) \to (x_1, x_2, x_3 + x_1k)$$

and the lines

$$[y_1, y_2, y_3] \to [y_1, y_2, y_3 + y_1k]$$

for some k in the semifield. We will show in Lemma 3.5 that this is a collineation called a translation. We must first show that α fixes every point on $[0, 0, 1]$ and stabilizes every line through $(0, 0, 1)$. Points on $[0, 0, 1]$ are $(0, 0, 1)$ and of the form $(0, 1, x_3)$. Clearly α fixes these points. Similarly, lines through $(0, 0, 1)$ are $[0, 0, 1]$ and those of the form $[0, 1, y_3]$. Again, it is clear from the definition of α that these lines are stabilized. Thus α is a $(0, 0, 1)$-$[0, 0, 1]$ central collineation. We now show that the projective plane π constructed above is $(0, 0, 1)$-$[0, 0, 1]$ transitive. All points not on $[0, 0, 1]$ are of the form $P = (1, x_2, x_3)$. The line $(0, 0, 1) : (1, x_2, x_3) = [0, 1, -x_2]$, and points other than $(0, 0, 1)$ on this line are of the form $(1, x_2, x_4)$ for some x_4 in the coordinatizing semifield. We show that for any $P = (1, x_2, x_3)$, there exists a $(0, 0, 1)$-$[0, 0, 1]$ central collineation sending P to an arbitrary $Q = (1, x_2, x_4)$. Notice that

$$\alpha(1, x_2, x_3) = (1, x_2, x_3 + k).$$

Since the semifield is a group under addition, we let $k = x_4 - x_3$, and so we have successfully mapped P to Q. Thus π is $(0, 0, 1)$-$[0, 0, 1]$ transitive.

Now that we have accomplished the main goals of this section, we will now lead into further properties of projective planes and the semifields that coordinatize them.

3 Isotopy

We often consider two algebras to be the same if they are isomorphic. When dealing with nonassociative algebras, however, we need to extend this concept to the notion of *isotopy* because there is a a greater variety of finite semifields as compared to finite fields. In this section, we will be defining what isotopy is, making some observations, and proving a few theorems to get a little better handle on this complicated subject. Then we will outline a fundamental theorem connecting isotopy with projective planes. But first we must define isotopy.

Definition 3.1 *We say that two algebras, A and A', are* **isotopic** *if there exist invertible linear transformations, P, Q, and R from A' to A, such that if $a, b \in A'$, then $R(a \cdot b) = P(a)Q(b)$. We will denote the isotopy by $(P, Q; R)$. In this case we call A' an* **isotope** *of A.*

We notice from the definition of isotopy that if two semifields are isomorphic, then they are isotopic. If A and B are isomorphic algebras, then for all $a, b \in A$, there is an isomorphism $\theta : A \to B$ such that $\theta(ab) = \theta(a)\theta(b)$. Since θ is an invertible linear transformation, $(\theta, \theta; \theta)$ is an isotopy.

In the definition notice that we say that we call one algebra an isotope of another algebra. However, the following lemma will allow us to say that two algebras are isotopic and say that a particular isotope is in an isotopy class, much like isomorphism.

Lemma 3.1 *Isotopy is an equivalence relation.*

Proof: We will show that that isotopy is reflexive, symmetric, and transitive. First it is clear that isotopy is reflexive because an algebra A is isomorphic to itself, so it must be isotopic to itself. Now to show that isotopy is symmetric, we show that if an algebra A is an isotope of an algebra B, then B is an isotope of A. If A is an isotope of B, then there exist invertible linear transformations, $P, Q, R : A \to B$ such that

$$R(a \cdot b) = P(a)Q(b)$$

for all $a, b \in A$. Since P, Q, and R are invertible and onto, for all $c, d, \in B$ there exist unique elements $a, b \in A$ such that $P(a) = c$ and $Q(b) = d$, so we have:

$$R^{-1}(cb) = P^{-1}(c) \cdot Q^{-1}(d).$$

Therefore $(P^{-1}, Q^{-1}; R^{-1}) : B \to A$ is an isotopy, and B is an isotope of A. Thus isotopy is symmetric.

Next we show that if A is an isotope of B and B is an isotope of C, then A is an isotope of C. If A is an isotope of B, then there exist invertible linear transformations $P, Q, R : A \to B$ such that

$$R(a \cdot b) = P(a)Q(b)$$

for all $a, b \in A$. Similarly, if B is an isotope of C, then there exist invertible linear transformations $S, T, V : B \to C$ such that

$$V(c \cdot d) = S(c)T(d)$$

for all $c, d \in B$. Therefore:

$$\begin{aligned} R(a \cdot b) &= P(a)Q(b) \\ \Rightarrow V(R(a \cdot b)) &= V(P(a)Q(b)) \\ \Rightarrow (VR)(a \cdot b)) &= S(P(a))T(Q(b)) \\ \Rightarrow (VR)(a \cdot b)) &= (SP)(a)(TQ)(b). \end{aligned}$$

Therefore $(SP, TQ; VR) : A \to C$ is an isotopy and A is isotopic to C. So isotopy is an equivalence relation. *QED.*

We also observe that if A and B are two algebras such that A is associative and B is not, then there does not exist an isomorphism between A and B. If there did exist an isomorphism $\theta : A \to B$, then for all $a, b, c \in A$, $\theta((ab)c) = \theta(ab)\theta(c) = (\theta(a)\theta(b))\theta(c)$. However, since A is associative, $\theta((ab)c) = \theta(a(bc)) = \theta(a)\theta(bc) = \theta(a)(\theta(b)\theta(c))$. So $(\theta(a)\theta(b))\theta(c) = \theta(a)(\theta(b)\theta(c))$, which means that B is associative. It will later be shown that for the types of algebras we are concerned with, this means that A and B are nonisotopic as well.

One important result by Albert [2] is the observation that finite-dimensional associative algebras with 1 are isotopic if and only if they are isomorphic. We will give a proof of this claim later.

Isotopy of semifields is a difficult thing to prove; most of the time, computers are used to show whether or not two semifields are isomorphic. As an example, there are 23 nonisomorphic proper semifields of order 16, but only 2 isotopic classes. Each can be represented as a vector space over $GF(4)$, with basis $(1, \lambda)$, but they differ in their definition of multiplication:

$$(a + \lambda b)(c + \lambda d) = (ac + b^2 d) + \lambda(bc + a^2 d + b^2 d^2)$$

and

$$(a + \lambda b)(c + \lambda d) = (ac + \omega b^2 d) + \lambda(bc + a^2 d).$$

Theorem 3.1 *Let A be a semifield and let B be an algebra with 1 isotopic to A. Then B is a semifield.*

Proof: Our goal is to show that the algebra B has solutions to all linear equations. Let $(P, Q; R) : B \rightarrow A$ be an isotopy. The second axiom of a semifield says that we can solve linear equations. We need to show that the equations $ax = b$ and $yc = d$ are uniquely solvable in B for x and y when $a, c \neq 0$. There is a unique solution in A to

$$R(b) = P(a) \cdot X.$$

Then $Q^{-1}(\omega)$ satisfies

$$R(b) = P(a) \cdot Q(Q^{-1}(\omega))$$
$$R(b) = R(a \cdot Q^{-1}(\omega)).$$

Since R is one-to-one,

$$b = a \cdot Q^{-1}(\omega).$$

Similarly, the other case holds. Therefore we can find solutions to linear equations in B, and B is a semifield. *QED*.

As a consequence, we can gain some feeling for why it is so much easier for semifields to be isotopic than isomorphic. Suppose D is a semifield with multiplication "$\cdot$". If $R, S, T : D \rightarrow D$ are any invertible linear transformations we may define a new operation $*$ on D by

$$x * y = R^{-1}(S(x) \cdot T(y)).$$

Then D with multiplication $*$ is almost a semifield isotopic to the original one. (It may lack an identity element for multiplication.) Albert [2] observes that if A is an algebra with 1 which is not associative then there is some algebra isotopic to A which is not isomorphic to A. However, if A is associative, isotopy coincides with isomorphism, as we demonstrate in Theorem 3.3.

Once we have an isotopy, there are instances where we can streamline it in a certain sense using a special kind of isotopy.

Definition 3.2 *Let $(A, \cdot)$ be an algebra over the field K. By a* **principal isotope** *of A we mean A together with a second multiplication $*$ on A such that there is an isotopy of the form $(S, T; I) : (A, \cdot) \rightarrow (A, *)$. In other words,*

$$S(a) * T(c) = a \cdot c$$

for all $a, c, \in A$. We also say that $(A, \cdot)$ is a **principal isotope** *of $(A, *)$.*

Notice that the definition of principal isotopy only allows for two objects to be principally isotopic if they have the same elements, but just different definitions of multiplication. Consequently, two "different" algebras can only be discussed in the concept of principal isotopy after their elements are identified by a bijection. We also show here that principal isotopy, like isotopy, is an equivalence relation, so we are able to say that two algebras are principly isotopic

Lemma 3.2 *Principal isotopy is an equivalence relation.*

Proof: We proceed in a manner like Lemma 3.1. Clearly, an algebra A is principally isotopic to itself. If $(A, \cdot)$ is principally isotopic to $(A, *)$, then $(P, Q; I) : (A, \cdot) \to (A, *)$ is an isotopy, so for all $a, b \in A$,

$$a \cdot b = P(a) * Q(b).$$

Again, since P and Q are invertible and onto, for all $c, d \in (A, *)$ there exist unique $a, b \in (A, \cdot)$ such that $a = P^{-1}(c)$ and $b = Q^{-1}(d)$. So

$$P^{-1}(c) \cdot Q^{-1}(d) = c * d.$$

Therefore $(P^{-1}, Q^{-1}; I) : (A, *) \to (A, \cdot)$ is a principal isotopy and $(A, *)$ is principally isotopic to $(A, \cdot)$. Thus principal isotopy is symmetric.

Lastly we show that principal isotopy is transitive. If $(P, Q; I) : (A, \cdot) \to (A, *)$ is a principal isotopy and $(S, T; J) : (A, *) \to (A, \circ)$ is a principal isotopy, then for all $a, b, c, d \in A$:

$$a \cdot b = P(a) * Q(b)$$

and

$$c * d = S(c) \circ T(d).$$

Therefore:

$$\begin{aligned} a \cdot b &= P(a) * Q(b) \\ &= S(P(a)) \circ T(Q(b)) \\ &= (SP)(a) \circ (TQ)(b). \end{aligned}$$

So $(SP, TQ; JI) : (A, \cdot) \to (A, \circ)$ is a principal isotopy and $(A, \cdot)$ is principally isotopic to $(A, \circ)$. Therefore principal isotopy is an equivalence relation. *QED.*

Another important result of principal isotopy allows us to deal with isotopies that are not vector spaces over the same field in a very nice way using principal isotopy.

Theorem 3.2 *If* $(P, Q; R) : (A, \cdot) \to (B, \circ)$ *is an isotopy than there exists a principal isotope* $(A, *)$ *for* A *such that* $(A, *)$ *is isomorphic to* $(B, \circ)$.

Proof: Define $*$ on A by

$$a * c = R^{-1}(R(a) \circ R(c))$$

for all $a, c \in A$. By construction R is linear, invertible, and

$$R(a * c) = R(a) \circ R(c).$$

Thus $R : (A, *) \to (B, \circ)$ is an algebra isomorphism.

Define $S = R^{-1}P : (A, \cdot) \to (A, *)$ and $T = R^{-1}Q : (A, \cdot) \to (A, *)$. We argue that

$$(S, T; I) : (A, \cdot) \to (A, *)$$

is an isotopy. Indeed, for $a, c \in A$

$$\begin{aligned} S(a) * T(c) &= R^{-1}P(a) * R^{-1}Q(c) \\ &= R^{-1}(RR^{-1}P(a) \circ RR^{-1}Q(c)) \\ &= R^{-1}(P(a) \circ Q(c)) \\ &= R^{-1}R(a \cdot c) \\ &= a \cdot c. \end{aligned}$$

QED.

In practice this means that if A is isotopic to B we may replace B with an isomorphic copy which looks like A as a vector space and replaces the isotopy with an isotopy of the form $(S, T; I)$. Equivalently, if A is isotopic to B then the algebra structure on B can be "transferred" to a principal isotope of A.

We now move into a new proof of Albert's theorem that two finite dimensional associative algebras are isotopic if and only if they are isomorphic.

Definition 3.3 *We say an associative algebra A with 1 is* **von Neumann finite** *if for every $a, b \in A$ such that $ab = 1$, then necessarily $ba = 1$.*

Examples of von Neumann finite algebras are commutative rings, division rings, and finite-dimensional associative algebras with 1. The first two examples given here are obviously von Neumann finite, so we give a brief explanation of why the third example is von Neumann finite.

Suppose that A is a finite-dimensional algebra over the scalar field F. Let $\{1 = x_1, x_2, ..., x_n\}$ be a basis for A over F. Left multiplication by $a \in A$ gives rise to a matrix $\bar{a}$, and similarly $\bar{b}$ represents $b \in A$. If $ab = 1$, then $\bar{a}\bar{b} = 1$. However, $\bar{a}\bar{b} = 1$ implies $\bar{b}\bar{a} = 1$ for matrices. Now

$$\begin{aligned} 1 = x_1 &= \bar{b}\bar{a}(x_1) \\ &= bax_1 \\ &= ba. \end{aligned}$$

Therefore $ab = 1$ implies $ba = 1$, and finite-dimensional associative algebras are von Neumann finite.

Theorem 3.3 *If A and B are two algebras with B associative and von Neumann finite, then A and B are isomorphic if and only if they are isotopic.*

Proof: We already know that isomorphisms are isotopies, so we only need to check implication the other way. Suppose we have an isotopy, $(P, Q; R) : A \to B$, with B a von Neumann finite associative algebra. Then we know that if $a, b \in A$ that $R(ab) = P(a)Q(b)$. If $b = 1$, then $R(a) = P(a)Q(1)$, and if $a = 1$, then $R(b) = P(1)Q(b)$. Since R is invertible, it is onto, so choose $a \in A$ such that $R(a) = 1$. So $1 = P(a)Q(1)$, and $Q(1)$ has a left inverse. By the restriction of B to a von Neumann finite algebra, $Q(1)$ must have a two-sided inverse, $P(a)$. Using a similar logic, we see that $P(1)^{-1}$

exists and is $Q(b)$. Now we define $f : A \to B$ by $f(x) = P(1)^{-1}R(x)Q(1)^{-1}$. We see that f is one-to-one and onto. If $x \neq y$ and $x, y \in A$, then since $R(x) \neq R(y), f(x) \neq f(y)$. Also, since R is onto, we see that f must also be onto. Lastly:

$$\begin{aligned}
f(xy) &= P(1)^{-1}R(xy)Q(1)^{-1} \\
&= P(1)^{-1}P(x)Q(y)Q(1)^{-1} \\
&= P(1)^{-1}P(x)Q(1)Q(1)^{-1}P(1)^{-1}P(1)Q(y)Q(1)^{-1} \\
&= P(1)^{-1}R(x)Q(1)^{-1}P(1)^{-1}R(y)Q(1)^{-1} \\
&= f(x)f(y).
\end{aligned}$$

So f is an isomorphism from A to B, *QED*.

With that introduction to isotopy, I now want to get to the most significant link betweem semifields and projective planes. Suppose we had two isomorphic projective planes. What can we say about the semifields that coordinatize them? It may seem logical to think that the semifields are isomorphic, but that is not the case. Instead, it turns out that the semifields that coordinatize them are isotopic! The converse is also true: If two semifields are isotopic, then the projective planes they coordinatize are isomorphic. The following theorem is due to Albert [1].

Theorem 3.4 *Two semifields coordinatize the same projective plane if and only if they are isotopic.*

We will not prove this right now, but will state and prove several lemmas along the way leading up to a complete proof.

Lemma 3.3 *Let π and π' be projective planes coordinatized by semifields and let $\alpha : \pi \to \pi'$ an isomorphism such that $\alpha(0,0,1) = (0,0,1), \alpha(0,1,0) = (0,1,0)$, and $\alpha(1,0,0) = (1,0,0)$. Then the semifields coordinatizing π and π' are isotopic.*

Proof: We know that [0, 0, 1] = (0, 0, 1):(0, 1, 0), so because α is an isomorphism,

$$\alpha[0,0,1] = \alpha(0,0,1) : \alpha(0,1,0) = (0,0,1) : (0,1,0) = [0,0,1].$$

We also know that for all a in the particular semifield that $(0,1,a) \in [0,0,1]$, so there must be a 1-1 correspondence Q such that

$$\alpha(0,1,a) = (0,1,Q(a)).$$

Since $\alpha[0,0,1] = [0,0,1]$, α simply maps the points on [0, 0, 1] to other points on that line. Similarly we find that α maps [0, 1, 0] to [0, 1, 0] and [1, 0, 0] to [1, 0, 0]. By the incidence equation, points of the form $(1,0,b)$ are incident to [0, 1, 0] and points of the form $(1,a,0)$ are incident to [1, 0, 0]. Thus there exist 1-1 correspondences P and R such that

$$\alpha(1,0,b) = (1,0,R(b))$$

and

$$\alpha(1,a,0) = (1,P(a),0).$$

From the rules of incidence and isomorphism, we find that:

$$\begin{aligned}(0,0,1),(1,a,0)\in[0,1,-a] &\Rightarrow [0,1,-a]=(0,0,1):(1,a,0)\\ &\Rightarrow \alpha[0,1,-a]=\alpha(0,0,1):\alpha(1,a,0)\\ &= (0,0,1):(1,P(a),0)\\ &= [0,1,-(P(a))]\end{aligned}$$

$$\begin{aligned}(0,1,a),(1,0,b)\in[1,a,b] &\Rightarrow [1,a,b]=(0,1,a):(1,0,b)\\ &\Rightarrow \alpha[1,a,b]=\alpha(0,1,a):\alpha(1,0,b)\\ &= (0,1,Q(a)):(1,0,R(b))\\ &= [1,Q(a),R(b)]\end{aligned}$$

$$\begin{aligned}(1,a,b) &= [0,1,-a]\cap[1,0,b]\\ &\Rightarrow \alpha(1,a,b)=\alpha[0,1,-a]\cap\alpha[1,0,b]\\ &= [0,1,-(P(a))]\cap[1,0,R(b)]\\ &= (1,P(a),R(b)).\end{aligned}$$

Because α is an isomorphism:

$$\begin{aligned}(1,x_2,x_3)\in[1,y_2,y_3] &\Leftrightarrow \alpha(1,x_2,x_3)\in\alpha[1,y_2,y_3]\\ &\Leftrightarrow (1,P(a),R(b))\in[1,Q(a),R(b)]\end{aligned}$$

When we translate this to the incidence equation we have:

$$x_3=x_2y_2+y_3\Leftrightarrow R(x_3)=P(x_2)Q(y_2)+R(y_3).$$

Because $x_3=x_2y_2+y_3$ and R is an isomorphism for addition, we also have:

$$\begin{aligned}R(x_2y_2+y_3) &= P(x_2)Q(y_2)+R(y_3)\\ R(x_2y_2)+R(y_3) &= P(x_2)Q(y_2)+R(y_3)\\ R(x_2y_2) &= P(x_2)Q(y_2).\end{aligned}$$

This holds for all x_2 and y_2 in the semifield corrdinatizing π, and so we have an isotopy $(P,Q;R)$. Therefore the two semifields coordinatizing π and π' are isotopic, QED.

We state and prove the converse of this lemma. The proof essentially goes backwards through the proof of the lemma above.

Lemma 3.4 *Let $(P,Q;R)$ be an isotopy from a finite semifield S' to a finite semifield S and let π', π be the planes they coordinatize, respectively. Define a map $\alpha:\pi\rightarrow\pi'$ by $\alpha(0,1,a)=(0,1,Q(a))$, $\alpha(1,0,b)=(1,0,R(b))$, and $\alpha(1,a,0)=(1,P(a),0)$ for the points and $\alpha[0,1,-a]=[0,1,-P(a)]$, $\alpha[1,a,b]=[1,Q(a),R(b)]$, and $\alpha(1,a,b)=\alpha[0,1,-a]\cap\alpha[1,0,b]=(1,P(a),R(b))$ for the lines. Then α is an isomorphism from π to π'.*

Proof: Now to show that α is an isomorphism, we must show that α is one-to-one, onto, and:

$$(x_1, x_2, x_3) \in [y_1, y_2, y_3] \Leftrightarrow \alpha(x_1, x_2, x_3) \in \alpha[y_1, y_2, y_3].$$

that is, that incidence is preserved under α. We look at every possible incidence relation and show that for all these cases that α preserves incidence.

First, if $(0, x_2, x_3)$ is a point, then it can be incident to certain lines of the form $[0.y_2, y_3]$ and $[1, y_2, y_3]$. By the incidence equation:

$$\begin{aligned} (0, x_2, x_3) \in [0, y_2, y_3] &\Leftrightarrow 0 = x_2 y_2 \\ &\Leftrightarrow x_2 = 0 \text{ or } y_2 = 0. \end{aligned}$$

Similarly:

$$\begin{aligned} \alpha(0, x_2, x_3) \in \alpha[0, y_2, y_3] &\Leftrightarrow (0, x_2, Q(x_3)) \in [0, y_2, P(y_3)] \\ &\Leftrightarrow 0 = x_2 y_2 \\ &\Leftrightarrow x_2 = 0 \text{ or } y_2 = 0. \end{aligned}$$

Therefore :

$$(0, x_2, x_3) \in [0, y_2, y_3] \Leftrightarrow \alpha(0, x_2, x_3) \in \alpha[0, y_2, y_3].$$

We continue on to the case if $(0, x_2, x_3) \in [1.y_2, y_3]$.

$$\begin{aligned} (0, x_2, x_3) \in [1.y_2, y_3] &\Leftrightarrow x_3 = x_2 y_2 \\ &\Leftrightarrow x_2 = 1 \text{ and } x_3 = y_2 \\ &\Leftrightarrow x_2 = 1 \text{ and } Q(x_3) = Q(y_2) \end{aligned}$$

$$\begin{aligned} \alpha(0, x_2, x_3) \in \alpha[1, y_2, y_3] &\Leftrightarrow (0, x_2, Q(x_3)) \in [1, Q(y_2), R(y_3)] \\ &\Leftrightarrow Q(x_3) = x_2 Q(y_2) \\ &\Leftrightarrow x_2 = 1 \text{ and } Q(x_3) = Q(y_2) \end{aligned}$$

Again, we see that incidence is preserved.

Next, if $(1, x_2, x_3)$ is a point, then it is incident to lines of the form $[0, y_2, y_3]$ and $[1, y_2, y_3]$. This presents two cases.

$$\begin{aligned} (1, x_2, x_3) \in [0, y_2, y_3] &\Leftrightarrow 0 = x_2 y_2 + y_3 \\ &\Leftrightarrow y_2 = 1 \text{ and } y_3 = -x_2 \\ &\Leftrightarrow y_2 = 1 \text{ and } P(y_3) = P(-x_2) \end{aligned}$$

$$\begin{aligned} \alpha(1, x_2, x_3) \in \alpha[0, y_2, y_3] &\Leftrightarrow (1, P(x_2), R(x_3)) \in [0, y_2, P(y_3)] \\ &\Leftrightarrow 0 = P(x_2) y_2 + P(y_3) \\ &\Leftrightarrow y_2 = 1 and P(y_3) = -P(x_2) = P(-x_2) \end{aligned}$$

Our last case is to check incidences when $(1, x_2, x_3) \in [1, y_2, y_3]$.

$$(1, x_2, x_3) \in [1, y_2, y_3] \Leftrightarrow x_3 = x_2 y_2 + y_3$$

Since R is an isomorphism on addition,

$$R(x_3) = R(x_2 y_2 + y_3) = R(x_2 y_2) + R(y_3).$$

But since $(P, Q; R)$ is an isotopy,

$$R(x_2 y_2) + R(y_3) = P(x_2)Q(y_2) + R(y_3).$$

So $R(x_3) = P(x_2)Q(y_2) + R(y_3)$, which is true if and only if:

$$(1, P(x_2), R(x_3)) \in [1, Q(y_2), R(y_3)] \Leftrightarrow \alpha(1, x_2, x_3) \in \alpha[1, y_2, y_3].$$

So we see that in all of these cases α preserves incidence from projective planes π to π'. Now we just need to show that α is one-to-one and onto. We check the mapping of points and lines. If $\alpha(1, a, b) = \alpha(1, c, d)$, then:

$$\begin{aligned} (1, P(a), R(b)) = (1, P(c), R(d)) &\Rightarrow P(a) = P(c) \text{ and } R(b) = R(d) \\ &\Rightarrow a = c \text{ and } b = d \\ &\Rightarrow (1, a, b) = (1, c, d). \end{aligned}$$

The other case for points, of the form $(0, a, b)$, follow in the same way from the conditions on α as stated in the statement of the lemma. Similarly, the two cases for lines, those of the form $[1, a, b]$ and those of the form $[0, a, b]$ follow immediately.

Since we are dealing with a finite projective plane and finite semifields, α is onto. Therefore, α is indeed an isomorphism of these two projective planes. *QED*.

Corollary 3.1 *Isotopic semifields coordinatize the same projective plane.*

So we are half of the way to our goal for this section. We have shown that if two semifields are isotopic, then the projective planes they coordinatize are isotopic. We will now proceed in the opposite direction, and will show that if we have two isomorphic projective planes, then we will see that the semifields that coordinatize them are isotopic.

Now we use this theorem to prove another important result.

Theorem 3.5 *Every collineation of a plane coordinatized by a proper semifield stabilizes a given line L and fixes a point $P \in L$.*

Proof: A complete proof of this requires much explanation, so I will instead give an outline of the steps taken to prove this. More details can be found in Albert [1] and Hall [5].

We showed in Theorem 2.5 that the plane π is coordinatized by a semifield if and only if there are distinct points E and F such that π is P-L-transitive for $L = E : F$ and all points $P \in E : F$, and for $P = F$ and all lines L through F. From Theorem 2.6, π is coordinatized by a finite field if and only if there exists $P \notin L$ such that π is P-L transitive. Therefore if π is coordinatized by a proper semifield then we know that π must be P-L-transitive for a given line L and all $P \in L$ and for given point P all lines L through P. It then follows that π must be P-L-transitive for a given line L and a point $P \in L$. Therefore every collineation of π must stabilize L and fix P by the definition of P-L-transitivity. *QED*.

The last step we need to prove the theorem is to define a couple families of collineations of a projective plane π, coordinatized by a semifield S. These collineations are called translations $\tau_{h,k}$ and shears $\sigma_{h,k}$, where $h, k, \in S$. They are defined as follows:

$$\tau_{h,k}(x_1, x_2, x_3) = (x_1, x_2 + x_1 h, x_3 + x_1 k)$$
$$\tau_{h,k}[y_1, y_2, y_3] = [y_1, y_2, y_3 - hy_2 + y_1 k]$$
$$\sigma_{h,k}(x_1, x_2, x_3) = (x_1, x_2, x_3 + x_2 h + x_1 k)$$
$$\sigma_{h,k}[y_1, y_2, y_3] = [y_1, y_2 + y_1 h, y_3 + y_1 k].$$

It's not immediately obvious that they are collineations, but we provide a proof.

Lemma 3.5 *$\tau_{h,k}$ and $\sigma_{h,k}$ define collineations.*

Proof: We use the incidence equation for homogeneous coordinates. If a point is incident to a line, then the image of the point should be incident to the image of the line under the collineation. We do this first for translations. We begin with the equation $y_1 x_3 = x_2 y_2 + x_1 y_3$, and under the translation mapping we have:

$$\begin{aligned} y_1(x_3 + x_1 k) &= (x_2 + x_1 h)y_2 + x_1(y_3 - hy_2 + y_1 k) \\ y_1 x_3 + y_1(x_1 k) &= x_2 y_2 + (x_1 h)y_2 + x_1 y_3 - x_1(hy_2) + x_1(y_1 k). \end{aligned}$$

Since $x_1, y_1 = 0, 1$, one quickly sees that $y_1(x_1 k) = x_1(y_1 k)$ and that $(x_1 h)y_2 = x_1(hy_2)$, so we cancel out the appropriate terms and have:

$$y_1 x_3 = x_2 y_2 + x_1 y_3.$$

Then we are left with the regular definition of incidence. So translations are collineations. We do the same for the shears.

$$\begin{aligned} y_1(x_3 + x_2 h + x_1 k) &= x_2(y_2 + y_1 h) + x_1(y_3 + y_1 k) \\ y_1 x_3 + y_1(x_2 h) + y_1(x_1 k) &= x_2 y_2 + x_2(y_1 h) + x_1 y_3 + x_1(y_1 k) \end{aligned}$$

Again, since $x_1, y_1 = 0, 1$, $y_1(x_2 h) = x_2(y_1 h)$ and $y_1(x_1 k) = x_1(y_1 k)$, so we cancel out the appropriate terms and see that:

$$y_1 x_3 = x_2 y_2 + x_1 y_3.$$

We are again left with the incidence equation, proving that these two families of maps do in fact define collineations. *QED*.

Now we can prove Theorem 3.4.

Theorem 3.4 *Two semifields coordinatize the same projective plane if and only if they are isotopic.*

Proof: We split this proof up into two cases. The first case will be where both coordinatizing semifields are proper semifields. In this case, we will satisfy the hypotheses of Lemma 3.3 to show that the semifields coordinatizing the two isomorphic projective planes are isomorphic. In the second, one of the coordinatizing semifields is associative.

Case 1: Both coordinatizing semifields are proper semifields.

Suppose we have an isomorphism $\beta : \pi \to \pi'$ between two projective planes coordinatized by two semifields S and S'. Choose a coordinitization of π such that π is $(0,0,1)$-$[0,0,1]$-transitive, then $\beta(0,0,1) = (0,0,1)$ and $\beta[0,0,1] = [0,0,1]$ by the lemma we just proved. Now $\beta(0,1,0) = (0,1,a)$, where $a \in S$, because all points of the form $(0,1,a) \in [0,0,1]$. Similarly, $\beta(1,0,0) = (1,b,c)$ for some $b, c \in S$ because $(1,0,0) \in [1,a,0]$, $(1,0,0) \in [0,1,0]$, $(1,b,c) \in [0,1,-b]$, and $(1,b,c) \in [1,a,-ba]$. Now define the isomorphism α:

$$\alpha = \tau_{-b,ba-c}\sigma_{-a,0}\beta.$$

Now we must show that α maps the points (0, 0, 1), (0, 1, 0), and (1, 0, 0) in some projective plane π to the points (0, 0, 1), (0, 1, 0), and (1, 0, 0) in some projective plane π'. So we check this:

$$\begin{aligned}
\alpha(1,0,0) &= \tau_{-b,ba-c}\sigma_{-a,0}\beta(1,0,0) \\
&= \tau_{-b,ba-c}\sigma_{-a,0}(1,b,c) \\
&= \tau_{-b,ba-c}(1,b,c+b(-a)) = \tau_{-b,ba-c}(1,b,c-ba) \\
&= (1,b-b,c-ba+ba-c) = (1,0,0)
\end{aligned}$$

$$\begin{aligned}
\alpha(0,1,0) &= \tau_{-b,ba-c}\sigma_{-a,0}\beta(0,1,0) \\
&= \tau_{-b,ba-c}\sigma_{-a,0}(0,1,a) \\
&= \tau_{-b,ba-c}(0,1,a+(-a)) = \tau_{-b,ba-c}(0,1,a) \\
&= (0,1,0)
\end{aligned}$$

$$\begin{aligned}
\alpha(0,0,1) &= \tau_{-b,ba-c}\sigma_{-a,0}\beta(0,0,1) \\
&= \tau_{-b,ba-c}\sigma_{-a,0}(0,0,1) \\
&= \tau_{-b,ba-c}(0,0,1) \\
&= (0,0,1).
\end{aligned}$$

From Lemma 3.3, this means that S and S' are isotopic. The converse for this case and the second case is precisely the corollary to one of the lemmas.

Case 2: One of the coordinatizing semifields is associative.

Theorem 3.5 is only stated for proper semifields, so it cannot be applied in this case. Indeed, it is false for projective planes coordinatized by fields. Consider the Fano Plane. One collineation of that plane is just a rotation of the plane, mapping the point $(0,0,1)$ to $(1,0,0)$, $(1,0,0)$ to $(0,1,0)$, and so on. So there is no guarantee that $(0,0,1)$ will map to $(0,0,1)$.

We proceed in the proof of this case. Let $\theta : \pi \to \pi'$ be an isomorphism and without loss of generality, suppose π is coordinatized by an associative field. Then there exists a $P \notin L$ such that π is P-L-transitive. Since isomorphism preserves incidence, π' is $\theta(P)$-$\theta(L)$-transitive with $\theta(P) \notin \theta(L)$. Therefore π' must be coordinatized by an associative field.

So now we quickly show that the fields coordinatizing π and π' are isotopic. Since π and π' are isomorphic, then there is a one-to-one correspondence of the points and lines. Therefore π and π'

each have the same number of points and lines. So the finite fields coordinatizing them have the same cardinality. It is clear from this observation that this means that F and F' are isomorphic and therefore isotopic. QED.

So now that we know that semifields coordinatize isomorphic projective planes if and only if they are isotopic, what can we do with it? First, this could possibly give us an easier means of determining whether or not two semifields are isotopic. Isomorphism is certainly an easier condition than isotopy to check for, so if we have two semifields, we can examine the projective planes they determine. If we have a mapping between two projective planes that preserves incidence, then we know that the two semifields are isotopic. We can use the lemmas stated earlier to get a little idea for what these maps look like. One disadvantage, though, is that for a semifield of cardinality n, the projective plane will have n^2+n+1 points, n^2+n+1 lines, and three elements of the semifield to determine each point and line, so computer checks will be impossible for some orders.

4 Dickson Quadratic Semifields

In 1906 the algebraist L. E. Dickson [4] considered ways to construct finite commutative semifields that were Galois fields. One result of his work was the discovery of a family of commutative proper semifields, the first such family of semifields. We will study this family here to learn about how to solve linear equations and discover which such semifields are isomorphic. This family is constructed from the field $F = GF(p^m)$, where p is an odd prime. Let the elements of the semifield be:

$$S = \{a + \lambda b | a, b \in F\},$$

define addition in the usual component-wise fashion, and define multiplication by

$$(a + \lambda b)(c + \lambda d) = (ac + \sigma(b)\sigma(d)f) + \lambda(ad + bc),$$

where σ is an automorphism of F and f is a nonsquare, nonzero element of F. This construction is a semifield of order p^{2m} which we will denote by (F, σ, f). We will see shortly that this is a semifield, why f must be nonsquare, and what conditions are necessary and sufficient for associativity.

Lemma 4.1 *Let p be a prime. If $p = 2$ then every nonzero element of $GF(p^m)$ is square. If p is odd, then the nonzero squares in $GF(p^m)$ constitute a subgroup of index two in the multiplication group of all nonzero elements. As a consequence, if σ is an automorphism of $GF(p^m)$, with p odd, and x is nonzero then $\frac{x}{\sigma(x)}$ and $x\sigma(x)$ are always squares in $GF(p^m)$.*

Proof: Let $GF(p^m)^\times$ be the multiplicative group of nonzero elements in a finite field $GF(p^m)$. Define $s : GF(p^m)^\times \to GF(p^m)^\times$ by $s(a) = a^2$. Then s is a group homomorphism. Let $Im(s)$ denote the image of s and $Ker(s)$ the kernel. Then

$$Im(s) \cong GF(p^m)^\times / Ker(s),$$

where

$$Ker(s) = \{x \in GF(p^m)^\times | x^2 = 1\}.$$

But in a field, $x^2 = 1$ if and only if $x = \pm 1$. If $p = 2$, then $1 = -1$, and the kernel is trivial, so s is one-to-one. Since $GF(2^m)^\times$ is finite, $Im(s) = GF(2^m)^\times$. So every nonzero element of $GF(2^m)$ is square. If $p \neq 2$, then $1 \neq -1$, so

$$|Im(s)| = \left| \frac{GF(p^m)^\times}{2} \right|.$$

Hence,

$$[GF(p^m)^\times : Im(s)] = 2.$$

If σ is an automorphism of $GF(p^m)$ then

$$\sigma(a^2) = (\sigma(a))^2.$$

That is,

$$\sigma(Im(s)) = Im(s).$$

Since

$$|GF(p^m)^\times : Im(s)| \leq 2,$$

it follows that σ also sends non-squares to non-squares. In other words, if $x \in GF(p^m)^\times$, then

$$x \equiv \sigma(x)(\text{mod } Im(s)).$$

It follows that

$$\frac{x}{\sigma(x)} \in Im(s)$$

and

$$x^2 \equiv x\sigma(x)(\text{mod } Im(s)).$$

QED.

This lemma tells us why Dickson quadratic semifields must be vector spaces over a field of odd characteristic. Nonsquares must be available.

Theorem 4.1 *The Dickson construction, (F, σ, f), is a semifield.*

Proof: We need to show that the four axioms are satisfied with this construction. First, it is clear that addition is a group, with the identity being 0. Second, suppose

$$(a + \lambda b)(c + \lambda d) = 0.$$

Then

$$ac + \sigma(b)\sigma(d)f = 0$$

and

$$ad + bc = 0.$$

Suppose $d \neq 0$. Let's substitute

$$a = -bcd^{-1}$$

into the equation with the automorphism. Then

$$-b(c^2)d^{-1} + \sigma(b)\sigma(d)f = 0.$$

Solving for f,

$$f = c^2 \frac{b}{\sigma(b)} \frac{d}{\sigma(d)}.$$

Recall the result of Lemma 4.1. This contradicts the assumption that f is not a square.

Now suppose that $d = 0$. Substituting this in above we have:

$$ac = 0$$

and

$$bc = 0.$$

Thus $a = 0$ or $c = 0$, and also $b = 0$ or $c = 0$. So any possibility gives us a factor 0. Therefore, the only situation for which the product of two elements is zero occurs when $a+\lambda b = 0$ or if $c+\lambda d = 0$.

Third, we show the distributive properties hold.

$$\begin{aligned}(x+\lambda y)((a+\lambda b)+(c+\lambda d)) &= (x+\lambda y)((a+c)+\lambda(b+d)) \\ &= x(a+c)+\sigma(y)\sigma(b+d)f+\lambda(x(b+d)+y(a+c)) \\ &= xa+\sigma(y)\sigma(b)f+\lambda(xb+ya)+xc+\sigma(y)\sigma(d)f+\lambda(xd+yc) \\ &= (x+\lambda y)(a+\lambda b)+(x+\lambda y)(c+\lambda d))\end{aligned}$$

A similar argument shows that the other distributive property holds.

Lastly, we show that there is a multiplicative identity, $1 = 1+\lambda 0$.

$$\begin{aligned}(1+\lambda 0)(a+\lambda b) &= 1a+0+\lambda(1b+0) \\ &= a+\lambda b \\ &= a1+\lambda(b1+0) \\ &= (a+\lambda b)(1+\lambda 0)\end{aligned}$$

So

$$(1+\lambda 0)(a+\lambda b) = (a+\lambda b)(1+\lambda 0) = (a+\lambda b).$$

Thus $1 = 1+\lambda 0$ is the multiplicative identity.

So Dickson's construction meets all the criteria for a finite semifield, QED.

One property of the Dickson semifields that does not in general hold for all semifields is that they are commutative. A quick look at the definition of multiplication of two elements of these semifields along with the property that all fields are commutative will show you why this is true.

$$\begin{aligned}(a+\lambda b)(c+\lambda d) &= (ac+\sigma(b)\sigma(d)f)+\lambda(ad+bc) \\ &= (ca+\sigma(d)\sigma(b)f+\lambda(da+cb) \\ &= (c+\lambda d)(a+\lambda b)\end{aligned}$$

Now we give the necessary and sufficient condition that will make a Dickson quadratic semifield associative.

Theorem 4.2 *A Dickson quadratic semifield (F, σ, f) is associative if and only if σ is the identity.*

Proof: Suppose first that the Dickson quadratic semifield, (F, σ, f) is associative. Let λ be the nonunity basis element of (F, σ, f) over F and let $a \in F$. If (F, σ, f) is associative then

$$\begin{aligned}(\lambda\cdot\lambda)\cdot a &= \lambda\cdot(\lambda\cdot a) \\ f\cdot a &= \lambda\cdot(\lambda a) \\ fa &= \sigma(a)f \\ a &= \sigma(a).\end{aligned}$$

Therefore σ is the identity.

Suppose now that σ is the identity automorphism. The multiplication is given by the following formula:

$$(a + \lambda b)(c + \lambda d) = (ac + bdf) + \lambda(ad + bc)$$

Since f is not a square, this is precisely the multiplication of the field

$$\frac{GF(p^m)[X]}{(X^2 - f)},$$

where X is sent to λ. Here the Dickson construction is the field of order p^{2m}, which is associative, *QED*.

Now the second axiom for finite semifields only requires that the semifield have no zero divisors. We want to see how Dickson semifields meet the equivalent property that linear equations can be solved. That is, how does one solve the equation $(a + \lambda b)(x + \lambda y) = (c + \lambda d)$ for $(x + \lambda y)$? We will begin by multiplying the numbers out.

$$\begin{aligned}(c + \lambda d) &= (a + \lambda b)(x + \lambda y)\\ &= (ax + \sigma(b)\sigma(y)f) + \lambda(bx + ay)\end{aligned}$$

This lends itself to the following system:

$$\begin{cases} ax + \sigma(b)\sigma(y)f = c \\ bx + ay = d. \end{cases}$$

Now if $b = 0$, then $x = a^{-1}c$ and $y = a^{-1}d$. We also get an easy solution if $a = 0$: $x = b^{-1}d$ and $y = \sigma^{-1}((\sigma(b))^{-1}cf^{-1})$. So suppose that $a, b \neq 0$. Then $x = \frac{d-ay}{b}$, and

$$a\frac{d - ay}{b} + \sigma(b)\sigma(y)f = c$$
$$ad - a^2y + \sigma(b)\sigma(y)bf = bc.$$

So now all we need to do is solve for y, which sounds easier than it turns out to be, since there is a σ in the way. We do see that:

$$y = \frac{ad + b\sigma(b)\sigma(y)f - bc}{a^2}.$$

We know that $a \neq 0$, so we are fine. To simplify this equation, let

$$r = \frac{ad - bc}{a^2}$$
$$s = \frac{b\sigma(b)f}{a^2}$$

so that $y = r + s\sigma(y)$. If σ^n is the identity, then we apply σ to $y = r + s\sigma(y)$, substitute into $\sigma(y)$. We repeat this process so that we eventually apply σ $n - 1$ times to $y = r + s\sigma(y)$, substituting into $\sigma^k(y)$ on the kth step. We see how this is run below.

$$\begin{aligned}
y &= r + s\sigma(y) \\
\sigma(y) &= \sigma(r) + \sigma(s)\sigma^2(y) \\
\Rightarrow y &= r + s(\sigma(r) + \sigma(s)\sigma^2(y)) \\
\sigma^2(y) &= \sigma^2(r) + \sigma^2(s)\sigma^3(y) \\
\Rightarrow y &= r + s(\sigma(r) + \sigma(s)(\sigma^2(r) + \sigma^2(s)\sigma^3(y))) \\
&\cdots \\
\sigma^{n-1}(y) &= \sigma^{n-1}(r) + \sigma^{n-1}(s)y
\end{aligned}$$

Then we follow the pattern we see forming and see that:

$$y = \sum_{i=0}^{n-1}\left[\sigma^i(r)\prod_{j=0}^{i-1}\sigma^j(s)\right] + \left(\prod_{k=0}^{n-1}\sigma^k(s)\right)y.$$

So our solution for y is:

$$y = \frac{\sum_{i=0}^{n-1}[\sigma^i(r)\prod_{j=0}^{i-1}\sigma^j(s)]}{1 - \prod_{k=0}^{n-1}(\sigma^k(s))}.$$

From this we can find x. The only stumbling block here is if $\prod_{k=0}^{n-1}(\sigma^k(s)) = 1$. If σ is the generator of the group of automorphisms of $GF(p^m)$, then the product of the $\sigma^k(s)$ is the norm of s. If $s \in GF(p^m)$, the norm of s is denoted $N_{GF(p^m)/GF(p^d)}$, where $GF(p^d)$ is the fixed field of σ. Hilbert's Theorem 90 states that if E is a Galois extension of a field F, and $Gal(E/F) = \langle\sigma\rangle$, then $N_{E/F}(s) = 1$ if and only if $s = \frac{\sigma(z)}{z}$ for some $z \in E \setminus \{0\}$. Since $GF(p^m)$ is a Galois extension of $GF(p^d)$, the theorem applies. Now $\frac{\sigma(z)}{z}$ is always a square, but $s = \frac{b\sigma(b)f}{a^2}$ is not a square by Lemma 4.1. So in this case we can find y, and then find x, and therefore find our solution to the equation $(a + \lambda b)(x + \lambda y) = (c + \lambda d)$! Since Dickson quadratic semifields are commutative, finding the solution, $(x + \lambda y)$, to $(x + \lambda y)(a + \lambda b) = (c + \lambda d)$ is not necessary.

If the above equations hold, then we can find inverses. If in the above equation $c = 1$ and $d = 0$, then:

$$r = \frac{-b}{a^2}$$

$$s = \frac{b\sigma(b)f}{a^2}$$

and we can use the same formula as above to find the inverse of $x + \lambda y$.

To learn a little bit more about the properties of this family of semifields, we will investigate the nature of isomorphism and isotopy in these semifields. So we ask ourselves the question: to what extent are σ and f isomorphism invariants?

Theorem 4.3 *Two Dickson semifields, (F, σ, f) and (F, σ_*, f_*), are isomorphic if and only if $\sigma_* = \sigma$.*

To see why, first consider an isomorphism

$$\theta : (F, \sigma, f) \to (F, \sigma_*, f_*)$$

such that $\theta(F) = F$. (We do not assume θ is the identity.) Suppose also that $\theta(\lambda) = x + \lambda y$ for some $x, y \in F$. Since θ is an isomorphism, for every $a \in F$:

$$\begin{aligned}
\theta(\lambda a \cdot \lambda) &= \theta(\lambda a) * \theta(\lambda) \\
\theta(\sigma(a)f) &= (\theta(\lambda) * \theta(a)) * \theta(\lambda) \\
\theta(\sigma(a))\theta(f) &= ((x + \lambda y) * \theta(a)) * (x + \lambda y) \\
\theta(\sigma(a))\theta(f) &= (x\theta(a) + \lambda(y\theta(a))) * (x + \lambda y) \\
\theta(\sigma(a))\theta(f) &= x^2\theta(a) + \sigma_*(y)^2\sigma_*(\theta(a))f_* + \lambda(2xy\theta(a)).
\end{aligned}$$

Therefore

$$2xy\theta(a) = 0.$$

Take $a = 1$. Then $xy = 0$, so either $x = 0$ or $y = 0$. Suppose $y = 0$. Then $\theta(c + \lambda d) \in F$ for all $c, d \in F$, so $\theta((F, \sigma, f)) \subseteq F$. However, θ is an isomorphism and the cardinality of (F, σ, f) is greater than the cardinality of F, so $y \neq 0$. Therefore $\theta(\lambda) = \lambda y$ for some $y \in F$. Now we have

$$\theta(\sigma(a))\theta(f) = \sigma_*(y)^2\sigma_*(\theta(a))f_*.$$

Again, let $a = 1$, then

$$\theta(f) = \sigma_*(y)^2 f_*.$$

Substituting this back into the equation above, we have

$$\theta(\sigma(a))\theta(f) = \theta(f)\sigma_*(\theta(a)).$$

Since $f \neq 0$,

$$\theta(\sigma(a)) = \sigma_*(\theta(a)).$$

Now we show that the automorphisms commute. Since σ_* is an automorphism of $F = GF(p^m)$, there is some $k \geq 0$ with $\sigma_*(z) = z^{p^k}$ for all $z \in F$. Consequently,

$$\begin{aligned}
\theta(\sigma_*(z)) &= \theta(z^{p^k}) \\
&= (\theta(z))^{p^k} \\
&= \sigma_*(\theta(z)).
\end{aligned}$$

For the calculation we interrupted,

$$\sigma_*(\theta(a)) = \theta(\sigma_*(a)),$$

so

$$\theta(\sigma(a)) = \theta(\sigma_*(a)).$$

Since θ is one-to-one

$$\sigma(a) = \sigma_*(a).$$

We conclude that

$$\sigma = \sigma_*.$$

Now suppose $\sigma_* = \sigma$. Let $\theta : (F, \sigma, f) \to (F, \sigma, f_*)$ be a map such that θ restricts to an automorphism of F and sends

$$a + \lambda b \to \theta(a) + \lambda(y\theta(b))$$

where

$$y = \sigma^{-1}\left(\sqrt{\frac{\theta(f)}{f_*}}\right).$$

We showed in Lemma 4.1 that $\theta(f)$ is nonsquare and that the ratio of two nonsquares in a finite field is square. Therefore we can find the square root above. We also do not care which square root is taken. The motivation for this assignment of y is from the first half of this proof where we saw that $\theta(f) = \sigma_*(y)^2 f_*$.

We show that θ is an isomorphism. For every $a + \lambda b, c + \lambda d \in (F, \sigma, f)$:

$$\begin{aligned}
\theta(a+\lambda b) * \theta(c+\lambda d) &= (\theta(a) + \lambda(y\theta(b))) * (\theta(c) + \lambda(y\theta(d))) \\
&= \theta(ac) + \sigma(y)^2\sigma(\theta(bd))f_* + \lambda(y\theta(bc+ad)) \\
&= \theta(ac) + \sigma\left(\sigma^{-1}\left(\sqrt{\frac{\theta(f)}{f_*}}\right)\right)^2 \sigma(\theta(bd))f_* + \lambda(y\theta(bc+ad)) \\
&= \theta(ac) + \left(\sqrt{\frac{\theta(f)}{f_*}}\right)^2 \sigma(\theta(bd))f_* + \lambda(y\theta(bc+ad)) \\
&= \theta(ac) + \frac{\theta(f)}{f_*}\sigma(\theta(bd))f_* + \lambda(y\theta(bc+ad)) \\
&= \theta(ac) + \theta(f)\sigma(\theta(bd)) + \lambda(y\theta(bc+ad)) \\
&= \theta(ac) + \theta(f)\theta(\sigma(bd)) + \lambda(y\theta(bc+ad)) \\
&= \theta(ac + \sigma(bd)f + \lambda(bc+ad)) \\
&= \theta((a+\lambda b)\cdot(c+\lambda d))
\end{aligned}$$

Thus θ is an isomorphism. *QED.*

We already know that $\theta(\lambda) = \lambda y$ for some $y \in F$, so we find y and thus determine what θ maps an arbitrary element of (F, σ, f) to. In the proof above we saw that

$$\theta(f) = \sigma(y)^2 f_*.$$

Thus

$$y = \sigma^{-1}\left(\sqrt{\frac{\theta(f)}{f_*}}\right).$$

Therefore the isomorphism

$$\theta : (F, \sigma, f) \to (F, \sigma, f_*)$$

can be described

$$\theta(a + \lambda(b)) = \theta(a) + \lambda\left(\sigma^{-1}\left(\sqrt{\frac{\theta(f)}{f_*}}\right)\theta(b)\right).$$

The point of this special example is that F is an isomorphism invariant for (F, σ, f). Therefore the classification of isomorphisms of Dickson quadratic semifields above is complete.

Definition 4.1 *Let S be a semifield. The* **middle nucleus** *of S is $N(S) = \{y \in S | (xy)z = x(yz)\ \forall x, z \in R\}$.*

For example, the middle nucleus of any associative field is the entire field.

Theorem 4.4 *The middle nucleus of a proper Dickson quadratic semifield, $S = (F, \sigma, f)$, is F.*

Proof: We show mutual containment. Suppose $y \in F$ and let $a + \lambda b, c + \lambda d \in (F, \sigma, f)$. Then

$$\begin{aligned}
[(a + \lambda b) \cdot y] \cdot (c + \lambda d) &= (ay + \lambda by) \cdot (c + \lambda d) \\
&= acy + \sigma(bdy)f + \lambda(bcy + ady) \\
&= (a + \lambda b) \cdot (cy + \lambda dy) \\
&= (a + \lambda b) \cdot [y \cdot (c + \lambda d)].
\end{aligned}$$

Therefore $y \in N(S)$ and $F \subseteq N(S)$.

Now suppose $y_1 + \lambda y_2 \in N(S)$. In particular,

$$\begin{aligned}
[(a + \lambda) \cdot (y_1 + \lambda y_2)] \cdot (\lambda) &= (a + \lambda) \cdot [(y_1 + \lambda y_2) \cdot (\lambda)] \\
(ay_1 + \sigma(y_2)f + \lambda(y_1 + ay_2)) \cdot (\lambda) &= (a + \lambda) \cdot (\sigma(y_2)f + \lambda(y_1)) \\
\sigma(y_1)f + \sigma(ay_2)f + \lambda(ay_1 + \sigma(y_2)f) &= a\sigma(y_2)f + \sigma(y_1)f + \lambda(\sigma(y_2)f + ay_1) \\
\sigma(a)\sigma(y_2)f &= a\sigma(y_2)f.
\end{aligned}$$

If $y_2 \neq 0$, then $\sigma(a) = a$, making the semifield an associative field. Therefore $y_2 = 0$, so $y_1 + \lambda y_2 = y_1 \in F$. So $N(S) \subseteq F$. By mutual containment, $N(S) = F$, *QED*.

Theorem 4.5 *If $\theta : R \to S$ is an isomorphism of semifields, then $\theta(N(R)) \subseteq N(S)$.*

Proof: Let $y \in N(R)$. Then for all $x, z \in R$:

$$\begin{aligned}
\theta((x \cdot y) \cdot z) &= \theta(x \cdot (y \cdot z)) \\
\theta(x \cdot y) * \theta(z) &= \theta(x) * \theta(y \cdot z) \\
(\theta(x) * \theta(y)) * \theta(z) &= \theta(x) * (\theta(y) * \theta(z))
\end{aligned}$$

Therefore $\theta(y) \in N(S)$ and $\theta(N(R)) \subseteq N(S)$, *QED*.

In the case that R and S are Dickson quadratic semifields, this means that $\theta(F) \subseteq F$, since the middle nucleus of such semifields is F. However, since θ is an isomorphism, $\theta(F)$ and F have the same cardinality, so $\theta(F) = F$ for every isomorphism of two Dickson quadratic semifields. Therefore the classification of isomorphisms of Dickson quadratic semifields given above is complete. Here we provide an example of an isomorphism.

Example 4.1 *Suppose $F = GF(5^2) = \frac{GF(5)[X]}{X^2-2}$, and σ is the automorphism of F defined by $\sigma(x) = x^5$.*

Two nonsquare elements of F are 2 and 3. Let $S = (F, \sigma, 2)$ and $(S, *) = (F, \sigma, 3)$. If $\theta : S \to (S, *)$ is an isomorphism with the accompanying automorphism θ being the identity, then

$$\theta(x + \lambda y) = x + \lambda((2 \cdot 3^{-1})y) = x + \lambda(4y).$$

So for an example of why this is an isomorphism, we choose two random elements of S: $(1 + 3\omega) + \lambda(2 + 4\omega)$ and $(2 + 3\omega) + \lambda(2 + \omega)$. Then:

$$\begin{aligned}
\theta(((1 + 3\omega) + \lambda(2 + 4\omega))((2 + 3\omega) + \lambda(2 + \omega))) &= \theta((2 + 4\omega) + \lambda(1 + \omega)) \\
&= (2 + 4\omega) + \lambda(4 + 4\omega).
\end{aligned}$$

$$\begin{aligned}\theta((1+3\omega)+\lambda(2+4\omega))\theta((2+3\omega)+\lambda(2+\omega)) &= (1+3\omega)+\lambda(3+\omega))((2+3\omega)+\lambda(3+4\omega)) \\ &= (2+4\omega)+\lambda(4+4\omega).\end{aligned}$$

Burmester [3] has characterized isomorphisms and isotopies of Dickson semifields according to Math Reviews. The reference was not accessible, so we are not sure what his characterizations of isomorphisms and isotopies are.

This wraps up our study on Dickson quadratic semifields. We were able to find solutions to many linear equations, if the automorphism used in the definition of multiplication was a generator of the Galois group of automorphisms of the ground field. We then gave a form that describes isomorphisms of these semifields. Future work would certainly include determining which Dickson quadratic semifields are isotopic and learning about some number theoretic properties of this and other families of semifields.

Bibliography

1. Albert, A. A., Finite Division Algebras and Finite Planes, *Proc. Sympos. Appl. Math.* **10**, American Mathematics Society, Providence, RI (1960), 53-70.

2. Albert, A. A., Non-associative Algebras, I, *Annals of Mathematics.* **43** (1942), 685-707.

3. Burmester, M. V. D., On the commutative non-associative division algebras of even order of L. E. Dickson, *Rendeconte de Matematica e delle sue Applicazioni.* **5** Ser. 21, (1962), 143-166.

4. Dickson, L. E., On commutative linear algebras in which division is always uniquely possible, *Trans. Amer. Math. Soc.* **7**, (1906) 370-390.

5. Hall, M., Jr., *The Theory of Groups*, pp. 346-420. MacMillan, New York, 1959.

6. Isaacs, I. Martin, *Algebra: A Graduate Course.* Brooks/Cole Publishing Company, Pacific Grove, CA, 1994.

7. Jenner, W. E., Lectures on Non-Associative Algebras, *Dept. of Mathematics, UNC Chapel Hill.* (1973).

8. Kleinfeld, E., A History of Finite Semifields, *Finite Geometries: Proc. of a Conference in Honor of T. G. Ostrom.* (1983), 275-277.

9. Knuth, Donald E., Finite Semifields and Projective Planes, *Journal of Algebra.* **2** (1965), 182-217.

10. Lidl, Rudolf and Niederreiter, Harald, *Introduction to Finite Fields and their Applications.* Cambridge University Press, Cambridge, U.K., 1994.

11. Schafer, R. D., *An Introduction to Nonassociative Algebras.* Academic Press, New York, 1966.

12. Wene, G. P., Semifields of dimension $2n$, $n \geq 3$, over $GF(p^m)$ that have left primitive elements, *Geom. Dedicata.* **41** (1992), no. 1, 1-3.

Vita

Eric J. Landquist was born on January 11, 1978 in Worcester, MA to Gary and Dianne Landquist and spent most of his childhood years growing up in Rutland, MA. He graduated from Massachusetts Academy of Mathematics and Science in May, 1996 and enrolled at Virginia Tech that fall. He earned a Bachelor of Science in Mathematics under the Applied Discrete Mathematics option in December, 1998 with a minor in Computer Science. He continued at Virginia Tech to pursue a Master of Science degree in Mathematics, which he earned in May, 2000. His current plan is to stay in the Blacksburg area to teach for a year before pursuing a PhD in Mathematics.