2016-01-01

Twenty-Seven Element Albertian Semifields

Thomas Joel Hughes
University of Texas at El Paso, tjhughes2@miners.utep.edu

Twenty-Seven Element Albertian Semifields

THOMAS HUGHES

Master's Program in Mathematical Sciences

APPROVED:

Piotr Wojciechowski, Ph.D., Chair

Emil Schwab, Ph.D.

Vladik Kreinovich, Ph.D.

Charles Ambler, Ph.D.
Dean of the Graduate School

Twenty-Seven Element Albertian Semifields

by

THOMAS HUGHES

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE

Master's Program in Mathematical Sciences

THE UNIVERSITY OF TEXAS AT EL PASO

December 2016

Acknowledgements

First and foremost, I'd like to acknowledge and thank my advisor Dr. Piotr Wojciechowski, who inspired me to pursue serious studies in mathematics and encouraged me to take on this topic. I'd like also to acknowledge and thank Matthew Wojciechowski, from the Department of Computer Science at Ohio State University, whose help and collaboration on developing a program and interface, which found semifields and their respective 2-periodic bases, made it possible to obtain some of the crucial results in this thesis. Finally, I'd like to acknowledge everyone in The Department of Mathematical Sciences at The University of Texas of El Paso, whose insight, expertise, and great help has made this work possible.

Abstract

In 1958 Abraham Adrian Albert published his findings on the now famous class of semifields known as twisted fields [3] or, as we refer to them in this thesis, Albertian semifields. Since the publication of his findings, interest in the topic of semifields has grown and, naturally, some progress has been made in the subject, but there is still much to be studied. Moreover, the greater portion of modern efforts have been made to develop a theory of semifields, with less attention paid to more practical considerations. In this thesis, we will narrow our investigations to a specific subclass of Albert's semifields, namely, those that contain exactly twenty-seven elements. We will derive the specific equations used to compute products in the semifields of this subclass, and construct multiplication tables for both a basis of the semifield, as well as for the twenty-seven element semifield entire. Lastly, we will demonstrate that, in fact, there are only four such semifields which are unique up to an isomorphism.

Contents

Chapter 1

Introduction

1.1 Semifields

In this section we will define a semifield and cover some basic related concepts. In keeping with a more modern approach, we will rely heavily on Knuth's introduction to the topic [9].

Definition 1.1.1. *A semifield is a set S with two binary operations called addition and multiplication that satisfy the following axioms:*

1. *S is an abelian group with respect to addition with identity element 0.*
2. *For $a \neq 0$ the equations $ax = b$ and $ya = b$ are both uniquely solvable for x and y.*
3. *$a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.*
4. *There is an element 1 in S such that $1 \cdot a = a \cdot 1 = a$.*

Notice it follows from this definition that every field is also a semifield. Thus, by *proper semifield* we mean a semifield which is not also a field; in particular, that there exist elements a, b, c such that $a \cdot (b \cdot c) \neq (a \cdot b) \cdot c$. In this thesis, we will be considering only finite semifields and so the above general axioms, can be slightly relaxed. In particular, axiom 2 can be replaced with a weaker statement as we demonstrate now

Proposition 1.1.1. *If S is finite, satisfies the semifield axioms 1, 3, and 4, and has no zero divisors, then S is a semifield.*

Proof. Let $a \neq 0 \in S$ and define $\phi : S \to S$ in the following way

$$\phi(x) = xa$$

Now consider

$$\phi(x_1) = \phi(x_2)$$

$$x_1 a = x_2 a$$

and so by axiom 1 we have

$$x_1 a - x_2 a = 0$$

and by axiom 3 we have

$$(x_1 - x_2)a = 0$$

and since S has no zero divisors and $a \neq 0$, it follows that

$$x_1 = x_2$$

therefore, ϕ is injective. Since S is finite, it therefore follows that ϕ is a bijection. Thus there always exists a unique x satisfying

$$\phi(x) = y$$

$$xa = y$$

Furthermore, an extremely similar argument shows that, for $a \neq 0 \in S$ there always exists a unique x satisfying

$$ax = y$$

Thus we get that when $a \neq 0 \in S$ the equations $ax = b$ and $ya = b$ are both uniquely solvable for x and y. Therefore S is a semifield. □

Thus, for a finite semifield, S, we can replace axiom 2 with the weaker statement that S has no zero divisors. This substitution will be exploited throughout this thesis.

Definition 1.1.2. *We say S is a pre-semifield if it satisfies all the axioms for a semifield, except possibly 4.*

We now make a crucial observation relating semifields and vector spaces. If we let S be a finite semifield, and let $\mathbb{F}$ be the field $GF(p)$, where p is the characteristic of S, then we can consider the elements of $\mathbb{F}$ to be scalars and S is a vector space over $\mathbb{F}$ [5]. In particular, scalar multiplication would give, for $\alpha \in \mathbb{F}$ and $v \in S$

$$\alpha v \to \underbrace{v + v + \ldots + v}_{\alpha - times}$$

To be sure, S will have p^n elements where n is the dimension of S over $\mathbb{F}$. In fact, historically, semifields went by several different names which were suggestive of this relationship, such as "nonassociative division ring" and "nonassociative division algebra"[3, 7].

This correspondence between semifields and vector spaces is especially important here, for if we consider a finite semifield S as a vector space over a field $\mathbb{F}$ it first follows that this vector space must be finite-dimensional. Let $\{v_1, v_2, \ldots, v_n\}$ be a basis of S over $\mathbb{F}$. Then if we take $x, y \in S$ such that $x = a_1v_1 + a_2v_2 + \ldots + a_nv_n$ and $y = a'_1v_1 + a'_2v_2 + \ldots + a'_nv_n$ then computing the product $x \cdot y$ in S yields

$$\begin{aligned} x \cdot y &= (a_1v_1 + a_2v_2 + \ldots + a_nv_n) \cdot (a'_1v_1 + a'_2v_2 + \ldots + a'_nv_n) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} (a_i a'_j) v_i \cdot v_j \end{aligned}$$

which therefore implies that determining the products $v_i \cdot v_j$ will be enough to define multiplication in S completely. That is, we can determine products in S simply by procuring all the products on the basis.

Finally, this introduction to the topic of finite semifields would be remiss without a brief mention on the least finite semifield. In fact, Knuth [9] has shown that, indeed, any finite semifield must contain at least 16 elements. Thus the family of sixteen-element finite semifields is the family of smallest finite semifields. Examples of such semifields can be found in Knuth's *Finite Semifields and Projective Planes*[9] and work from Cordero and Wene [6].

1.2 Preliminaries

In this section we will present some well-known theorems which will be used, either explicitly or tacitly, later on.

Theorem 1.2.1. *[5] The multiplicative group of all nonzero elements of a finite field is cyclic.*

Theorem 1.2.2. *[1] If $\mathscr{R}$ is a field with characteristic p then*

$$(x+y)^p = x^p + y^p$$

Theorem 1.2.3. *[4] A finite field $\mathscr{R}$ has p^n elements where p is prime.*

Theorem 1.2.4. *[4] If p is a prime and n is a positive integer, then there exists a field of cardinality p^n, and every two such fields are isomorphic.*

Theorem 1.2.5. *[5] The quotient ring $\mathscr{R}/\mathfrak{a}$ is a field if and only if $\mathfrak{a}$ is a maximal ideal.*

Theorem 1.2.6. *[5] If $p \in \mathbb{Z}_p[x]$ is a polynomial irreducible in $\mathbb{Z}_p$, then the principal ideal generated by p, $\langle p \rangle$, is a maximal ideal.*

Chapter 2

Albert's Construction

In this chapter we will go over the construction of the class of finite semifields discovered by Albert [3]. Whilst detailing the construction of the general class of Albertian semifields, we will concomitantly use the results to derive the materials which will be needed in the construction of the basis multiplication tables for the specific twenty-seven element subclass dealt with in this thesis.

2.1 Introduction

We begin by letting $\mathscr{F}$ be the field of $q = p^m$ elements and $\mathscr{R}$ be the field of degree n over $\mathscr{F}$. We make the assumption that

$$q > 2, \qquad n > 2$$

and select c to be any element of $\mathscr{R}$ such that

$$c \neq -1, \qquad c \neq a^{q-1}$$

for any a in $\mathscr{R}$. Upon developing the correct product, we will find that each $\mathscr{R}$ and c will define a semifield which will be denoted $\mathscr{D}(\mathscr{R}, c)$.

Our investigations will examine the simplest of such semifields. That is, when $q = 3$ and $n = 3$. This means that $\mathscr{F}$ is the field of $q = 3$ elements and $\mathscr{R}$ is the the field of degree 3 over $\mathscr{F}$. Thus, $\mathscr{R}$ is 3-dimensional over $\mathscr{F}$. So there exists a basis, $\{v_1, v_2, v_3\}$, of $\mathscr{R}$ such that, for every $x \in \mathscr{R}$ we have

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 \qquad \text{where } \alpha_i \in \mathscr{F}$$

Since $\alpha_i \in \mathscr{F}$, $|\mathscr{F}| = 3$, and $1 \leq i \leq 3$, it follows that there exist $3^3 = 27$ expressions of the form $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3$. Since $\{v_1, v_2, v_3\}$ is a basis, and therefore expression in $\mathscr{R}$ is unique, it follows that $|\mathscr{R}| = 27$. Thus, by Theorem 1.2.4, in general, we can simply take $\mathscr{R} = GF(p^n)$ and $\mathscr{F} = \mathbb{Z}_p$. Thus, when $q = 3$, we can take $\mathscr{R} = GF(27)$ and $\mathscr{F} = \mathbb{Z}_3$.

Furthermore, considering our selections of c, we refer to the addition and multiplication tables of $\mathscr{R}$, found in Appendix A. We note that the elements of $\mathscr{R}$ are given generic numerical names, 0 through 26, though this does not indicate an order on $\mathscr{R}$ of any kind. We clarify that the additive identity is denoted 0 and the multiplicative identity is denoted 1, per convention. Since $c \neq a^{q-1}$ it follows that $c \neq a^{3-1} = a^2$ for any $a \in \mathscr{R}$. Also $c \neq -1$. That is, c is a valid selection so long as it is not a square and not the additive inverse of the multiplicative identity. A quick glance at our multiplication table reveals that the valid selections for c are as follows

$$c = 3, 5, 8, 10, 11, 12, 18, 21, 22, 23, 25, 26$$

where 2 is omitted since $2 + 1 = 1 + 2 = 0$ making 2 the additive inverse of 1. For this reason, we will often denote 2 by -1.

2.2 The Construction

It will be important to establish some notation presently. We observe that, since $\mathscr{R}$ is a field, it follows that multiplication is commutative and therefore the product on $\mathscr{R}$ satisfies

$$xy = yx$$

From this, we can define a transformation $R_y : \mathscr{R} \to \mathscr{R}$ such that

$$R_y(x) = xy$$

If we denote the space of linear operators on $\mathscr{R}$ by $\mathcal{L}(\mathscr{R})$, then we have the following Proposition.

Proposition 2.2.1. *$R_k \in \mathcal{L}(\mathscr{R})$ and is invertible when $k \neq 0$.*

Proof. Let $k \neq 0$, $\alpha \in \mathscr{R}$ and $x, y \in \mathscr{R}$. Then

$$R_k(x+y) = k(x+y) = kx + ky = R_k(x) + R_k(y)$$

and

$$R_k(\alpha x) = k\alpha x = \alpha k x = \alpha R_k(x)$$

Thus $R_k \in \mathcal{L}(\mathscr{R})$. To show that R_k is invertible, we consider

$$\begin{aligned} R_k(x) &= 0 \\ kx &= 0 \end{aligned}$$

and since $k \neq 0$ and $\mathscr{R}$ is a field, it follows that

$$x = 0$$

Thus $ker(R_k) = \{0\}$. Therefore, R_k is invertible. □

Another important transformation, $S : \mathscr{R} \to \mathscr{R}$, is given by

$$S(x) = x^q$$

Thus, the map S is the well-known Frobenius automorphism [8] on $\mathscr{R}$. In our case, we have chosen $q = 3$, which then means that, for our purposes, we will take $S(x) = x^3$. Since the group of automorphisms on $\mathscr{R}$ are closed under composition, it follows that $\forall\, i \in \mathbb{N}$, $S^i = \underbrace{S \circ S \circ \ldots \circ S}_{i-times}$ is an automorphism. Thus it then follows that

$$\begin{aligned} \left(S^i \circ R_y\right)(x) &= S^i(xy) \\ &= S^i(x) S^i(y) \\ &= \left(R_{S^i(y)} \circ S^i\right)(x) \end{aligned}$$

so that we have

$$S^i \circ R_y = R_{S^i(y)} \circ S^i \tag{2.2.1}$$

Now, if we let $\sigma = 1 + q + q^2 + \ldots + q^{n-1}$ and define $v : \mathscr{R} \to \mathscr{R}$ by

$$v(x) = x^{1+q+q^2+\ldots+q^{n-1}} = x^\sigma$$

then we have, for the case $q = 3$, that $v(x) = x^{1+3+3^2} = x^{1+3+9} = x^{13}$. We will denote $v(c) = c^\sigma = c^{13} = \alpha \in \mathscr{F}$. We now furnish ourselves with a result which will be important later.

Theorem 2.2.1. *$c \neq a^{q-1} \Rightarrow c^\sigma \neq 1$ for any $a \in \mathscr{R}$*

Proof. We proceed with proof by contrapositive. Let $c^\sigma = 1$. Since $c \neq 0$ and the set of all nonzero elements in $\mathscr{R}$ forms a cyclic multiplicative group of order $q^n - 1$ [2], it follows that

$$c = w^\lambda$$

for some generator w. Now since w is a generator it follows that $o(w) = q^n - 1$. Thus,

$$1 = c^\sigma = w^{\sigma\lambda}$$

So then $\sigma\lambda | q^n - 1$. However, since

$$q^n - 1 = (1 + q + q^2 + \ldots + q^{n-1})(q - 1) = \sigma(q - 1)$$

it follows that $\lambda = (q - 1)k$ for some $k \in \mathbb{Z}$, and thus that $q - 1 | \lambda$. Therefore,

$$c = w^\lambda = w^{(q-1)k} = (w^k)^{q-1} = a^{q-1}$$

where $a = w^k$. □

Thus, by our selection of c, we have the following corollary.

Corollary 2.2.1. *$\alpha \neq 1$.*

We are now ready to define a new product which will, in turn, produce a pre-semifield, which we will denote by $\mathscr{R}^*$. We define the product $* : \mathscr{R} \times \mathscr{R} \to \mathscr{R}$ by

$$x * y = xS(y) - cyS(x) = xy^q - cyx^q \tag{2.2.2}$$

Where c is as defined in the above. Thus, for the case $q = 3$, the product formula will be given by

$$x * y = xy^3 - cyx^3 \tag{2.2.3}$$

Then $\mathscr{R}^* = (\mathscr{R}, +, *, 0)$. Before proceeding, we demonstrate that, indeed, $\mathscr{R}^*$ is a pre-semifield. But first,

Lemma 2.2.1. *For every $y \neq 0$ in $\mathscr{R}$ there exists an x such that*

$$yx^q - xy^q \neq 0$$

Proof. We proceed by contradiction. Suppose there exists $y \neq 0 \in \mathscr{R}$ such that for every $x \in \mathscr{R}$ we have

$$yx^q - xy^q = 0$$

If $y \in \mathscr{F}$ it follows that $y^q = y$. Therefore, we get

$$(x^q - x)y = 0$$

Since $y \neq 0$ it follows that we get $x^q - x = 0$ for every $x \in \mathscr{R}$. Therefore, $x^q = x$ for every $x \in \mathscr{R}$. In particular, for $x \notin \mathscr{F}$, contradicting with $S(x) \neq x$ when $x \in \mathscr{R} \setminus \mathscr{F}$ [8]. Now if $y \notin \mathscr{F}$ then, for precisely the same reasons we will have that $y^q \neq y$. But then for $x \neq 0 \in \mathscr{F}$ we will have $x^q = x$ leaving us with

$$x(y^q - y) = 0$$

implying either that $x = 0$ or $y^q = y$ which is a contradiction. Therefore, for every $y \in \mathscr{R}$ such that $y \neq 0$, there exists x such that $yx^q - xy^q \neq 0$. □

Theorem 2.2.2. *$\mathscr{R}^*$ is a pre-semifield*

Proof. Clearly, $\mathscr{R}^*$ is finite and has at least two elements.

1. Since $\mathscr{R}^*$ has the same addition operation as $\mathscr{R}$, it follows that $\mathscr{R}^*$ is an additive abelian group with identity 0.

2. To demonstrate that $\mathscr{R}^*$ has no zero divisors, we suppose, to the the contrary, that there are $x, y \neq 0$ such that $x * y = 0$. So, by (2.2.2), we have

$$\begin{aligned} 0 &= xy^q - cyx^q \\ cyx^q &= xy^q \\ c &= xy^q x^{-q} y^{-1} \\ c &= y^{q-1} x^{-(q-1)} \\ c &= (yx^{-1})^{q-1} \end{aligned}$$

   which is contrary to our assumption that $c \neq a^{q-1}$ for any a. Thus whenever $x * y = 0$ we must have that either $x = 0$ or $y = 0$.

3. To demonstrate distributivity, we compute

$$x * (y + z) = xS(y + z) - c(y + z)S(x)$$

   and since S is an automorphism,

$$\begin{aligned} &= xS(y) + xS(z) - cyS(x) - czS(x) \\ &= (xS(y) - cyS(x)) + (xS(z) - czS(x)) \\ &= (x * z) + (x * z) \end{aligned}$$

   and also

$$\begin{aligned} (x + y) * z &= (x + y)S(z) - czS(x + y) \\ &= xS(z) + yS(z) - czS(x) - czS(y) \\ &= (xS(z) - czS(x)) + (yS(z) - czS(y)) \\ &= (x * z) + (y * z) \end{aligned}$$

Which establishes that $*$ is distributive over addition.

□

Remark. $p^q - p \neq 0$ [2]

Proposition 2.2.2. *$\mathscr{R}^*$ is noncommutative.*

Proof. We claim $p * 1 \neq 1 * p$. Suppose to the contrary, then we should have

$$\begin{aligned} p * 1 &= 1 * p \\ p1^q - c1p^q &= 1p^q - cp1^q \\ p - cp^q &= p^q - cp \\ p - p^q &= cp^q - cp \\ p - p^q &= c(p^q - p) \end{aligned}$$

which, following from our previous remark, gives us

$$\begin{aligned} (p - p^q)(-(p - p^q))^{-1} &= c \\ -1 &= c \end{aligned}$$

contrary to our choice $c \neq -1$. □

In fact, we can generalize this proof to make an even stronger claim.

Proposition 2.2.3. *There does not exist $y \neq 0 \in \mathscr{R}^*$ that commutes with every element in $\mathscr{R}^*$.*

Proof. We suppose, to the contrary, that there exists $y \neq 0 \in \mathscr{R}^*$ such that for every $x \in \mathscr{R}^*$ we must have

$$x * y = y * x$$

In particular, the above must hold for x such that $yx^q - xy^q \neq 0$, whose existence follows from Lemma 2.2.1. But then

$$\begin{aligned} xy^q - cyx^q &= yx^q - cxy^q \\ xy^q - yx^q &= cyx^q - cxy^q \\ xy^q - yx^q &= c(yx^q - xy^q) \\ (xy^q - yx^q)(-(xy^q - yx^q))^{-1} &= c \\ -1 &= c \end{aligned}$$

which contradicts with our choice of $c \neq -1$. □

Corollary 2.2.2. *$\mathscr{R}^*$ does not have an identity element*

Proof. An identity in $\mathscr{R}^*$ would have to commute with every element in $\mathscr{R}^*$. □

Now, following from (2.2.2), we define $R_y^* : \mathscr{R} \to \mathscr{R}$ and $L_x^* : \mathscr{R} \to \mathscr{R}$ by

$$R_y^* = R_{S(y)} - (R_{cy} \circ S), \qquad L_x^* = (R_x \circ S) - R_{cS(x)} \tag{2.2.4}$$

Proposition 2.2.4. *$R_y^*, L_x^* \in \mathcal{L}(\mathscr{R})$ are invertible when $y, x \neq 0$ respectively.*

Proof. Since S is an automorphism, it follows that it is invertible and is linear. Furthermore, since $y, x \neq 0$, it follows from Proposition 2.2.1 that $R_{S(y)}, R_{cy}, R_x, R_{cS(x)} \in \mathcal{L}(\mathscr{R})$. It immediately follows that $R_y^*, L_x^* \in \mathcal{L}(\mathscr{R})$. To show invertibility, we simply observe that since $\mathscr{R}^*$ has no zero divisors and $x, y \neq 0$, it follows

$$R_y^*(z) = z * y = 0 \iff z = 0$$

and

$$L_x^*(z) = x * z \iff z = 0$$

which shows that both R_y^* and L_x^* have trivial kernels, which implies that they are invertible.

□

Let

$$f = e * e = e - c \tag{2.2.5}$$

Now, for reasons which will soon become clear, we define

$$P = (R_e^*)^{-1} = (I - (R_c \circ S))^{-1} \tag{2.2.6}$$

and

$$Q = (L_e^*)^{-1} = (S - R_c)^{-1} \tag{2.2.7}$$

In particular, for $q = 3$, we have

$$P^{-1}(x) = x - cx^3, \quad Q^{-1}(y) = y^3 - cy$$

So, by (2.2.5) we have

$$P^{-1}(e) = R_e^*(e) = f$$

and

$$Q^{-1}(e) = L_e^*(e) = f$$

implying that

$$P(f) = Q(f) = (S \circ P)(f) = (S \circ Q)(f) = e \tag{2.2.8}$$

We are now ready to begin constructing Albert's semifield, which we denoted $\mathscr{D}(\mathscr{R}, c)$. We will define the product on this space by $\cdot : \mathscr{R} \times \mathscr{R} \to \mathscr{R}$

$$x \cdot y = P(x) * Q(y) = P(x)\left[(S \circ Q)(y)\right] - cQ(y)\left[(S \circ P)(x)\right] \tag{2.2.9}$$

Then $\mathscr{D}(\mathscr{R}, c) = (\mathscr{R}, +, \cdot)$ is a finite semifield which we demonstrate now.

Theorem 2.2.3. *$\mathscr{D}(\mathscr{R}, c)$ is a finite semifield with unity element $f = e - c$.*

Proof. It is obvious that $\mathscr{D}(\mathscr{R}, c)$ is finite and has at least two elements.

1. By definition, addition in $\mathscr{D}(\mathscr{R}, c)$ agrees with addition in $\mathscr{R}$. Therefore, addition forms an abelian group with identity element 0.

2. To show that $\mathscr{D}(\mathscr{R}, c)$ has no zero divisors we suppose, to the contrary, that $x, y \neq 0$ and $x \cdot y = 0$. But then we get

$$P(x) * Q(y) = 0$$

Since, by Theorem 2.2.2, we have already demonstrated that $\mathscr{R}^*$ has no zero divisors, it follows that $P(x) = 0$ or $Q(y) = 0$. However since, by Proposition 2.2.4, both P and Q are invertible, they must have trivial kernels. Therefore, either $x = 0$ or $y = 0$ as desired.

3. To show that multiplication in $\mathscr{D}(\mathscr{R}, c)$ is distributive, we observe that since S, Q, and P are all linear transformations it follows that

$$\begin{aligned}
x \cdot (y + z) &= P(x) * Q(y + z) \\
&= P(x)\,[(S \circ Q)(y + z)] - cQ(y + z)\,[(S \circ P)(x)] \\
&= P(x)\,[(S \circ Q)(y) + (S \circ Q)(z)] \\
&\quad - c\,[Q(y) + Q(z)]\,[(S \circ P)(x)] \\
&= P(x)\,[(S \circ Q)(y)] - cQ(y)\,[(S \circ P)(x)] \\
&\quad + P(x)\,[(S \circ Q)(z)] - cQ(z)\,[(S \circ P)(z)] \\
&= x \cdot y + x \cdot z
\end{aligned}$$

Also,

$$\begin{aligned}(x+y)\cdot z &= P(x+y) * Q(z)\\ &= P(x+y)\left[(S\circ Q)(z)\right]\\ &- cQ(z)\left[(S\circ P)(x+y)\right]\\ &= \left[P(x)+P(y)\right]\left[(S\circ Q)(z)\right]\\ &- cQ(z)\left[(S\circ P)(x)+(S\circ P)(y)\right]\\ &= P(x)\left[(S\circ Q)(z)\right] - cQ(z)\left[(S\circ P)(x)\right]\\ &+ P(y)\left[(S\circ Q)(z)\right] - cQ(z)\left[(S\circ P)(y)\right]\\ &= x\cdot z + y\cdot z\end{aligned}$$

which then establishes distributivity over addition.

4. Finally, to establish that f is the unity element of $\mathscr{D}(\mathscr{R}, c)$ we compute

$$\begin{aligned}f\cdot y &= P(f) * Q(y)\\ &= e * Q(y)\end{aligned}$$

by (2.2.4) we get

$$= L_e^*(Q(y))$$

and by (2.2.7)

$$\begin{aligned}&= Q^{-1}(Q(y))\\ &= y\end{aligned}$$

Also,

$$\begin{aligned}x\cdot f &= P(x) * Q(f)\\ &= P(x) * e\\ &= R_e^*(P(x))\end{aligned}$$

and by (2.2.6)

$$= P^{-1}(P(x))$$

$$= x$$

Therefore, f is the identity element of $\mathscr{D}(\mathscr{R}, c)$.

□

It has been shown by Albert that, indeed when $c \neq -1, a^{q-1}$, $\mathscr{D}(\mathscr{R}, c)$ is non-commutative [3]. Now it should seem that our work is still incomplete, for we are still in want of expressions for P and Q, for without these, it would be impossible to compute products in $\mathscr{D}(\mathscr{R}, c)$ directly.

2.3 Formulas for P and Q

We define, for $1 \leq i \leq n$

$$c_i = cS(c)S^2(c)\dots S^{i-1}(c) = c^{1+q+q^2+\dots+q^{i-1}}$$

which then implies the recursive equalities

$$c_{i+1} = S(c_i)c = c_i S^i(c) \tag{2.3.1}$$

Before we proceed, we demonstrate a few important propositions. We let I denote the identity transformation.

Proposition 2.3.1. $S^n = I$

Proof.

$$S^n(x) = x^{q^n}$$

and by Fermat's Little Theorem

$$= x$$

and thus

$$S^n = I$$

□

We recall that $\alpha = c^{1+q+q^2+\ldots+q^{n-1}}$.

Proposition 2.3.2. $c_n = \alpha$

Proof.

$$\begin{aligned} c_n &= cS(c)S^2(c)\ldots S^{n-1}(c) \\ &= c\, c^q\, c^{q^2} \ldots c^{q^{n-1}} \\ &= c^{1+q+q^2+\ldots+q^{n-1}} \\ &= c^{\sigma} \\ &= \alpha \end{aligned}$$

□

Proposition 2.3.3. $(R_c \circ S)^i = R_{c_i} \circ S^i$

Proof. We proceed with induction. If $i = 1$, then

$$(R_c \circ S)^1 = R_c \circ S$$

is clearly true. Now, let the claim hold for i. We calculate

$$(R_c \circ S)^{i+1} = (R_c \circ S) \circ (R_c \circ S)^i$$

by the inductive hypothesis, we get

$$\begin{aligned} &= (R_c \circ S) \circ (R_{c_i} \circ S^i) \\ &= R_c \circ (S \circ R_{c_i}) \circ S^i \end{aligned}$$

and by (2.2.1), it follows

$$= (R_c \circ R_{S(c_i)}) \circ (S \circ S^i)$$
$$= R_{cS(c_i)} \circ S^{i+1}$$

and by (2.3.1), it follows

$$= R_{c_{i+1}} \circ S^{i+1}$$

as desired. □

Corollary 2.3.1. $(R_c \circ S)^n = \alpha I$

Proof. By Proposition 2.3.3, we have

$$(R_c \circ S)^n = R_{c_n} \circ S^n$$

and by propositions (2.3.1) and (2.3.2), it follows that

$$= R_\alpha \circ I$$
$$= \alpha I$$

□

Now, if $T \in \mathcal{L}(\mathscr{R})$, then we have the relation

$$I^n - T^n = (I - T) \circ (I + T + T^2 + \ldots + T^{n-1})$$

So, if we take $T = R_c \circ S$, then by our Corollary 2.3.1 we get that

$$(I - (R_c \circ S)) \circ (I + (R_c \circ S) + (R_c \circ S)^2 + \ldots + (R_c \circ S)^{n-1}) = I^n - (R_c \circ S)^n$$
$$= I - (R_c \circ S)^n$$
$$= I - \alpha I$$
$$= (1 - \alpha)I$$

Thus, since $P^{-1} = I - R_c \circ S$, it follows that

Corollary 2.3.2. $(1-\alpha)P = I + (R_{c_1} \circ S) + (R_{c_2} \circ S^2) + \ldots + (R_{c_{n-1}} \circ S^{n-1})$

We note that from corollary (2.2.1) we have

$$P = (1-\alpha)^{-1}(I + (R_{c_1} \circ S) + (R_{c_2} \circ S^2) + \ldots + (R_{c_{n-1}} \circ S^{n-1}))$$

To get Q, we first demonstrate a necessary result.

Proposition 2.3.4. $S^{n-(i+1)}(c_i) = S^{n-i}(c_i)S^{n-(i+1)}(c)$

Proof. So, by (2.3.1), we have

$$S^{n-(i+1)}(c_i) = S^{n-(i+1)}(S(c_i)c)$$

and since $S^{n-(i+1)}$ is an automorphism, we have

$$\begin{aligned} &= (S^{n-(i+1)} \circ S)(c_i)S^{n-(i+1)}(c) \\ &= S^{n-i}(c_i)S^{n-(i+1)}(c) \end{aligned}$$

□

Corollary 2.3.3. $R_{S^{n-i}(c_i)} \circ R_{S^{n-(i+1)}(c_1)} = R_{S^{n-(i+1)}(c_i)}$

Theorem 2.3.1.

$$(1-\alpha)Q = S^{n-1} + (R_{S^{n-1}(c_1)} \circ S^{n-2}) + (R_{S^{n-2}(c_2)} \circ S^{n-3}) + \ldots + R_{S(c_{n-1})}$$

Proof. By composing the right hand side of the claimed equation with Q^{-1} we obtain

$$\begin{aligned} \left(S^{n-1} + (R_{S^{n-1}(c_1)} \circ S^{n-2}) + (R_{S^{n-2}(c_2)} \circ S^{n-3}) + \ldots + R_{S(c_{n-1})}\right) \circ \left(Q^{-1}\right) = \\ \left(S^{n-1} + (R_{S^{n-1}(c_1)} \circ S^{n-2}) + (R_{S^{n-2}(c_2)} \circ S^{n-3}) + \ldots + R_{S(c_{n-1})}\right) \circ (S - R_c) = \end{aligned}$$

and by (2.2.1), we get,

$$\begin{aligned} S^n + \left(R_{S^{n-1}(c_1)} \circ S^{n-1}\right) + \left(R_{S^{n-2}(c_2)} \circ S^{n-2}\right) + \ldots + \left(R_{S(c_{n-1})} \circ S\right) \\ - \left(R_{S^{n-1}(c)} \circ S^{n-1}\right) - \left(R_{S^{n-1}(c_1)} \circ R_{S^{n-2}(c_1)} \circ S^{n-2}\right) - \left(R_{S^{n-2}(c_2)} \circ R_{S^{n-1}(c_1)} \circ S^{n-3}\right) \\ - \ldots - \left(R_{S(c_{n-1})} \circ R_{c_1}\right) = \end{aligned}$$

and by Proposition (2.3.1) and Corollary (2.3.3), it follows that we have

$$\begin{aligned} I + \left(R_{S^{n-1}(c_1)} \circ S^{n-1}\right) + \left(R_{S^{n-2}(c_2)} \circ S^{n-2}\right) + \ldots + \left(R_{S(c_{n-1})} \circ S\right) \\ - \left(R_{S^{n-1}(c)} \circ S^{n-1}\right) - \left(R_{S^{n-2}(c_2)} \circ S^{n-2}\right) - \left(R_{S^{n-3}(c_3)} \circ S^{n-3}\right) \\ - \ldots - \left(R_{S(c_{n-1})} \circ R_{c_1}\right) = \end{aligned}$$

which reduces to

$$I - \left(R_{S(c_{n-1})} \circ R_{c_1}\right) =$$

and by (2.3.1) and Proposition 2.3.2 we get

$$I - \alpha I =$$

which implies the desired result. □

It is possible to express both $S \circ P$ and $S \circ Q$ as in Corollary (2.3.2) and Theorem (2.3.1). However, since we are primarily interested in computation, it will be, for our purposes, superfluous. Therefore, with regard to their derivations, we simply refer to Albert's text [3].

Chapter 3

Albertian Twenty-Seven Element Semifields

Now, having gone through the necessary construction, we will present our results. Our primary aim is to present the 3×3 basis tables for multiplication. We begin by gathering some results from the previous chapter.

We recall that, from our construction, we set $q = 3$ and $n = 3$, resulting in the field $\mathscr{R} = GF(27)$. Our possible selections of c (which was defined at the beginning of Chapter 2 Section 1) are given by

$$c = 3, 5, 8, 10, 11, 12, 18, 21, 22, 23, 25, 26$$

and therefore, we will have up to twelve semifields, which we denoted $\mathscr{D}(\mathscr{R}, c)$. As noted earlier, we have

$$\alpha = c^{13} \tag{3.0.1}$$

Following from our choice of q and n, the resultant general expressions for the transformations P and Q are as follows.

$$P = (1 - c^{13})^{-1}(I + (R_{c_1} \circ S) + (R_{c_2} \circ S^2)) \tag{3.0.2}$$

and

$$Q = (1 - c^{13})^{-1}(S^2 + (R_{S^2(c_1)} \circ S) + R_{S(c_2)}) \tag{3.0.3}$$

where c_1, c_2 were as defined in (2.3.1). To help provide context to the following results, we will use $\mathscr{D}(\mathscr{R}, 3)$ as an example to demonstrate some of the computational methods (see

also Appendix A and B) used in the derivation of our tables. All proceeding results can be derived analogously and, therefore, their details will be omitted.

3.1 The Semifields

3.1.1 $\mathscr{D}(\mathscr{R}, 3)$

We first compute

$$c_1 = 3, \quad c_2 = 3S(3) = 3(3^3) = 3^4 = 17, \quad c_3 = \alpha = 3^{13} = -1 \tag{3.1.1}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Since $(-1)(-1) = 1$ it follows that $(1-(-1))^{-1} = -1$. Thus, from (3.0.2), we get that

$$P = -I - (R_3 \circ S) - (R_{17} \circ S^2) \tag{3.1.2}$$

We also compute

$$\begin{aligned} S^2(c_1) &= S(S(3)) \\ &= S(3^3) \\ &= S(11) \\ &= 11^3 \\ &= 26 \end{aligned}$$

and

$$\begin{aligned} S(c_2) &= S(17) \\ &= 17^3 \\ &= 15 \end{aligned}$$

Thus, from (3.0.3),

$$Q = -S^2 - (R_{26} \circ S) - R_{15} \tag{3.1.3}$$

We also find that, by Theorem (2.2.3), $f = e - c = 1 - 3 = 7$ is the identity of $\mathscr{D}(\mathscr{R}, 3)$. It is then a simple matter of computation to verify that $\{7, 2, 21\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 7$, $u = 2$, and $v = 21$, we proceed with computing values for our table. We first obtain

$$\begin{aligned} P(7) &= -I(7) - (R_3 \circ S)(7) - (R_{17} \circ S^2)(7) \\ &= -7 - R_3(S(7)) - R_{17}(S^2(7)) \\ &= -7 - R_3(20) - R_{17}(14) \\ &= -7 - 25 - 15 \\ &= 5 + 14 + 21 \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} Q(7) &= -S^2(7) - (R_{26} \circ S)(7) - R_{15}(7) \\ &= -S(S(7)) - R_{26}(S(7)) - R_{15}(7) \\ &= -S(20) - R_{26}(20) - 16 \\ &= -14 - 11 - 16 \\ &= 25 + 19 + 23 \\ &= 1 \end{aligned}$$

and

$$\begin{aligned} P(2) &= -I(2) - (R_3 \circ S)(2) - (R_{17} \circ S^2)(2) \\ &= -2 - R_3(S(2)) - R_{17}(S^2(2)) \\ &= -2 - R_3(2) - R_{17}(2) \\ &= -2 - 6 - 22 \\ &= 1 + 3 + 17 \\ &= 9 \end{aligned}$$

and

$$\begin{aligned} Q(2) &= -S^2(2) - (R_{26} \circ S)(2) - R_{15}(2) \\ &= -S(S(2)) - R_{26}(S(2)) - R_{15}(2) \\ &= -S(2) - R_{26}(2) - 21 \\ &= -2 - 13 - 21 \\ &= 1 + 26 + 15 \\ &= 3 \end{aligned}$$

and

$$\begin{aligned} P(21) &= -I(21) - (R_3 \circ S)(21) - (R_{17} \circ S^2)(21) \\ &= -21 - R_3(S(21)) - R_{17}(S^2(21)) \\ &= -21 - R_3(23) - R_{17}(22) \\ &= -21 - 7 - 25 \\ &= 15 + 5 + 14 \\ &= 22 \end{aligned}$$

and

$$\begin{aligned} Q(21) &= -S^2(21) - (R_{26} \circ S)(21) - R_{15}(21) \\ &= -S(S(21)) - R_{26}(S(21)) - R_{15}(21) \\ &= -S(23) - R_{26}(23) - R_{15}(21) \\ &= -22 - 24 - 5 \\ &= 17 + 12 + 7 \\ &= 24 \end{aligned}$$

Thus we compute the following products

$$\begin{aligned} e \cdot e &= 7 \cdot 7 \\ &= P(7) * Q(7) \\ &= 1 * 1 \\ &= 1(1)^3 - 3(1)(1)^3 \\ &= 1 - 3 \\ &= 7 \\ &= e \end{aligned}$$

and

$$\begin{aligned} e \cdot u &= 7 \cdot 2 \\ &= P(7) * Q(2) \\ &= 1 * 3 \\ &= 1(3)^3 - 3(3)(1)^3 \\ &= 1(11) - 9(1)^3 \\ &= 11 - 9 \\ &= 11 + 18 \\ &= 2 \\ &= u \end{aligned}$$

and

$$\begin{aligned} e \cdot v &= 7 \cdot 21 \\ &= P(7) * Q(21) \\ &= 1 * 24 \\ &= 1(24)^3 - 3(24)(1)^3 \\ &= 4 - 10 \\ &= 4 + 20 \\ &= 21 \\ &= v \end{aligned}$$

and

$$\begin{aligned} u \cdot e &= 2 \cdot 7 \\ &= P(2) * Q(7) \\ &= 9 * 1 \\ &= 9(1)^3 - 3(1)(9)^3 \\ &= 9 - 3(24) \\ &= 9 - 10 \\ &= 9 + 20 \\ &= 2 \\ &= u \end{aligned}$$

and

$$\begin{aligned} u \cdot u &= 2 \cdot 2 \\ &= P(2) * Q(2) \\ &= 9 * 3 \\ &= 9(3)^3 - 3(3)(9)^3 \\ &= 9(11) - (9)(24) \\ &= 8 - 14 \\ &= 8 + 25 \\ &= 21 \\ &= v \end{aligned}$$

and

$$\begin{aligned} u \cdot v &= 2 \cdot 21 \\ &= P(2) * Q(21) \\ &= 9 * 24 \\ &= 9(24)^3 - 3(24)(9)^3 \\ &= 9(4) - 3(15) \\ &= 20 - 2 \\ &= 20 + 1 \\ &= 18 \\ &= 7 + 2 + 21 \\ &= e + u + v \end{aligned}$$

and

$$\begin{aligned} v \cdot e &= 21 \cdot 7 \\ &= P(21) * Q(7) \\ &= 22 * 1 \\ &= 22(1)^3 - 3(1)(22)^3 \\ &= 22 - 3(21) \\ &= 22 - 1 \\ &= 22 + 2 \\ &= 21 \\ &= v \end{aligned}$$

and

$$\begin{aligned} v \cdot u &= 21 \cdot 2 \\ &= P(21) * Q(2) \\ &= 22 * 3 \\ &= 22(3)^3 - 3(3)(22)^3 \\ &= 22(11) - 9(21) \\ &= 20 - 3 \\ &= 20 + 6 \\ &= 26 \\ &= 5 + 21 \\ &= -7 + 21 \\ &= -e + v \end{aligned}$$

and

$$\begin{aligned} v \cdot v &= 21 \cdot 21 \\ &= P(21) * Q(21) \\ &= 22 * 24 \\ &= 22(24)^3 - 3(24)(22)^3 \\ &= 22(4) - 10(21) \\ &= 26 - 24 \\ &= 26 + 12 \\ &= 2 \\ &= u \end{aligned}$$

Thus, together, these products produce the following table

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e+u+v$
v	v	$-e+v$	u

3.1.2 $\mathscr{D}(\mathscr{R}, 5)$

We first compute

$$c_1 = 5, \quad c_2 = 5S(5) = 5(5^3) = 5^4 = 4, \quad c_3 = \alpha = 5^{13} = -1 \tag{3.1.4}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_5 \circ S) - (R_4 \circ S^2) \tag{3.1.5}$$

and

$$Q = -S^2 - (R_{25} \circ S) - (R_9) \tag{3.1.6}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 5 = 8$ is the identity of $\mathscr{D}(\mathscr{R}, 5)$. It is then a simple matter of computation to verify that $\{8, 2, 22\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 8$, $u = 2$, and $v = 22$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e - u - v$
v	v	$-e + u - v$	u

3.1.3 $\mathscr{D}(\mathscr{R}, 8)$

We first compute

$$c_1 = 8, \quad c_2 = 8S(8) = 8(8^3) = 8^4 = 20, \quad c_3 = \alpha = 8^{13} = -1 \tag{3.1.7}$$

Then $(1 - \alpha) = (1 - (-1)) = 1 + 1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_8 \circ S) - (R_{20} \circ S^2) \tag{3.1.8}$$

and

$$Q = -S^2 - (R_{12} \circ S) - (R_{14}) \tag{3.1.9}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 8 = 5$ is the identity of $\mathscr{D}(\mathscr{R}, 8)$. It is then a simple matter of computation to verify that $\{5, 10, 23\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 5$, $u = 10$, and $v = 23$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e+u$
v	v	$-e-u+v$	u

3.1.4 $\mathscr{D}(\mathscr{R}, 10)$

We first compute

$$c_1 = 10, \quad c_2 = 10S(10) = 10(10^3) = 10^4 = 9, \quad c_3 = \alpha = 10^{13} = -1 \tag{3.1.10}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{10} \circ S) - (R_9 \circ S^2) \tag{3.1.11}$$

and

$$Q = -S^2 - (R_5 \circ S) - (R_{24}) \tag{3.1.12}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 10 = 18$ is the identity of $\mathscr{D}(\mathscr{R}, 10)$. It is then a simple matter of computation to verify that $\{18, 2, 21\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 18$, $u = 2$, and $v = 21$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e-u-v$
v	v	$-e+u-v$	u

3.1.5 $\mathscr{D}(\mathscr{R}, 11)$

We first compute

$$c_1 = 11, \quad c_2 = 11S(11) = 11(11^3) = 11^4 = 15, \quad c_3 = \alpha = 11^{13} = -1 \tag{3.1.13}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{11} \circ S) - (R_{15} \circ S^2) \tag{3.1.14}$$

and

$$Q = -S^2 - (R_3 \circ S) - (R_{16}) \tag{3.1.15}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 11 = 20$ is the identity of $\mathscr{D}(\mathscr{R}, 11)$. It is then a simple matter of computation to verify that $\{20, 2, 23\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 20$, $u = 2$, and $v = 23$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e+u+v$
v	v	$-e+v$	u

3.1.6 $\mathscr{D}(\mathscr{R}, 12)$

We first compute

$$c_1 = 12, \quad c_2 = 12S(12) = 12(12^3) = 12^4 = 7, \quad c_3 = \alpha = 12^{13} = -1 \tag{3.1.16}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{12} \circ S) - (R_7 \circ S^2) \tag{3.1.17}$$

and

$$Q = -S^2 - (R_{18} \circ S) - (R_{20}) \tag{3.1.18}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 12 = 25$ is the identity of $\mathscr{D}(\mathscr{R}, 12)$. It is then a simple matter of computation to verify that $\{25, 5, 21\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 25$, $u = 5$, and $v = 21$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e + u$
v	v	$-e - u + v$	u

3.1.7 $\mathscr{D}(\mathscr{R}, 18)$

We first compute

$$c_1 = 18, \quad c_2 = 18S(18) = 18(18^3) = 18^4 = 14, \quad c_3 = \alpha = 18^{13} = -1 \tag{3.1.19}$$

Then $(1 - \alpha) = (1 - (-1)) = 1 + 1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{18} \circ S) - (R_{14} \circ S^2) \tag{3.1.20}$$

and

$$Q = -S^2 - (R_8 \circ S) - (R_7) \tag{3.1.21}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 18 = 10$ is the identity of $\mathscr{D}(\mathscr{R}, 18)$. It is then a simple matter of computation to verify that $\{10, 25, 22\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 10$, $u = 25$, and $v = 22$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e+u$
v	v	$-e-u+v$	u

3.1.8 $\mathscr{D}(\mathscr{R}, 21)$

We first compute

$$c_1 = 21, \quad c_2 = 21S(21) = 21(21^3) = 21^4 = 13, \quad c_3 = \alpha = 21^{13} = -1 \tag{3.1.22}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{21} \circ S) - (R_{13} \circ S^2) \tag{3.1.23}$$

and

$$Q = -S^2 - (R_{22} \circ S) - (R_6) \tag{3.1.24}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 21 = 16$ is the identity of $\mathscr{D}(\mathscr{R}, 21)$. It is then a simple matter of computation to verify that $\{16, 5, 21\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 16$, $u = 5$, and $v = 21$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e+u+v$
v	v	$-e+u$	u

3.1.9 $\mathscr{D}(\mathscr{R}, 22)$

We first compute

$$c_1 = 22, \quad c_2 = 22S(22) = 22(22^3) = 22^4 = 19, \quad c_3 = \alpha = 22^{13} = -1 \tag{3.1.25}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{22} \circ S) - (R_{19} \circ S^2) \tag{3.1.26}$$

and

$$Q = -S^2 - (R_{23} \circ S) - (R_{13}) \tag{3.1.27}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 22 = 15$ is the identity of $\mathscr{D}(\mathscr{R}, 22)$. It is then a simple matter of computation to verify that $\{15, 25, 22\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 15$, $u = 25$, and $v = 22$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e+u+v$
v	v	$-e+u$	u

3.1.10 $\mathscr{D}(\mathscr{R}, 23)$

We first compute

$$c_1 = 23, \quad c_2 = 23S(23) = 23(23^3) = 23^4 = 6, \quad c_3 = \alpha = 23^{13} = -1 \tag{3.1.28}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{23} \circ S) - (R_6 \circ S^2) \tag{3.1.29}$$

and

$$Q = -S^2 - (R_{21} \circ S) - (R_{19}) \tag{3.1.30}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 23 = 17$ is the identity of $\mathscr{D}(\mathscr{R}, 23)$. It is then a simple matter of computation to verify that $\{17, 10, 23\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 17$, $u = 10$, and $v = 23$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e + u + v$
v	v	$-e + u$	u

3.1.11 $\mathscr{D}(\mathscr{R}, 25)$

We first compute

$$c_1 = 25, \quad c_2 = 25S(25) = 25(25^3) = 25^4 = 24, \quad c_3 = \alpha = 25^{13} = -1 \tag{3.1.31}$$

Then $(1 - \alpha) = (1 - (-1)) = 1 + 1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{25} \circ S) - (R_{24} \circ S^2) \tag{3.1.32}$$

and

$$Q = -S^2 - (R_{10} \circ S) - (R_4) \tag{3.1.33}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 25 = 12$ is the identity of $\mathscr{D}(\mathscr{R}, 25)$. It is then a simple matter of computation to verify that $\{12, 2, 23\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 17$, $u = 2$, and $v = 23$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e-u-v$
v	v	$-e+u-v$	u

3.1.12 $\mathscr{D}(\mathscr{R}, 26)$

We first compute

$$c_1 = 26, \quad c_2 = 26S(26) = 26(26^3) = 26^4 = 16, \quad c_3 = \alpha = 26^{13} = -1 \tag{3.1.34}$$

Then $(1-\alpha) = (1-(-1)) = 1+1 = -1$. Thus, from (3.1.1), (3.1.2), and some simple computation, we get that

$$P = -I - (R_{26} \circ S) - (R_{16} \circ S^2) \tag{3.1.35}$$

and

$$Q = -S^2 - (R_{11} \circ S) - (R_{17}) \tag{3.1.36}$$

We also find that, by theorem (2.2.3), $f = e - c = 1 - 26 = 14$ is the identity of $\mathscr{D}(\mathscr{R}, 26)$. It is then a simple matter of computation to verify that $\{14, 2, 22\}$ forms a basis of $\mathscr{R}$ over $\mathscr{F}$. The choice of this particular basis will become clear a little later. Thus, if we let $e = 14$, $u = 2$, and $v = 22$, then our table is given by

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e+u+v$
v	v	$-e+v$	u

3.2 Isomorphisms

An immediate observation of our tables should reveal that there seems to be redundancies. Thus, it seems only proper to find which semifields are unique, and which are merely

isomorphic copies of others. By observing the tables we can see there is always an element x such that x and x^2 are linearly independent and $x^2 \cdot x^2 = x$. This observation then motivates the following definitions.

Definition 3.2.1. *An element, x, is said to be 2-periodic when $x^2 \cdot x^2 = x^4 = x$.*

Definition 3.2.2. *A basis is said to be 2-periodic when it is of the form $\{e, x, x^2\}$ where x is 2-periodic.*

Clearly then, from our tables, we can see that every Albertian semifield has at least one 2-periodic basis.

Proposition 3.2.1. *Let $\mathscr{D}_1$ and $\mathscr{D}_2$ be twenty-seven element Albertian semifields. Then $\mathscr{D}_1 \cong \mathscr{D}_2$ iff they have 2-periodic bases which generate the same multiplication tables. That is to say, we will have for $\mathscr{D}_1$*

$\cdot$	e	u	v
e	e	u	v
u	u	v	$\alpha_1 e + \beta_1 u + \gamma_1 v$
v	v	$\alpha_2 e + \beta_2 u + \gamma_2 v$	u

if and only if, there exists a basis $\{e', u', v'\}$ of $\mathscr{D}_2$ such that

$\cdot$	e'	u'	v'
e'	e'	u'	v'
u'	u'	v'	$\alpha_1 e' + \beta_1 u' + \gamma_1 v'$
v'	v'	$\alpha_2 e' + \beta_2 u' + \gamma_2 v'$	u'

Proof. $\Rightarrow$: Let $\mathscr{D}_1$ and $\mathscr{D}_2$ be Albertian semifields and let $\phi : \mathscr{D}_1 \to \mathscr{D}_2$ be an isomorphism. Let $\{e, u, v\}$ be a 2-periodic basis for $\mathscr{D}_1$. We claim $\{\phi(e), \phi(u), \phi(v)\}$ is a 2-periodic basis of $\mathscr{D}_2$ which generates the same multiplication tables. Firstly, to show that $\{\phi(e), \phi(u), \phi(v)\}$ is a 2-periodic basis, we observe that, since $\{e, u, v\}$ is 2-periodic and ϕ is an isomorphism,

it follows that $\phi(e)$ is the identity of $\mathscr{D}_2$, that $\{\phi(e), \phi(u), \phi(v)\}$ is a basis of $\mathscr{D}_2$, and that

$$\begin{aligned}\phi(v) &= \phi(u^2) \\ &= \phi(u) \cdot \phi(u) \\ &= [\phi(u)]^2\end{aligned}$$

and

$$\begin{aligned}[\phi(v)]^2 &= \phi(v) \cdot \phi(v) \\ &= \phi(v \cdot v) \\ &= \phi(u)\end{aligned}$$

Thus $\{\phi(e), \phi(u), \phi(v)\}$ is a 2-periodic basis of $\mathscr{D}_2$. To show these bases generate the same table, we need only to compute

$$\begin{aligned}\phi(u) \cdot \phi(v) &= \phi(u \cdot v) \\ &= \phi(\alpha_1 e + \beta_1 u + \gamma_1 v) \\ &= \alpha_1\phi(e) + \beta_1\phi(u) + \gamma_1\phi(v)\end{aligned}$$

and

$$\begin{aligned}\phi(v) \cdot \phi(u) &= \phi(v \cdot u) \\ &= \phi(\alpha_2 e + \beta_2 u + \gamma_2 v) \\ &= \alpha_2\phi(e) + \beta_2\phi(u) + \gamma_2\phi(v)\end{aligned}$$

Thus, these bases generate the same multiplication tables.

$\Leftarrow$: Let $\phi : \mathscr{D}_1 \to \mathscr{D}_2$ be linear and let $\{e, u, v\}$ and $\{\phi(e), \phi(u), \phi(v)\}$ be 2-periodic bases of $\mathscr{D}_1$ and $\mathscr{D}_2$, respectively, that generate the same multiplication tables. Since ϕ is linear and it sends a basis of $\mathscr{D}_1$ to a basis of $\mathscr{D}_2$, it follows that ϕ is a bijection. We claim that ϕ is multiplicative, and therefore an isomorphism. To check this, we simply compute for

$x = a_1e + b_1u + c_1v$, $y = a_2e + b_2u + c_2v$, and $a_i, b_i, c_i \in \mathscr{F}$

$$\begin{aligned}
\phi(x \cdot y) &= \phi[(a_1e + b_1u + c_1v) \cdot (a_2e + b_2u + c_2v)] \\
&= \phi[a_1a_2e + a_1b_2u + a_1c_2v + b_1a_2u + b_1b_2u^2 + b_1c_2u \cdot v + c_1a_2v + c_1b_2v \cdot u + c_1c_2v^2] \\
&= a_1a_2\phi(e) + (a_1b_2 + b_1a_2)\phi(u) + (a_1c_2 + c_1a_2)\phi(v) + b_1b_2\phi(u^2) + b_1c_2\phi(u \cdot v) \\
&+ c_1b_2\phi(v \cdot u) + c_1c_2\phi(v^2) \\
&= a_1a_2\phi(e) + (a_1b_2 + b_1a_2)\phi(u) + (a_1c_2 + c_1a_2)\phi(v) + b_1b_2\phi(v) + c_1c_2\phi(u) \\
&+ b_1c_2\phi(\alpha_1e + \beta_1u + \gamma_1v) + c_1b_2\phi(\alpha_2e + \beta_2u + \gamma_2v) \\
&= a_1a_2\phi(e) + (a_1b_2 + b_1a_2)\phi(u) + (a_1c_2 + c_1a_2)\phi(v) + b_1b_2\phi(v) \\
&+ c_1c_2\phi(u) + b_1c_2\phi(u) \cdot \phi(v) + c_1b_2\phi(v) \cdot \phi(u)
\end{aligned}$$

and

$$\begin{aligned}
\phi(x) \cdot \phi(y) &= (a_1\phi(e) + b_1\phi(u) + c_1\phi(v)) \cdot (a_2\phi(e) + b_2\phi(u) + c_2\phi(v)) \\
&= a_1a_2(\phi(e))^2 + a_1b_2\phi(e) \cdot \phi(u) + a_1c_2\phi(e) \cdot \phi(v) + b_1c_2\phi(u) \cdot \phi(e) + b_1b_2(\phi(u))^2 \\
&+ b_1c_2\phi(u) \cdot \phi(v) + c_1a_2\phi(v) \cdot \phi(e) + c_1b_2\phi(v) \cdot \phi(u) + c_1c_2(\phi(v))^2 \\
&= a_1a_2\phi(e) + (a_1b_2 + b_1a_2)\phi(u) + (a_1c_2 + c_1a_2)\phi(v) + b_1b_2\phi(v) + c_1c_2\phi(u) \\
&+ b_1c_2\phi(u) \cdot \phi(v) + c_1b_2\phi(v) \cdot \phi(u)
\end{aligned}$$

Thus, $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$. Therefore, $\mathscr{D}_1 \cong \mathscr{D}_2$ □

Corollary 3.2.1. *We have the following isomorphisms*

$$\mathscr{D}(\mathscr{R}, 3) \cong \mathscr{D}(\mathscr{R}, 11) \cong \mathscr{D}(\mathscr{R}, 26)$$

$$\mathscr{D}(\mathscr{R}, 5) \cong \mathscr{D}(\mathscr{R}, 10) \cong \mathscr{D}(\mathscr{R}, 25)$$

$$\mathscr{D}(\mathscr{R}, 8) \cong \mathscr{D}(\mathscr{R}, 12) \cong \mathscr{D}(\mathscr{R}, 18)$$

$$\mathscr{D}(\mathscr{R}, 21) \cong \mathscr{D}(\mathscr{R}, 23) \cong \mathscr{D}(\mathscr{R}, 22)$$

Proof. By Proposition 3.2.1 and observing the tables in the previous chapter. □

Now, utilizing computer calculation (which was made possible by a collaboration with Matthew Wojciechowski), it can be shown that all semifields isomorphic to $\mathscr{D}(\mathscr{R}, 3)$ and $\mathscr{D}(\mathscr{R}, 21)$ have only one 2-periodic basis, whereas all semifields isomorphic to $\mathscr{D}(\mathscr{R}, 5)$ and $\mathscr{D}(\mathscr{R}, 8)$ have two 2-periodic bases. Thus, it follows that

$$\mathscr{D}(\mathscr{R}, 3), \mathscr{D}(\mathscr{R}, 21) \ncong \mathscr{D}(\mathscr{R}, 5), \mathscr{D}(\mathscr{R}, 8)$$

Proposition 3.2.2. $\mathscr{D}(\mathscr{R}, 3) \ncong \mathscr{D}(\mathscr{R}, 21)$

Proof. $\mathscr{D}(\mathscr{R}, 3)$ admits only one 2-periodic basis, videlicet, $\{7, 2, 21\}$. If we let $e = 7, u = 2,$ and $v = 21$ then we get

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e + u + v$
v	v	$-e + v$	u

Additionally, if we let $e = 7, u = 21,$ and $v = 2$ then we get

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e + u$
v	v	$e + u + v$	u

$\mathscr{D}(\mathscr{R}, 21)$ also admits only one 2-periodic basis, videlicet, $\{16, 5, 21\}$. If we let $e = 16, u = 5,$ and $v = 21$ then we get

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e + u + v$
v	v	$-e + u$	u

Additionally, if we let $e = 16, u = 21,$ and $v = 5$ then we get

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e+v$
v	v	$e+u+v$	u

Since none of these tables correspond, it follows from Proposition 3.2.1 that $\mathscr{D}(\mathscr{R},3) \ncong \mathscr{D}(\mathscr{R},21)$. □

Proposition 3.2.3. $\mathscr{D}(\mathscr{R},5) \ncong \mathscr{D}(\mathscr{R},8)$

Proof. $\mathscr{D}(\mathscr{R},5)$ admits the 2-periodic basis $\{8,2,22\}$ which generates

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e-u-v$
v	v	$-e+u-v$	u

and

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e-u+v$
v	v	$e-u-v$	u

and the 2-periodic basis $\{8,12,18\}$ which generates

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e-u+v$
v	v	$-e+u$	u

and

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e+v$
v	v	$-e+u-v$	u

$\mathscr{D}(\mathscr{R},8)$ admits the 2-periodic basis $\{5,10,23\}$ which generates

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e+u$
v	v	$-e-u+v$	u

and

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e+u-v$
v	v	$-e+v$	u

and the 2-periodic basis $\{5,8,18\}$ which generates

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e+u-v$
v	v	$e-u-v$	u

and

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e-u-v$
v	v	$-e-u+v$	u

Clearly, these tables differ which, by Proposition 3.2.1, implies the result. □

3.2.1 Conclusion

Altogether, we get that there are only four unique twenty-seven element Albertian semifields. In particular, any twenty-seven element Albertian semifield will be an isomorphic copy of one of the following

$$\mathscr{D}(\mathscr{R},3), \mathscr{D}(\mathscr{R},5), \mathscr{D}(\mathscr{R},8), \mathscr{D}(\mathscr{R},21)$$

We recall their tables

$\mathscr{D}(\mathscr{R},3)$:

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e+u+v$
v	v	$-e+v$	u

$\mathscr{D}(\mathscr{R},5)$:

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e-u-v$
v	v	$-e+u-v$	u

$\mathscr{D}(\mathscr{R}, 8)$:

$\cdot$	e	u	v
e	e	u	v
u	u	v	$-e+u$
v	v	$-e-u+v$	u

$\mathscr{D}(\mathscr{R}, 21)$:

$\cdot$	e	u	v
e	e	u	v
u	u	v	$e+u+v$
v	v	$-e+u$	u

Bibliography

[1] A.A. Albert. *Modern Higher Algebra*. University of Chicago Press, 1937.

[2] A.A. Albert. *Fundamental Concepts of Higher Algebra*. The University of Chicago Press, 1956.

[3] A.A. Albert. Finite noncommutative division algebras. *Proceedings of the American Mathematical Society*, 9(6):928–932, December 1958.

[4] J.R. Bastida. *Field Extensions and Galois Theory*, volume 22. Addison-Wesley Publishing Company, 1984.

[5] A. Clarke. *Elements of Abstract Algebra*. Dover Publications, 1984.

[6] M. Cordero and G.P. Wene. A survey of finite semifields. *Discrete Mathematics*, 208/209:125–137, March 1999.

[7] L.E. Dickson. Linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society*, 7(3):370–390, April 1906.

[8] D.S. Dummit and R.S. Foote. *Abstract Algebra*. Wiley, 2003.

[9] D.E. Knuth. *Finite Semifields and Projective Planes*. PhD thesis, California Institute of Technology, January 1963.

[10] J. Kok. http://www.rangevoting.org/GF27.html.

Appendix A

Multiplication and Addition Tables for $GF(27)$

We supply the multiplication and addition tables for the field $GF(27)$ [10]. The multiplication table is as follows

×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	0	2	1	6	8	7	3	5	4	18	20	19	24	26	25	21	23	22	9	11	10	15	17	16	12	14	13
3	0	3	6	9	12	15	18	21	24	11	14	17	20	23	26	2	5	8	19	22	25	1	4	7	10	13	16
4	0	4	8	12	16	11	24	19	23	20	21	25	5	6	1	17	9	13	10	14	15	22	26	18	7	2	3
5	0	5	7	15	11	13	21	26	19	2	4	6	17	10	12	23	25	18	1	3	8	16	9	14	22	24	20
6	0	6	3	18	24	21	9	15	12	19	25	22	10	16	13	1	7	4	11	17	14	2	8	5	20	26	23
7	0	7	5	21	19	26	15	13	11	1	8	3	22	20	24	16	14	9	2	6	4	23	18	25	17	12	10
8	0	8	4	24	23	19	12	11	16	10	15	14	7	3	2	22	18	26	20	25	21	17	13	9	5	1	6
9	0	9	18	11	20	2	19	1	10	17	26	8	25	7	16	6	15	24	22	4	13	3	12	21	14	23	5
10	0	10	20	14	21	4	25	8	15	26	6	16	1	11	18	12	22	5	13	23	3	24	7	17	2	9	19
11	0	11	19	17	25	6	22	3	14	8	16	24	13	21	5	18	2	10	4	12	23	9	20	1	26	7	15
12	0	12	24	20	5	17	10	22	7	25	1	13	15	18	3	8	11	23	14	26	2	4	16	19	21	6	9
13	0	13	26	23	6	10	16	20	3	7	11	21	18	4	17	14	24	1	5	15	19	25	2	12	9	22	8
14	0	14	25	26	1	12	13	24	2	16	18	5	3	17	19	20	4	15	23	7	9	10	21	8	6	11	22
15	0	15	21	2	17	23	1	16	22	6	12	18	8	14	20	7	13	19	3	9	24	5	11	26	4	10	25
16	0	16	23	5	9	25	7	14	18	15	22	2	11	24	4	13	20	6	21	1	17	26	3	10	19	8	12
17	0	17	22	8	13	18	4	9	26	24	5	10	23	1	15	19	6	14	12	20	7	11	25	3	16	21	2
18	0	18	9	19	10	1	11	2	20	22	13	4	14	5	23	3	21	12	17	8	26	6	24	15	25	16	7
19	0	19	11	22	14	3	17	6	25	4	23	12	26	15	7	9	1	20	8	24	16	18	10	2	13	5	21
20	0	20	10	25	15	8	14	4	21	13	3	23	2	19	9	24	17	7	26	16	6	12	5	22	1	18	11
21	0	21	15	1	22	16	2	23	17	3	24	9	4	25	10	5	26	11	6	18	12	7	19	13	8	20	14
22	0	22	17	4	26	9	8	18	13	12	7	20	16	2	21	11	3	25	24	10	5	19	14	6	23	15	1
23	0	23	16	7	18	14	5	25	9	21	17	1	19	12	8	26	10	3	15	2	22	13	6	20	11	4	24
24	0	24	12	10	7	22	20	17	5	14	2	26	21	9	6	4	19	16	25	13	1	8	23	11	15	3	18
25	0	25	14	13	2	24	26	12	1	23	9	7	6	22	11	10	8	21	16	5	18	20	15	4	3	19	17
26	0	26	13	16	3	20	23	10	6	5	19	15	9	8	22	25	12	2	7	21	11	14	1	24	18	17	4

The addition table for $GF(27)$ is as follows

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24
2	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	25
3	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20
4	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	9	22	23	21	25	26	24	19	20	18
5	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19
6	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23
7	7	8	6	1	2	0	4	5	3	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21
8	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8
10	10	11	9	13	14	12	16	17	15	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6
11	11	9	10	14	12	13	17	15	16	20	18	19	23	21	22	26	24	25	2	0	1	5	3	4	8	6	7
12	12	13	14	15	16	17	9	10	11	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2
13	13	14	12	16	17	15	10	11	9	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0
14	14	12	13	17	15	16	11	9	10	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1
15	15	16	17	9	10	11	12	13	14	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5
16	16	17	15	10	11	9	13	14	12	25	26	24	19	20	18	22	23	21	7	8	6	1	2	0	4	5	3
17	17	15	16	11	9	10	14	12	13	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4
18	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	18	22	23	21	25	26	24	1	2	0	4	5	3	7	8	6	10	11	9	13	14	12	16	17	15
20	20	18	19	23	21	22	26	24	25	2	0	1	5	3	4	8	6	7	11	9	10	14	12	13	17	15	16
21	21	22	23	24	25	26	18	19	20	3	4	5	6	7	8	0	1	2	12	13	14	15	16	17	9	10	11
22	22	23	21	25	26	24	19	20	18	4	5	3	7	8	6	1	2	0	13	14	12	16	17	15	10	11	9
23	23	21	22	26	24	25	20	18	19	5	3	4	8	6	7	2	0	1	14	12	13	17	15	16	11	9	10
24	24	25	26	18	19	20	21	22	23	6	7	8	0	1	2	3	4	5	15	16	17	9	10	11	12	13	14
25	25	26	24	19	20	18	22	23	21	7	8	6	1	2	0	4	5	3	16	17	15	10	11	9	13	14	12
26	26	24	25	20	18	19	23	21	22	8	6	7	2	0	1	5	3	4	17	15	16	11	9	10	14	12	13

Appendix B

Appendix B: Programs

These are some of the programs used to help compute products in the semifields. All but the first have comments to help show what each command is doing. In general, the tables for $GF(27)$ are used to compute the transformations P and Q separately. The outputs of these are then utilized in a process very nearly resembling the one outlined in $\mathscr{D}(\mathscr{R}, 3)$ to compute products.

B.0.1 $\mathscr{D}(\mathscr{R}, 3)$

```
public class multiplication {

public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}
```

```
public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}
public static int P(int[][] marr, int[][] addarr, int x){
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 3, fieldmultcubed(marr, x));
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 17, k);
int f = fieldmultnegative(marr, e);
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}
public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 26);
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 15);
int f = fieldmultnegative(marr, e);
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);
```

```
}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][]addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 3, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.2 $\mathscr{D}(\mathscr{R}, 5)$

```
public class mulitplication2 {

public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}
```

```
public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 5, fieldmultcubed(marr, x));
//d=-SR5
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 4, k);
//f=-SSR4
int f = fieldmultnegative(marr, e);
//g=-I-SR5
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
```

```
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 25);
//d=-SR25
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 9);
//f=-R9
int f = fieldmultnegative(marr, e);
//g=-SS-SR25
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}
```

```
public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 5, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.3 $\mathscr{D}(\mathscr{R}, 8)$

```
public class multiplication8 {

public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
```

```
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 8, fieldmultcubed(marr, x));
//d=-SR8
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 20, k);
//f=-SSR20
int f = fieldmultnegative(marr, e);
//g=-I-SR8
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 12);
//d=-SR12
int d = fieldmultnegative(marr, c);
```

```
int e = fieldmultiply(marr, x, 14);
//f=-R14
int f = fieldmultnegative(marr, e);
//g=-SS-SR12
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 8, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.4 $\mathscr{D}(\mathscr{R}, 10)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 10, fieldmultcubed(marr, x));
//d=-SR10
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 9, k);
```

```
//f=-SSR9
int f = fieldmultnegative(marr, e);
//g=-I-SR10
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 5);
//d=-SR5
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 24);
//f=-R24
int f = fieldmultnegative(marr, e);
//g=-SS-SR5
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}
```

```
public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 10, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.5 $\mathscr{D}(\mathscr{R}, 11)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}
```

```
public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 11, fieldmultcubed(marr, x));
//d=-SR11
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 15, k);
//f=-SSR15
int f = fieldmultnegative(marr, e);
//g=-I-SR11
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
```

```
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 3);
//d=-SR3
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 16);
//f=-R16
int f = fieldmultnegative(marr, e);
//g=-SS-SR3
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 11, b);
int d = fieldmultnegative(marr, c);
```

```
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.6 $\mathscr{D}(\mathscr{R}, 12)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 12, fieldmultcubed(marr, x));
```

```
//d=-SR12
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 7, k);
//f=-SSR7
int f = fieldmultnegative(marr, e);
//g=-I-SR12
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 18);
//d=-SR18
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 20);
//f=-R20
int f = fieldmultnegative(marr, e);
//g=-SS-SR18
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}
```

```
public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 12, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.7 $\mathscr{D}(\mathscr{R}, 18)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}
```

```
public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 18, fieldmultcubed(marr, x));
//d=-SR18
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 14, k);
//f=-SSR14
int f = fieldmultnegative(marr, e);
//g=-I-SR18
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}
```

```
public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 8);
//d=-SR8
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 7);
//f=-R7
int f = fieldmultnegative(marr, e);
//g=-SS-SR8
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
```

```
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 18, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.8 $\mathscr{D}(\mathscr{R}, 21)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}
```

```
public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 21, fieldmultcubed(marr, x));
//d=-SR21
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 13, k);
//f=-SSR13
int f = fieldmultnegative(marr, e);
//g=-I-SR21
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 22);
//d=-SR22
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 6);
//f=-R6
int f = fieldmultnegative(marr, e);
//g=-SS-SR22
int g = fieldadd(addarr, b, d);
```

```
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 21, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.9 $\mathscr{D}(\mathscr{R}, 22)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}
```

```
public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 22, fieldmultcubed(marr, x));
//d=-SR22
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 19, k);
//f=-SSR19
int f = fieldmultnegative(marr, e);
//g=-I-SR22
int g = fieldadd(addarr, a, d);
```

```
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 23);
//d=-SR23
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 13);
//f=-R13
int f = fieldmultnegative(marr, e);
//g=-SS-SR23
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}
```

```
public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 22, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.10 $\mathscr{D}(\mathscr{R}, 23)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
```

```
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 23, fieldmultcubed(marr, x));
//d=-SR23
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 6, k);
//f=-SSR6
int f = fieldmultnegative(marr, e);
//g=-I-SR23
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 21);
//d=-SR21
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 19);
```

```
//f=-R19
int f = fieldmultnegative(marr, e);
//g=-SS-SR21
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 23, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.11 $\mathscr{D}(\mathscr{R}, 25)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}

public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 25, fieldmultcubed(marr, x));
//d=-SR25
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 24, k);
```

```
//f=-SSR24
int f = fieldmultnegative(marr, e);
//g=-I-SR25
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 10);
//d=-SR10
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 4);
//f=-R4
int f = fieldmultnegative(marr, e);
//g=-SS-SR10
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}
```

```
public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 25, b);
int d = fieldmultnegative(marr, c);
int e = fieldadd(addarr, a, d);
return(e);
}
```

B.0.12 $\mathscr{D}(\mathscr{R}, 26)$

```
public static int fieldmultiply(int[][] marr,int x, int y){
return(marr[x][y]);
}

public static int fieldmultcubed(int[][] marr, int x){
return(fieldmultiply(marr, fieldmultiply(marr, x, x), x));
}

public static int fieldmultnined(int[][] marr, int x){
return(fieldmultcubed(marr, fieldmultcubed(marr, x)));
}
```

```
public static int fieldadd(int[][] addarr, int x, int y){
return(addarr[x][y]);
}
public static int fieldmultnegative(int[][] marr, int x){
return(fieldmultiply(marr, 2, x));
}

public static int P(int[][] marr, int[][] addarr, int x){
//a=-I
int a = fieldmultnegative(marr, x);
int b = fieldmultiply(marr, 26, fieldmultcubed(marr, x));
//d=-SR26
int d = fieldmultnegative(marr, b);
int k = fieldmultnined(marr, x);
int e = fieldmultiply(marr, 16, k);
//f=-SSR16
int f = fieldmultnegative(marr, e);
//g=-I-SR26
int g = fieldadd(addarr, a, d);
int h = fieldadd(addarr, g, f);
return(h);
}

public static int Q(int[][] marr, int[][] addarr, int x){
int a = fieldmultnined(marr, x);
//b=-SS
int b = fieldmultnegative(marr, a);
```

```
int c = fieldmultiply(marr, fieldmultcubed(marr, x), 11);
//d=-SR11
int d = fieldmultnegative(marr, c);
int e = fieldmultiply(marr, x, 17);
//f=-R17
int f = fieldmultnegative(marr, e);
//g=-SS-SR11
int g = fieldadd(addarr, b, d);
int h = fieldadd(addarr, g, f);
return(h);

}

public static int SQ(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, Q(marr, addarr, x)));
}

public static int SP(int[][] marr, int[][] addarr, int x){
return(fieldmultcubed(marr, P(marr, addarr, x)));
}

public static int albertMultiplication
(int[][] marr, int[][] addarr, int x, int y)
{
int a = fieldmultiply(marr, P(marr, addarr, x), SQ(marr, addarr, y));
int b = fieldmultiply(marr, SP(marr, addarr, x), Q(marr, addarr, y));
int c = fieldmultiply(marr, 26, b);
int d = fieldmultnegative(marr, c);
```

```
int e = fieldadd(addarr, a, d);
return(e);
}
```

Curriculum Vitae

Thomas Hughes was born on May 15, 1991. He attended St. Joseph Parochial School and Cathedral High School , both located in El Paso, Texas. Following his high school graduation in 2009, he attended a film school in Los Angeles, California. He spent a year there before deciding to return to El Paso to pursue a BS in Biology at The University of Texas at El Paso. Not far into his degree he developed a passion for mathematics and soon after switched his major. During his first semester as a Mathematics major he worked as an Undergraduate Teaching Assistant for The Department of Mathematics, garnering valuable experience working closely with students as a tutor as well as an instructor for the Pre-Calculus workshops. Thomas went on to enroll in the Dual Credit Fast Track Program which allowed him to take graduate classes during his undergraduate career. He graduated with a BS in Mathematics during the 2015 Summer Semester.

Immediately following his graduation, Thomas enrolled in the Graduate School of The University of Texas at El Paso. While pursuing his MS in Mathematics, he worked as a Graduate Teaching Assistant for The Department of Mathematics. His thesis material was a continuation of thesis material he had been chosen to work on as an undergraduate.

Contact: 5890 Bandolero Dr. Apt. 2144
El Paso, Texas 79912-4927
915-319-9093