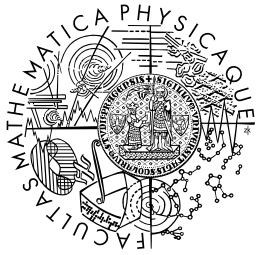

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Ondřej Tittl

Rank Two Commutative Semifields

Department of Algebra

Supervisor of the bachelor thesis: Dr. rer. nat. Faruk Gölogluu

Study programme: Mathematics for Information Technologies

Study branch: Mathematics for Information Technologies

Prague 2022

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Author's signature

I would like to thank to my supervisor Dr. rer. nat. Faruk Gölogluu for his patience and guidance.

Title: Rank Two Commutative Semifields

Author: Ondřej Tittl

Department: Department of Algebra

Supervisor: Dr. rer. nat. Faruk Göloglu, Department of Algebra

Abstract: In this thesis we will explain what are semifields and what interesting properties these algebraic objects possesses. In the first chapter we will go over some basics and preliminaries to understand what semifields are. In the second chapter we will prove some useful lemmata for either commutative and non-commutative case of semifields and provide some examples. At last we will try to do some research by ourselves, where we will try to find some examples of semifields.

Keywords: finite, commutative, semifields, vector, space

Contents

Introduction

Throughout this thesis we will explore the basics of *finite semifields* and go into more details with *rank two finite semifields*. First we will go through the preliminaries, where we will define semifields, their nuclei and how we can view semifields as vector spaces over their nuclei. For those purposes we will use Wedderburn's theorem and some basics from linear algebra.

In the second chapter we will study cases of both commutative and non-commutative rank two semifields. In this chapter we will examine the properties of both types of semifields and how our choices in specific cases determine the properties of the semifields. We will conduct proofs of some lemmata, which were omitted from the articles in sources. At the end of this section we will also provide some examples of different types of semifields, where we will expand arguments, which were not mentioned in the articles.

Throughout this thesis we use the articles by Cohen and Ganley [1982], Ganley [1981], Knuth [1965], Ball and Lavrauw [2002] and Blokhuis et al. [2003]. From these articles we put together theorems, lemmata, definitions and examples where we expand proofs that are usually very brief or omitted.

1. Preliminaries

In this thesis we assume $q = p^n$ where p is a prime unless we explicitly state otherwise. Throughout this thesis when we say *semifields* we mean finite semifields. The main focus of this thesis are finite semifields which are defined as follows.

Definition 1. *Let S be a finite set with two binary operations "$+$", "$*$" such that*

S1) *$(S, +)$ is a group,*

S2) *both distributive laws hold in S, that is*

$$\begin{aligned} a*(b+c) &= a*b + a*c, \\ (b+c)*a &= b*a + c*a, \quad \forall a,\, b,\, c \in S, \end{aligned}$$

S3) *$x * y = 0$ if and only if $x = 0$ or $y = 0$, $\quad \forall x,\, y \in S$*

S4) *there exists a multiplicative identity 1, such that $\quad \forall x \in S \quad$ holds*

$$x * 1 = x = 1 * x.$$

Then we say that $(S, +, *)$ is a finite semifield.

Now we are going to formulate Wedderburn's theorem which yields a strong property for associative finite semifields.

Theorem 1 (Wedderburn)**.** *Every finite associative semifield is a finite field.*

All finite fields are semifields. If $(S, +, *)$ is associative, then by Wedderburn's theorem S is a finite field. We call *proper* semifields those semifields S which are not fields. That is, the multiplication in proper semifields *is not associative.*

By a pre-semifield we understand a set with the operations "$+$" and "$*$" satisfying all the axioms of a semifield, except perhaps the **S4)**.

1.1 About pre-semifields

First let us formulate and prove a theorem regarding additive group of a pre-semifield. The argument was provided by [Knuth, 1965, p. 185] and we expand some steps.

Theorem 2. *The additive group of a pre-semifield is elementary abelian.*

Proof. First, let us show that the additive group of a pre-semifield $(P, +, *)$ is abelian. By group axioms "$+$" is associative. Let $a,\, b,\, c,\, d \in P$ then by the distributive laws we obtain,

$$\begin{aligned} a*c + a*d + b*c + b*d &= a*(c+d) + b*(c+d) \quad (\text{using } \mathbf{S2}) \\ &= (a+b)*(c+d) \\ &= a*c + b*c + a*d + b*d. \end{aligned} \tag{1.1}$$

Axiom **S3)** states that $x * y = 0$ if and only if either $x = 0$ or $y = 0$. Let us now suppose that $x * y_1 = z$ and $x * y_2 = z$. Then if we subtract these two equations and use the distributivity axiom we obtain that $x * (y_1 - y_2) = 0$. But if $y_1 \neq y_2$ then $y_1 - y_2 \neq 0$ which would be a contradiction to the axiom **S3)** therefore $y_1 = y_2$. From these arguments and finiteness we obtain that all the elements of P can be written as a product. Therefore for all x, $y \in P$ there exists a, b, c, $d \in P$ such that $x = a * d$ and $y = b * c$. From this fact, (1.1) and the fact that the axiom **S2)** yields $x + y = a * d + b * c = b * c + a * d = y + x$ follows that $(P, +)$ is abelian.

Now we need to show that the group $(P, +)$ is *elementary abelian*. Let us have integers n, m and let us suppose that $0 \neq a \in P$ and $((nm)a)a = 0$, then

$$0 = ((nma)a) = (\underbrace{a + \cdots + a}_{nm})a = (\underbrace{a + \cdots + a}_{n})(\underbrace{a + \cdots + a}_{m}) = (na)(ma).$$

Because $a \neq 0$ and the multiplication of non-zero elements of P is non-zero, then either $na = 0$ or $ma = 0$ and from this follows that either m or n is a prime p which is the additive order of a.

This prime p must be the same for all non-zero elements of P and is called the characteristic of the pre-semifield which can be seen from the following argument. If p would not be the same for all elements, then there would exist non-zero elements a, $b \in P$, such that $\mathrm{ord}(a) = p_1$, $\mathrm{ord}(b) = p_2$ and $p_1 \neq p_2$. Now by the distributivity axiom **S2)** we obtain

$$(p_2 a) * b = 0,$$

which is a contradiction to the axiom **S3)**. Therefore the additive order must be the same for all non-zero elements of P, hence $(P, +)$ is elementary abelian. This concludes our proof. □

Now since the additive group of a pre-semifield $(P, +)$ is elementary abelian we can write pre-semifields as $(\mathbb{F}_p^n, +, *)$.

Now we can formulate the following lemma whose idea comes from [Knuth, 1965, p. 186].

Lemma 3. *Let $P = (\mathbb{F}_p^n, +, *)$ be a pre-semifield then we can write left and right multiplication as $\mathbb{F}_p$-linear transformations L_x, R_y of the vector space P into itself. That is we can write left and right multiplication of a pre-semifield as $\mathbb{F}_p$-linear mappings*

$$L_x,\ R_y \colon \mathbb{F}_p^n \to \mathbb{F}_p^n$$

such that

$$L_x(y) = x * y = R_y(x).$$

Proof. We will show this only for L_x. For R_y the proof is analogous. We assume that $P = (\mathbb{F}_p^n, +, *)$ is a pre-semifield. Let us suppose $0 \neq x \in P$. From the definition of L_x we have that $L_x(y) = x * y$ for all $y \in P$. Since P is a pre-semifield we obtain for all y, $z \in P$ that

$$L_x(y + z) = x * (y + z) = x * y + x * z = L_x(y) + L_x(z).$$

In this series of equations we have only used the axiom **S2)** and the definition of L_x.

Now for a scalar $c \in \mathbb{F}_p$ we have that

$$L_x(cy) = x * (cy) = x * (\underbrace{y + \cdots + y}_{c}) = \underbrace{x * y + \cdots + x * y}_{c} = c(x * y) = cL_x(y).$$

Here we again used only the axiom **S2)** and the definiton of L_x. From these two properties we can see that L_x is $\mathbb{F}_p$-linear.

□

By this lemma we can now write left and right multiplication in a pre-semifield as $\mathbb{F}_p$-linear mappings L_x, R_y. We can also define the multiplication in a pre-semifield as an $\mathbb{F}_p$-bilinear mapping

$$B\colon \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^n$$

such that

$$x * y = B(x, y)$$

then

$$L_x(y) = B(x, y) = R_y(x).$$

Another important thing we can notice is that the left and right multiplication L_x, R_y for *non-zero* elements x, y are actually *permutations* of the elements of the pre-semifield $P = (\mathbb{F}_p^n, +, *)$, which is clear from the following argument. We will show this only for right multiplication. For the left multiplication the argument is analogous.

Let us fix a non-zero element $y \in P$. First we show that every $a \in P$ can be uniquely written as $R_y(x)$ for some $x \in P$. Suppose that $R_y(x_2) = a = R_y(x_1)$ and that $x_1 \neq x_2$. Now we subtract these two equations and we obtain $R_y(x_1 - x_2) = 0$. But if $x_1 \neq x_2$ then $x_1 - x_2 \neq 0$ which is a contradiction to the axiom **S3)**. Analogously we show that every $b \in P$ can be written as $L_x(y)$. Therefore all elements of P can be written in such way. And therefore L_x, R_y are bijective because they are injective between two finite sets of the same cardinality. Hence we can see that left and right multiplication are actually permutations of the elements of pre-semifield.

1.2 Isotopy and Kaplansky's trick

We would like to distinguish between pre-semifields that are in a certain way the same and those that are different. For this reason we need to define what is *isotopy*.

Definition 2. *Let $q = p^n$. Two pre-semifields $P = (\mathbb{F}_q, +, *)$ and $P' = (\mathbb{F}_q, +, \circ)$ are said to be* isotopic *if there exist $\mathbb{F}_p$-linear bijections L, M, N of $\mathbb{F}_q$ such that*

$$N(x * y) = L(x) \circ M(y).$$

Such a triple (N, L, M) is called an isotopism *between P and P'. Additionaly if $L = M$ then we call such a triple a* strong isotopism *and P, P'* strongly isotopic.

Now we will formulate a theorem about semifields being similar using definition above.

Theorem 4 (Kaplansky's trick)**.** *A pre-semifield $P = (\mathbb{F}_p^n, +, \circ)$ is isotopic to a semifield $S = (\mathbb{F}_p^n, +, *)$ defining the new multiplication as*

$$(x \circ e) * (e \circ y) = (x \circ y),$$

where $0 \neq e \in \mathbb{F}_p^n$, making $(e \circ e)$ the new multiplicative identity in S.

Proof. Let $P = (\mathbb{F}_p^n, +, \circ)$ be a pre-semifield and $S = (\mathbb{F}_p^n, +, *)$ be a semifield and let us fix an element $e \in P \backslash \{0\}$. Therefore as we have shown in Section 1.1 we can write left and right multiplication as an $\mathbb{F}_p$-linear mappings L_e, $R_e \colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ such that $L_e(x) = e \circ x$ and $R_e(x) = x \circ e$. The functions L_e, R_e are $\mathbb{F}_p$-linear by Lemma 3. Hence we can define "$*$" as

$$R_e(x) * L_e(y) = x \circ y. \tag{1.2}$$

As we have shown in Section 1.1, L_e, R_e are for a non-zero e actually *permutations*. For all a, $b \in P$ there exist some x, $y \in P$ such that $a = R_e(x)$ and $b = L_e(y)$. Therefore $x = R_e^{-1}(a)$ and $y = L_e^{-1}(b)$ hence we have

$$R_e^{-1}(a) \circ L_e^{-1}(b) = R_e(x) * L_e(y) = a * b.$$

Thus we can see that the operation "$*$" is well defined. Therefore P and S are isotopic. Isotopy preserves being a pre-semifield therefore all axioms of pre-semifield hold in S. Because the operation "$*$" is well defined then $(e \circ e)$ is the multiplicative identity in S and thus S is a semifield. This concludes our proof. □

1.3 Nuclei

From Section 1.2 and the fact that the additive group of a pre-semifield is elementary abelian we obtain that the additive group of a semifield is elementary abelian.

Now let us define the *nuclei* of finite semifields.

Definition 3. *Let $S = (\mathbb{F}_p^n, +, *)$ be a semifield. We define the subsets*

$$\begin{aligned}
\mathbb{N}_m &= \Big\{ x \in S \;\Big|\; (y * x) * z = y * (x * z), \quad \forall\, y,\, z \in S \Big\}, \\
\mathbb{N}_l &= \Big\{ x \in S \;\Big|\; (x * y) * z = x * (y * z), \quad \forall\, y,\, z \in S \Big\}, \\
\mathbb{N}_r &= \Big\{ x \in S \;\Big|\; (y * z) * x = y * (z * x), \quad \forall\, y,\, z \in S \Big\},
\end{aligned}$$

as the middle, left and right nuclei of the semifield S.

The intersection of $\mathbb{N}_m$, $\mathbb{N}_l$, $\mathbb{N}_r$ is known as the *nucleus* $\mathbb{N}$ of S. The set

$$\mathbb{C}_S = \Big\{ x \in \mathbb{N} \;\Big|\; a * x = x * a, \quad \forall\, a \in S \Big\}$$

is called the *centre* of S. It is easy to see that $\mathbb{F}_p$ is a subset in all of the nuclei. Let us also define a *weak nucleus* of a semifield. Let us now have $q = p^r$.

Definition 4. *Let $S = (\mathbb{F}_q^n, +, *)$ be a finite semifield and let $\mathbb{W} = \mathbb{F}_q$ be a subset of S such that for all x, y, $z \in S$ holds $x * (y * z) = (x * y) * z$ whenever* any two *of x, y, $z \in \mathbb{W}$. Then we say that $\mathbb{W}$ is a* weak nucleus *of S.*

We define weak nucleus as a finite field because we will view semifields as a finite-dimensional vector spaces over said field. The fact that a set is a weak nucleus of a semifield does not imply it is a nucleus and vice versa.

We can notice that the nuclei are in fact finite fields.

Theorem 5. *Let $S = (\mathbb{F}_p^n, +, *)$ be a semifield. The nuclei $\mathbb{N}_m$, $\mathbb{N}_l$, $\mathbb{N}_r$, $\mathbb{N}$ and the centre $\mathbb{C}_S$ are finite fields.*

Proof. We will show that fact for the middle nucleus. The proof for other nuclei and centre is analogous.

Let $S = (\mathbb{F}_p^n, +, *)$ be a semifield and let $\mathbb{N}_m$ be the middle nucleus of the semifield S. Let us now recall that the middle nucleus is defined as follows

$$\mathbb{N}_m = \Big\{ x \in S \,\Big|\, (y * x) * z = y * (x * z), \quad \forall\, y,\, z \in S \Big\}.$$

From the definition we know that $\mathbb{N}_m \subseteq S$. First we want to show, that $1,\, 0 \in \mathbb{N}_m$. This immediately follows from these facts

$$(x * 1) * y = x * y = x * (1 * y), \quad \forall x,\, y \in S$$

and

$$(x * 0) * y = 0 = x * (0 * y), \quad \forall x,\, y \in S.$$

Now we want to show $\forall\, a,\, b \in \mathbb{N}_m$ that $a + b$, $a * b$ and $-a$ are in $\mathbb{N}_m$. First let us verify the closure under addition. We have $\forall x,\, y \in S$ that

$$\begin{aligned} (x * a) * y &= x * (a * y), \\ (x * b) * y &= x * (b * y). \end{aligned}$$

By adding these two equations we obtain that

$$(x * a) * y + (x * b) * y = x * (a * y) + x * (b * y) \tag{1.3}$$

then from distributivity axiom we obtain that

$$\begin{aligned} (x * a) * y + (x * b) * y &= (x * a + x * b) * y \\ &= (x * (a + b)) * y \end{aligned} \tag{1.4}$$

and

$$\begin{aligned} x * (a * y) + x * (b * y) &= x * (a * y + b * y) \\ &= x * ((a + b) * y). \end{aligned} \tag{1.5}$$

Combining (1.3), (1.4) and (1.5) we obtain that $a + b \in \mathbb{N}_m$.

Now let us show that $-a \in \mathbb{N}_m$. The additive order of a in S is a prime p because $(S, +)$ is elementary abelian as we have shown in Section 1.1. From this and the fact that $\mathbb{N}_m$ is closed under addition we have for all $a \in \mathbb{N}_m$ that also

$$2a, \ldots, (p-1)a \in \mathbb{N}_m.$$

But since the order of a is p then it follows that $(p-1)a + a = 0$. Therefore $(p-1)a = -a$ and thus $-a \in \mathbb{N}_m$. Hence we can see that $(\mathbb{N}_m, +)$ is a group. Thus **S1)** holds.

Let us now verify the closure under multiplication. Let us have arbitrary $a, b \in \mathbb{N}_m$ and arbitrary $x, y \in S$ and we want to show that $a * b \in \mathbb{N}_m$. By using the defining condition of $\mathbb{N}_m$ we obtain

$$\begin{aligned}\Big[x * (a * b)\Big] * y =& \Big[(x * a) * b\Big] * y \\ =& (x * a) * (b * y) \\ =& x * \Big[a * (b * y)\Big] \\ =& x * \Big[(a * b) * y\Big].\end{aligned}$$

In this series of equalities we have used the defining condition of $\mathbb{N}_m$ and assumption that $(x * a)$, $(b * y)$ are in S. Thus we have shown that $\mathbb{N}_m$ is closed under multiplication. From the properties of $\mathbb{N}_m$ follows that the multiplication is associative in $\mathbb{N}_m$. Since $\mathbb{N}_m$ is a subset of S and the axiom **S3)** holds in S, there cannot exist $x, y \in \mathbb{N}_m$, $x \neq 0$, $y \neq 0$ such that $x * y = 0$. Hence **S3)** holds in $\mathbb{N}_m$. Similarly the axioms **S2)**, **S4)** holds in $\mathbb{N}_m$. Hence we can see that $(N_m, +, *)$ satisfies all axioms of a semifield and is associative. Then by Wedderburn's theorem 1 $(\mathbb{N}_m, +, *)$ is a finite field. Which concludes our proof. □

We have already shown in Section 1.1 that a semifield is a vector space over $\mathbb{F}_p$. Now we are going to show that a semifield can be represented as a left and right *vector space* over its middle nucleus. It can also be represented as a left vector space over its left nucleus and right vector space over its right nucleus. However we are just going to show this fact for the middle, left and weak nuclei. The proof for right nucleus is analogous. The idea of the following theorem comes again from [Knuth, 1965, p. 185].

Theorem 6. *A semifield can be represented as a left and right vector space over its middle and weak nuclei, left vector space over its left nucleus and right vector space over its right nucleus.*

Proof. Let $S = (\mathbb{F}_p^n, +, *)$ be a semifield and $\mathbb{N}_m = \mathbb{F}_{p^r}$ be its middle nucleus.

Now we will verify that vector space axioms hold in S. All the axioms of a vector space except compatibility of scalar multiplication with field multiplication immediately follow from the facts that S is a vector space over $\mathbb{F}_p$ as was shown in Section 1.1 and the fact that $\mathbb{N}_m$ is a finite field which was shown in Theorem 5. The only thing we need to verify by ourselves is the compatibility of scalar multiplication with field multiplication.

Let us have arbitrary $a, b \in \mathbb{N}_m$ and an arbitrary $x \in S$. From the defining condition of the middle nucleus we obtain that

$$a * (b * x) = (a * b) * x$$

holds but *only* for middle, left (if we take $a, b \in \mathbb{N}_l$) and weak nuclei. For right nucleus we have the following condition for all $a, b \in \mathbb{N}_r$

$$x * (a * b) = (x * a) * b$$

from the defining condition of right nucleus. Again this condition holds for right, middle and weak nuclei but does not hold for the left nucleus. We have verified

all the axioms of a vector space thus we can see that the semifield S can be represented as a left vector space over its left nucleus, right vector space over its right nucleus and left and right vector space over its middle and weak nuclei. This concludes our proof.

□

In the second chapter we will mainly focus on the semifields that are *rank two* over their middle nuclei, which means such semifields S, that are at most two-dimensional vector spaces over $\mathbb{N}_m$.

We can now formulate a well known theorem about commutative semifields. This theorem states that if a semifield is commutative then left and right nuclei coincide.

Theorem 7. *If S is a commutative semifield then $\mathbb{N}_l = \mathbb{N}_r$.*

Proof. First let us recall that

$$\mathbb{N}_l = \Big\{ x \in S \,\Big|\, (x * y) * z = x * (y * z), \quad \forall\, y,\, z \in S \Big\}$$

and

$$\mathbb{N}_r = \Big\{ x \in S \,\Big|\, (y * z) * x = y * (z * x), \quad \forall\, y,\, z \in S \Big\}.$$

Let $S = (S, +, *)$ be a semifield. First let us show that $\mathbb{N}_l \subseteq \mathbb{N}_r$. For all $x \in \mathbb{N}_l$ and for all $y,\, z \in S$ from the defining condition of $\mathbb{N}_l$ we have that

$$x * (y * z) = (x * y) * z \tag{1.6}$$

and we want to show that commutativity of the multiplication "$*$" implies that $x \in \mathbb{N}_r$. From the left side of (1.6) we have that

$$\begin{aligned} x * (y * z) &= (y * z) * x \\ &= (z * y) * x \end{aligned} \tag{1.7}$$

and from the right side of (1.6) we have that

$$\begin{aligned} (x * y) * z &= z * (x * y) \\ &= z * (y * x). \end{aligned} \tag{1.8}$$

Hence from (1.6), (1.7) and (1.8) we obtain that for all $x \in \mathbb{N}_l$ is in $\mathbb{N}_r$. Therefore $\mathbb{N}_l \subseteq \mathbb{N}_r$ and from symmetry of defining conditions we obtain that $\mathbb{N}_l = \mathbb{N}_r$ if "$*$" is commutative.

□

1.4 Linearised polynomials

For our purposes we need to formulate the theorem about *Lagrange interpolation*.

Theorem 8 (Lagrange interpolation)**.** *Let $\mathbb{F}_q$, $q = p^n$ be a finite field and let us have a mapping $\widetilde{f}\colon \mathbb{F}_q \to \mathbb{F}_q$. Then there exists exactly one polynomial $f \in \mathbb{F}_q[x]$ of degree $\leq q-1$ such that $f(x) = \widetilde{f}(x) \quad \forall x \in \mathbb{F}_q$. The polynomial f can be expressed as follows*

$$f(x) = \sum_{\alpha \in \mathbb{F}_q} \widetilde{f}(\alpha)\Big(1 - (x - \alpha)^{q-1}\Big).$$

Proof. Firstly let us show the uniqueness of this representation. Let us have polynomials g, $h \in \mathbb{F}_q[x]$ of degree $\leq q-1$ and let us suppose that $(g-h)(x) = 0$ for all $x \in \mathbb{F}_q$. But from the fundamental theorem of algebra we know that if the polynomial $g-h$ is non-zero then it can have *at most* $q-1$ zeroes. Therefore in $\mathbb{F}_q$ there exist at least one element which is not its root. Hence $g = h$.

From the above arguments and cardinality of $\mathbb{F}_q$ we can see that there are exactly q^q polynomials of degree $\leq q-1$. It is also well known that there exists exactly q^q functions from the finite field $\mathbb{F}_q$ into itself. Since the number of these polynomials and functions are the same then there exists 1-to-1 correspondence between functions from $\mathbb{F}_q$ into itself and polynomials of degree at most $q-1$ over $\mathbb{F}_q[x]$.

From the Small Fermat Theorem and from properties of finite fields we can see that for all $\alpha \in \mathbb{F}_q$ holds

$$(x-\alpha)^{q-1} = \begin{cases} 0, & \text{if } x = \alpha, \\ 1, & \text{if } x \neq \alpha. \end{cases}$$

If in this equality $x \neq \alpha$ then $x - \alpha = a$ where $0 \neq a \in \mathbb{F}_q$ and from the Small Fermat Theorem we have for all non-zero a that $a^{q-1} = 1$. Therefore we can see that the polynomial

$$f = \sum_{\alpha \in \mathbb{F}_q} \widetilde{f}(\alpha)\Big(1 - (x-\alpha)^{q-1}\Big)$$

is in $\mathbb{F}_q[x]$ of degree $\leq q-1$. We can also see that for all $\alpha \in \mathbb{F}_q$ holds that

$$\widetilde{f}(\alpha) = f(\alpha) = 0 + \cdots + 0 + \widetilde{f}(\alpha)\Big(1 - (\alpha-\alpha)^{q-1}\Big) + 0 + \cdots + 0.$$

□

Let $q = p^n$. The automorphisms of a finite field $\mathbb{F}_q$ are mappings

$$\varphi \colon \mathbb{F}_q \to \mathbb{F}_q$$

such that for all a, $b \in \mathbb{F}_q$ holds

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

and

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

That is these mappings preserve both addition and multiplication. It is well known that in a finite field all automorphisms are of the following form

$$\begin{aligned} \varphi : \mathbb{F}_q &\to \mathbb{F}_q \\ a &\mapsto a^{p^i} \end{aligned}$$

where $i \in \{0, \ldots, n-1\}$. It is also well known that automorphisms of $\mathbb{F}_q$ form a group, which is denoted by

$$\mathrm{Aut}(\mathbb{F}_q) := \Big\{\varphi \colon \mathbb{F}_q \to \mathbb{F}_q \;\Big|\; \varphi \text{ is automorphism of } \mathbb{F}_q\Big\}.$$

In this thesis we would like to work with *polynomials* possessing similar additive properties but not necessarily multiplicative properties of automorphisms.

Therefore for our purposes we would like to introduce another lemma about *linearised* polynomials. Linearised polynomials in $\mathbb{F}_{p^n}[x]$ are of the form

$$\sum_{i=0}^{n-1} a_i x^{p^i}, \qquad \text{where } \forall i, \quad a_i \in \mathbb{F}_{p^n}.$$

These polynomials possess linear properties, which follow from the Frobenius endomorphism, they represent $\mathbb{F}_p$-linear transformations of $\mathbb{F}_{p^n}$.

Lemma 9. *All $\mathbb{F}_p$-linear transformations of $\mathbb{F}_{p^n}$ into itself are of the form*

$$f(x) = \sum_{i=0}^{n-1} f_i x^{p^i}, \quad \forall i, \quad f_i \in \mathbb{F}_{p^n}.$$

That is, there exists a bijection between linearised polynomials and $\mathbb{F}_p$-linear transformations of $\mathbb{F}_p^n$ into itself.

Proof. First let us show that linearised polynomials are $\mathbb{F}_p$-linear. Let $f \in \mathbb{F}_{p^n}[x]$ be a linearised polynomial. Now from Frobenius endomorphism we obtain that

$$f(x+y) = \sum_{i=0}^{n-1} f_i (x+y)^{p^i} = \sum_{i=0}^{n-1} f_i x^{p^i} + \sum_{i=0}^{n-1} f_i y^{p^i} = f(x) + f(y).$$

Now let us have $c \in \mathbb{F}_p$ then again from Frobenius endomorphism and from the fact that in $\mathbb{F}_p$ holds $c^{p^i} = c$ for all $1 \leq i \leq n-1$ and from commutativity of field multiplication, we obtain that

$$f(cx) = \sum_{i=0}^{n-1} f_i (cx)^{p^i} = \sum_{i=0}^{n-1} f_i c^{p^i} x^{p^i} = \sum_{i=0}^{n-1} f_i c x^{p^i} = c \sum_{i=0}^{n-1} f_i x^{p^i} = c f(x).$$

Thus we can see that all linearised polynomials are $\mathbb{F}_p$-linear.

The uniqueness of linearised polynomials can be seen from more general Lagrange interpolation Theorem 8, which shows that *every* function over a finite field can be uniquely expressed as a polynomial over said field.

From the above arguments and size of the finite field $\mathbb{F}_{p^n}$ we can see that there are exactly p^{n^2} of $\mathbb{F}_p$-linear polynomials.

In the vector space $\mathbb{F}_p^n$ are all linear mappings matrices of size $n \times n$. Therefore there is exactly p^{n^2} of $n \times n$ matrices in $\mathbb{F}_p^n$.

Thus we can see that the number of $n \times n$ matrices and linearised polynomials is the same hence there exists 1-to-1 correspondence between these matrices and linearised polynomials. This concludes our proof.

□

Let $q = p^n$. Now we would like to define the set of squares in a finite field $\mathbb{F}_q$, this will be important later when we go over some examples of semifields.

Definition 5. *We define the squares of a finite field $\mathbb{F}_q$ as $SQ_{\mathbb{F}_q} = \left\{ x^2 \,\middle|\, x \in \mathbb{F}_q^\times \right\}$, where $\mathbb{F}_q^\times = \mathbb{F}_q \backslash \{0\}$ is the multiplicative group of the finite field $\mathbb{F}_q$.*

At last we would like to define some types of semifields by their multiplication. We will show examples of these semifields later in Chapter 2.

The following table shows some examples of at most two-dimensional semifields, which we will explore in Chapter 2. These examples are from Knuth [1965], Cohen and Ganley [1982] and Ball and Lavrauw [2002].

Name	$(a,b) * (c,d)$
Finite field	$\Big(\alpha ac + bc + ad,\ \beta ac + bd\Big)$
Dickson, Kantor, Knuth	$\Big(ad + bc, m(ac)^{\sigma} + bd\Big)$
Cohen-Ganley, Thas-Payne	$\Big(m(ac)^3 + bc + ad, m^3 ac + m(ac)^9 + bd\Big)$
Penttila-Williams	$\Big((ac)^9 + bc + ad, (ac)^{27} + bd\Big)$

m is a non-square in the field $\mathbb{F}_q$, σ is an automorphism in the field $\mathbb{F}_q$ and $x^2 - \alpha x - \beta$ is irreducible over $\mathbb{F}_q$.

Table 1.1: The multiplication in the known examples of semifields.

2. Rank two semifields commutative and non-commutative

2.1 Commutative case

Throughout this section we consider rank two semifields, that is such semifields $(S, +, *)$ that are at most two-dimensional vector spaces, over their middle nuclei $\mathbb{N}_m = \mathbb{F}_q$ as we have shown in Theorem 6, where $q = p^n$ for some odd prime p. We choose a $t \in S \backslash \mathbb{N}_m$ and the set $\{1, t\}$ is the basis of S over $\mathbb{N}_m$. By rank two commutative semifield we understand a semifield that has commutative multiplication "$*$" and is at most two-dimensional vector space over its middle nucleus. The multiplication "$*$" in rank two commutative semifield is defined as follows

$$(t * a + b) * (t * c + d) = t * (t * ac) + t * bc + t * ad + bd, \tag{2.1}$$

where a, b, c, $d \in \mathbb{N}_m$. Generally in rank two commutative semifields we can rewrite

$$(t * a) * (t * c) = t * (t * (ac))$$

because of the following argument. For all x, $y \in \mathbb{N}_m$ holds that

$$\begin{aligned}
(t * x) * (t * y) &= (t * x) * (y * t) \quad \text{(commutativity of } *) \\
&= t * (x * (y * t)) \quad \text{(property of } \mathbb{N}_m) \\
&= t * \Big((x * y) * t\Big) \quad \text{(property of } \mathbb{N}_m) \\
&= t * (t * (xy)) \quad \text{(commutativity of } *).
\end{aligned}$$

We decided not to write "$*$" between the elements x, y because $x * y$ is equal to xy in $\mathbb{N}_m$. Because multiplication by t is a linear transformation of the vector space S, as we have shown in Lemma 3, we can rewrite $t * (t * x) = t * L_1(x) + L_2(x) \quad \forall x \in \mathbb{F}_q$, where L_1, $L_2 : \mathbb{F}_q \to \mathbb{F}_q$ are $\mathbb{F}_p$-linear mappings. These mappings can be found using Lagrange interpolation Theorem 8. Thus we get the formula for multiplication, which can be written as follows

$$(t * a + b) * (t * c + d) = t * \Big[L_1(ac) + bc + ad\Big] + L_2(ac) + bd. \tag{2.2}$$

In the article by Cohen and Ganley [1982] there are a couple of lemmata whose proofs were not provided. Now we will formulate and prove them. The first lemma shows that we can choose an arbitrary $t \in S \backslash \mathbb{N}_m$. For a fixed t we can go through all the possible functions L_1, L_2 which yield a semifield multiplication to obtain all the possible semifields. In [Cohen and Ganley, 1982, p. 376] the lemma was formulated as follows and an idea of the proof was given but the details were omitted.

Lemma 10. *Let* $t \in S \backslash \mathbb{N}_m$, $\mathbb{N}_m = \mathbb{F}_q$. *Suppose that*

$$t * (t * x) = t * L_1(x) + L_2(x),$$

where $L_1,\ L_2 : \mathbb{F}_q \to \mathbb{F}_q$ *are* $\mathbb{F}_p$*-linear mappings, and that* $t' = t * a + b$ *for some* $a, b \in \mathbb{F}_q$*, with* $a \neq 0$*. Then*

$$t' * (t' * x) = t' * L_1'(x) + L_2'(x),$$

where

$$\begin{aligned} L_1'(x) &= a^{-1}L_1(a^2x) + 2bx, \\ L_2'(x) &= L_2(a^2x) - a^{-1}bL_1(a^2x) - b^2x. \end{aligned}$$

Proof. We have $t' = t * a + b$ for some $a, b \in \mathbb{N}_m$, where $a \neq 0$. Then from the multiplication formula (2.1) we obtain

$$\begin{aligned} t' * (t' * x) &= (t * a + b) * ((t * a + b)x) \\ &= (t * a + b) * (t * ax + bx) = t * (t * a^2x) + 2t * abx + b^2x. \end{aligned} \tag{2.3}$$

Now the multiplication formula (2.2) yields

$$\begin{aligned} t' * (t' * x) &= t * (t * a^2x) + 2t * abx + b^2x \\ &= t * L_1(a^2x) + L_2(a^2x) + 2t * abx + b^2x. \end{aligned}$$

Now we want to show that

$$t * L_1(a^2x) + L_2(a^2x) + 2t * abx + b^2x = t' * L_1'(x) + L_2'(x). \tag{2.4}$$

From this we get

$$\begin{aligned} t' * L_1'(x) + L_2'(x) =& (t * a + b) * \left[a^{-1}L_1(a^2x) + 2bx\right] + L_2(a^2x) \\ & - a^{-1}bL_1(a^2x) - b^2x \\ =& t * aa^{-1}L_1(a^2x) + 2t * abx + ba^{-1}L_1(a^2x) + 2b^2x + L_2(a^2x) \\ & - a^{-1}bL_1(a^2x) - b^2x \\ =& t * L_1(a^2x) + 2t * abx + b^2x + L_2(a^2x). \end{aligned} \tag{2.5}$$

Now from (2.3), (2.5) we see that (2.4) holds.

□

The second lemma characterizes L_1, L_2 leading to a semifield multiplication. The idea of the proof of this lemma comes from [Cohen and Ganley, 1982, p. 375].

Lemma 11. *The multiplication* (2.2) *yields a semifield if and only if*

i) $L_1,\ L_2 : \mathbb{F}_q \to \mathbb{F}_q$*, are* $\mathbb{F}_p$*- linear, and*

ii) $xy^2 + L_1(x)y - L_2(x) \neq 0 \quad \forall x, y \in \mathbb{F}_q$*, where* $x \neq 0$*.*

Proof. If S is a semifield then by Lemma 3 L_1, L_2 are $\mathbb{F}_p$-linear. Hence condition i) holds. Conversely, if condition i) holds then from linearity of L_1, L_2 we immediately obtain that both distributive laws hold.

Now let us show that if S is a semifield then the condition ii) holds. From multiplication formula (2.2) we derive following conditions

$$L_1(ac) + ad + bc = 0, \tag{2.6}$$

$$L_2(ac) + bd = 0. \tag{2.7}$$

And by axiom **S3)** we now obtain that S is a pre-semifield if and only if (2.6) and (2.7) holds for every $(a,\, b) \in \mathbb{F}_q \times \mathbb{F}_q \backslash \{(0,0)\}$ exactly when $c = d = 0$. If $c = 0$ then by (2.6), (2.7) is $ad = 0$ and $bd = 0$ because $L_1(\omega) = L_2(\omega) = 0$ if $\omega = 0$ hence $d = 0$. Therefore we can assume $c \neq 0$. Then the equations (2.6) and (2.7) can be written as

$$b = -(L_1(ac) + ad)c^{-1}$$

and

$$bd = -L_2(ac).$$

Now we can see that $a = 0$ implies $b = 0$ whenever $c \neq 0$. If $d = 0$ then from (2.6), (2.7) we obtain $a = b = 0$. Hence (2.6), (2.7) hold together if and only if

$$ad^2 + dL_1(ac) - cL_2(ac) \neq 0 \tag{2.8}$$

for all $a,\, c \in \mathbb{F}_q \backslash \{0\}$ and $d \in \mathbb{F}_q$. Where we used (2.7) and plugged in $b = -(L_1(ac) + ad)c^{-1}$ and used some elementary operations. We can now use substitution $x = ac$ and $y = dc^{-1}$ and we obtain

$$xy^2 + L_1(x)y - L_2(x) = 0. \tag{2.9}$$

Hence (2.9) holds if and only if S is a pre-semifield. We have already shown that these conditions are equal to a pre-semifield. Now we only need to show that if these two conditions hold then **S4)** holds. The fact that $1 \in S$ is clear. Let $a = 0$ and $b = 1$ thus $1 \in S$, then the element $(t0 + 1)$ is the multiplicative identity in S. Hence the axiom **S4)** holds. □

Let us recall the very well known fact that the discriminant of quadratic polynomial $ax^2 + bx + c$ is defined as

$$b^2 - 4ac.$$

We will make use of this in the following remark.

Remark. The second condition of the Lemma 11 is equivalent to the condition that

$$L_1^2(x) + 4xL_2(x) \tag{2.10}$$

is a *non-square* in $\mathbb{F}_q$ that is $L_1^2(x) + 4xL_2(x) \notin SQ_{\mathbb{F}_q}$. This follows from the fact that the discriminant of the polynomial

$$xy^2 + L_1(x)y - L_2(x)$$

is

$$\Big(L_1(x)y\Big)^2 + 4xy^2L_2(x) = y^2\Big(L_1^2(x) + 4xL_2(x)\Big).$$

Thus we can see that we only need to put $x \neq 0$ in the condition *ii*) of the lemma because if $y = 0$ and $x \neq 0$ then the polynomial from condition *ii*) still would not be equal to zero. Therefore if the discriminant is a non-square then the multiplication does not allow zero divisors.

The main result of [Cohen and Ganley, 1982, p. 377] is the following theorem that shows that there are no such *proper* rank two finite commutative semifields of even order.

Theorem 12. *There is no proper commutative semifield of even order which is of dimension 2 over its middle nucleus.*

The aim of this thesis are finite semifields, the proof is using advanced knowledge of finite fields and exponential sums. Therefore we are not going to prove this theorem but proof can be found in Cohen and Ganley [1982].

2.2 Examples of commutative semifields

Now we will show a couple of examples from Table 1.1. We will go over some other examples more thoroughly later in Section 2.4.

Before we get to the example let us recall the multiplication Formula (2.2)

$$(t * a + b) * (t * c + d) = t * \Big[L_1(ac) + bc + ad\Big] + L_2(ac) + bd.$$

2.2.1 Finite field

We are now going to show that the multiplication in rank two commutative semifield can represent a finite field. This example was left as an exercise in Cohen and Ganley [1982].

Example. Let us have α, $\beta \in \mathbb{F}_q$ and let

$$L_1(x) = \alpha x$$

and

$$L_2(x) = \beta x.$$

Then S is a finite field of order q^2 if and only if the polynomial $x^2 - \alpha x - \beta$ is irreducible over $\mathbb{F}_q$. Let us derive multiplication formula using t which is a root of $x^2 - \alpha x - \beta$.

$$\begin{aligned}(ta + b)(tc + d) &= t^2ac + tad + tbc + bd \\ &= (\beta + \alpha t)ac + tad + tbc + bd \\ &= t\alpha ac + tad + tbc + \beta ac + bd \\ &= t\Big(\alpha ac + ad + bc\Big) + \beta ac + bd\end{aligned}$$

From this we can see the multiplication in a finite field and the multiplication Formula (2.2) match. Hence we can see that this is the same multiplication as in Table 1.1. From this we can infer that if the polynomial is irreducible then the roots of this polynomial generate a quadratic extension of the finite field $\mathbb{F}_q$.

If the polynomial were reducible then there exists γ, $\delta \in \mathbb{F}_q$ such that

$$0 = x^2 - \alpha x - \beta = (x - \gamma)(x - \delta).$$

This would allow zero divisors which can be seen from the derivation of the multiplication above. However zero divisors are a contradiction to the axiom **S3)**. The roots of a reducible polynomial does not form a quadratic extension of $\mathbb{F}_q$ and therefore it would be only the finite field $\mathbb{F}_q$.

If we assume only odd characteristic then in the example above we can put $\alpha = 0$ and $\beta \neq 0$ in finite field of order q^2. Then we obtain functions $L_1(x) = 0$ and $L_2(x) = \beta x$.

2.2.2 Dickson commutative semifield

An example of a semifield that is two-dimensional vector space over $\mathbb{F}_q$ for some odd prime is *Dickson commutative semifield*. This semifield was firstly described by Dickson [1906]. And it is defined in Table 1.1 as follows.

Example. In Table 1.1 we have described that $(S, +, *)$ is a Dickson commutative semifield if for all a, b, c, $d \in S$ holds

$$(t * a + b) * (tc + d) = t * (ad + bc) + m(ac)^\sigma + bd,$$

where m is a non-square in $\mathbb{F}_q$ and σ is an automorphism of $\mathbb{F}_q$.

Now we can see that this multiplication corresponds to the multiplication in Table 2.1. That is we have the functions

$$L_1(x) = 0$$

and

$$L_2(x) = mx^\sigma,$$

where $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ and m is a non-square in $\mathbb{F}_q$ that is $m \notin SQ_{\mathbb{F}_q}$. Let us have a, b, c, $d \in S$ then we can see that this multiplication corresponds to Table 2.1 by computation using (2.2)

$$\begin{aligned}(t * a + b) * (t * c + d) &= t * \Big[ad + bc + L_1(ac)\Big] + L_2(ac) + bd \\ &= t * \Big[ad + bc\Big] + ma^\sigma c^\sigma + bd.\end{aligned}$$

2.2.3 Cohen-Ganley semifield

At last we would like to show the example from [Cohen and Ganley, 1982, p. 381] which they discovered as a new type of commutative semifields.

Example (Cohen-Ganley). Let $q = 3^k$, where $k \geq 2$ and let m be a non-square in $\mathbb{F}_q$. Then if

$$\begin{aligned}L_1(x) &= mx^3, \\ L_2(x) &= mx^9 + m^3x\end{aligned}$$

we obtain a proper commutative semifield. The functions L_1, L_2 are $\mathbb{F}_p$-linear. Now we just need to check the condition we obtained from the remark after Lemma 11 which states that

$$L_1^2(x) + 4xL_2(x)$$

must not be a square in $\mathbb{F}_q$. Here it is important that the characteristic is 3 because then we have that $4 \equiv 1 \bmod 3$. Let us show that this condition holds. We have that

$$L_1^2(x) + 4xL_2(x) = m^2x^6 + (mx^9 + m^3x)x = mx^2(x^8 - 2mx^4 + m^2) = mx^2(x^4 - m)^2.$$

Because m is a non-square and the remaining terms are squares then we obtain that this is a non-square for all x. Therefore the condition holds and thus we do not have zero divisors hence the Lemma 11 implies that the multiplication formula (2.2) yields a semifield.

2.2.4 Classification of certain types of semifields

Under certain circumstances the examples above are the only possibilities for a rank two semifield. To be more precise, if L_1, L_2 are $\mathbb{F}_{q_0}$-linear and if q_0 is "large" compared to n, the above examples are the only commutative semifields that are rank two over $\mathbb{F}_{q_0^n}$.

The following theorem comes from [Blokhuis et al., 2003, p. 106].

Theorem 13. *A commmutative semifield of rank 2 over its middle nucleus $\mathbb{N}_m = \mathbb{F}_q$ whose defining functions L_1 and L_2 are linear over the subfield $\mathbb{F}_{q_0}$, where $q = q_0^n$ and $q_0 \geq 4n^2 - 8n + 2$ is either the finite field $\mathbb{F}_{q^2}$ or is isotopic to a Dickson, Kantor or Knuth semifield.*

2.3 Non-commutative case

In this section we will again make use of Theorem 6 which enables us to view semifields as at most two-dimensional vector space over some field. In this section we generally assume that the multiplication "$*$" in semifield S is non-commutative. First let us recall the definition of a *weak nucleus*. Let us now have $q = p^r$ and let $S = (\mathbb{F}_q^n, +, *)$ be a semifield. We say that the subset $\mathbb{W} \subseteq S$ is a *weak nucleus* of S if for all x, y, $z \in S$ holds $x * (y * z) = (x * y) * z$ whenever *any two* of x, y, z are in $\mathbb{W}$.

Analogously as in the commutative case and as we have shown in Theorem 6 we view these semifields as at most two-dimensional over their weak nucleus. Note that the fact that a set is a weak nucleus of a semifield does not imply it is a nucleus and vice versa.

[Knuth, 1965, p. 212] formulated a theorem which shows that for a semifield which is two-dimensional over its weak nucleus, it is possible to choose $t \in S \backslash \mathbb{F}_q$ such that $a * t = t * a^\sigma \ \forall\, a \in \mathbb{F}_q$, where $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$. Let us formulate this theorem.

Theorem 14. *Let $\mathbb{W}$ be a weak nucleus for $(S, +, *)$, and let S have dimension two over $\mathbb{W}$. Then the elements of S have the form*

$$t * a + b, \quad a, b \in \mathbb{W}.$$

The element $t \in S$ can be chosen such that

$$a * t = t * a^\sigma$$

for all $a \in \mathbb{W}$ and for $\sigma \in \mathrm{Aut}(\mathbb{W})$.

We are not going to prove this theorem we are only going to use it but [Knuth, 1965, p. 212] provided a proof.

In Ganley [1981] they have defined *central weak nucleus* as follows.

Definition 6. *Let $S = (\mathbb{F}_q^n, +, *)$ be a semifield and $\mathbb{W} = \mathbb{F}_q$ be a subset of S such that $t * a = a * t$ for all $a \in \mathbb{W}$ and for all $t \in S$ then $\mathbb{W}$ is called* central weak nucleus.

It is called central weak nucleus because its defining condition reminds of the definition of centre.

Multiplication in rank two non-commutative weak nucleus semifield is rather similar to the multiplication in a rank two commutative semifields. Using Theorem 14 we can now define the rank two non-commutative weak nucleus semifield multiplication "$*$" in the following way

$$(t * a + b) * (t * c + d) = (t * a) * (t * c) + t * (ad) + t * (b^\sigma c) + bd, \tag{2.11}$$

for $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ and $\forall\, a,\, b,\, c,\, d \in \mathbb{F}_q$. Here we obtain $t * (b^\sigma c)$ from

$$\begin{aligned} b * (t * c) &= (b * t) * c \quad \text{(because } b,\, c \text{ are in } \mathbb{W}) \\ &= (t * b^\sigma) * c \quad \text{(using Theorem 14)} \\ &= t * (b^\sigma * c) \quad (b,\, c \in \mathbb{W}). \end{aligned}$$

Here similarly as in the commutative case we can rewrite the multiplication formula of rank two non-commutative semifield as

$$(t * a + b) * (t * c + d) = t * \Big[N_1(a, c) + ad + b^\sigma c\Big] + N_2(a, c) + bd, \tag{2.12}$$

where $a,\, b,\, c,\, d \in \mathbb{F}_q$. Analogously as in the commutative case $N_1,\, N_2 \colon \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q$ must be bilinear in order to satisfy *both* distributive laws. As in the commutative case [Ganley, 1981, p. 340] formulated the following two lemmata but did not provide the proofs. We will reformulate them and prove one of them, because the proof of the second one is similar to the proof of Lemma 11.

The first lemma again shows that the choice of $t \in S \backslash \mathbb{F}_q$ yields different functions $N_1,\, N_2$, however we can compute $N_1',\, N_2'$ such that it will lead to a rank two central weak nucleus semifield. If we fix a t we can obtain all the possible functions that define the rank two central weak nucleus semifield multiplication and this will give us all such possible semifields. In the following lemma [Ganley, 1981, p.340] again provided a hint for the proof but omitted the details.

Lemma 15. *Let $S = (\mathbb{F}_p^n, +, *)$ be a central weak nucleus semifield and let $\mathbb{F}_q$ be its central weak nucleus where $q = p^r$. Let $x,\, y \in \mathbb{F}_q$ and let $(t * a) * (t * c) = t * N_1(a, c) + N_2(a, c)$ and $t' = t * x + y$. With $x \neq 0$, then*

$$(t' * a) * (t' * c) = t' * N_1'(a, c) + N_2'(a, c),$$

where

$$\begin{aligned} N_1'(a, c) &= x^{-1} N_1(xa, xc) + 2yac \\ N_2'(a, c) &= N_2(xa, xc) - yx^{-1} N_1(xa, xc) - y^2 ac. \end{aligned}$$

Proof. Firstly by the multiplication formulae (2.11) and (2.12) we obtain

$$\begin{aligned} (t' * a) * (t' * c) &= \Big[(t * x + y)a\Big] * \Big[(t * x + y)c\Big] \\ &= (t * (xa)) * (t * (xc)) + t * (xayc) + (ya) * t * (xc) + yayc \\ &= t * \Big[x^{-1} N_1(xa, xc) + 2yac\Big] + N_2(xa, xc) + y^2 ac. \end{aligned}$$

Now let us compute the other side of the equation.

$$t' * N_1'(a,c) + N_2'(a,c) = (t * x + y) * \Big[x^{-1}N_1(xa,xc) + 2yac\Big] + N_2(xa,xc)$$
$$-y\Big[x^{-1}N_1(xa,xc) - yac\Big] = t * \Big[N_1(xa,xc) + 2xyac\Big] + N_2(xa,xc) + y^2ac.$$

Thus we see that both sides are equal, which concludes our proof.

□

The second lemma again characterizes N_1, N_2 leading to a semifield multiplication. [Ganley, 1981, p. 340] formulated it as follows.

Lemma 16. *The multiplication formula* (2.12) *is a semifield multiplication if and only if*

i) N_1, N_2 *are bilinear, and*

ii) $b^2c + bN_1(a,c) - aN_2(a,c) \neq 0 \quad \forall\, a,\, b,\, c \in \mathbb{F}_q$, *where* $a,\, c \neq 0$.

The proof of this lemma is analogous to the proof of Lemma 11.

As in the commutative case [Ganley, 1981, p. 342] has shown that there are no such *proper* rank two semifields of even characteristic.

2.4 Examples

In their article [Cohen and Ganley, 1982, p. 384] gave a *sporadic* example of a semifield. By sporadic example we understand such example, which was not classified. The following table is from [Ball and Lavrauw, 2002, p. 5]. It shows the known examples of types of finite semifields.

Name	$L_1(x)$	$L_2(x)$	$q = p^n$
Finite field	0	mx	odd
Dickson, Kantor, Knuth	0	mx^σ	odd
Cohen-Ganley, Thas-Payne	x^3	$m^{-1}x + mx^9$	3^n
Penttila-Williams	x^9	x^{27}	3^5

m is a non-square in the field $\mathbb{F}_q$, σ is an automorphism in the field $\mathbb{F}_q$.

Table 2.1: The known examples of rank two semifields in odd characteristic up to equivalence.

2.4.1 Sporadic example of Cohen-Ganley

Now we will go through the so called sporadic example [Cohen and Ganley, 1982, p. 384] provided in their article. We will expand some arguments in this example

Example (Cohen-Ganley). Let $q = 5^2$, so if we will consider the semifield S to be a two-dimensional vector space over $\mathbb{F}_q$, then $\#S = 5^4$. If we regard $\mathbb{F}_q$ as $\mathbb{F}_5(\sqrt{2})$, then the elements of $\mathbb{F}_q$ are of type $a + \sqrt{2}b$, where $a,\, b \in \mathbb{F}_5$. We will view $\mathbb{F}_5$ as

a set $\{0, \pm 1, \pm 2\}$. Then, the semifield is obtained by taking the multiplication functions as follows

$$L_1(x) = x^5 \text{ and } L_2(x) = 2\sqrt{2}x^5 + x.$$

From the second condition of Lemma 11 in odd characteristic we obtain equivalent condition for non-zero divisors, which then verifies if S is a semifield or not. The equivalent formulation is that we need $L_1^2(x) + 4xL_2(x)$ to be a non-square in S from the remark after the Lemma 11. So we can write

$$L_1^2(x) + 4xL_2(x) = x^2(x^8 - 2\sqrt{2}x^4 - 1) = f.$$

Which is always a non-square in S. We verify that, by plugging in all the possible values of x into that expression. Then it suffices to check that these values are not equal to any square in $\mathbb{F}_q$. The squares in $\mathbb{F}_5(\sqrt{2})$ are of the form $(a + \sqrt{2}b)^2 = c + \sqrt{2}d$ where a, b, c, $d \in \mathbb{F}_5(\sqrt{2})$. By computation we obtain that all squares in $\mathbb{F}_5(\sqrt{2})$ are

$$SQ_{\mathbb{F}_5(\sqrt{2})} = \left\{0, \pm 1, \pm 2, \pm(1 \pm \sqrt{2}), \pm(2 \pm \sqrt{2})\right\}.$$

All the non-squares in $\mathbb{F}_q$ are from this set

$$\{\pm\sqrt{2},\ \pm 2\sqrt{2},\ \pm(1 \pm 2\sqrt{2}),\ \pm(2 \pm \sqrt{2})\}.$$

Now we are going to plug in all the possible values into said expression.

$$\begin{aligned}
&f(1) = -2\sqrt{2},\ f(2) = 2\sqrt{2},\ f(-2) = 2\sqrt{2},\ f(-1) = -2\sqrt{2},\ f(\sqrt{2}) = -\sqrt{2},\\
&f(2\sqrt{2}) = \sqrt{2},\ f(-2\sqrt{2}) = \sqrt{2},\ f(-\sqrt{2}) = -\sqrt{2},\ f(1 + \sqrt{2}) = -2\sqrt{2},\\
&f(1 + 2\sqrt{2}) = \sqrt{2},\ f(1 - 2\sqrt{2}) = 2\sqrt{2},\ f(1 - \sqrt{2}) = \sqrt{2},\\
&f(2 + \sqrt{2}) = -2\sqrt{2},\ f(2 + 2\sqrt{2}) = 2\sqrt{2},\ f(2 - 2\sqrt{2}) = -\sqrt{2},\\
&f(2 - \sqrt{2}) = -\sqrt{2},\ f(-2 + \sqrt{2}) = -\sqrt{2},\ f(-2 + 2\sqrt{2}) = -\sqrt{2},\\
&f(-2 - 2\sqrt{2}) = 2\sqrt{2},\ f(-2 - \sqrt{2}) = -2\sqrt{2},\ f(-1 + \sqrt{2}) = \sqrt{2},\\
&f(-1 + 2\sqrt{2}) = 2\sqrt{2},\ f(-1 - 2\sqrt{2}) = \sqrt{2},\ f(-1 - \sqrt{2}) = -2\sqrt{2}
\end{aligned}$$

Hence we can see that these values are always a non-square in $\mathbb{F}_q$.

They have found this example by trial and error. [Ball and Lavrauw, 2002, p. 8] showed that this example is isotopic to a Dickson, Kantor, Knuth semifield.

2.4.2 Knuth's example

Another example is from [Knuth, 1965, p. 184]. We will again expand some arguments.

Example. Let $(S, +, *)$ be a two-dimensional vector space over $\mathbb{F}_4$. The elements of S are of the form $a + t * b$, where a, $b \in \mathbb{F}_4$ and $t \in S \backslash \mathbb{F}_4$. Addition is defined component-wise as in a vector space. Multiplication in S may be defined using the multiplication and addition in $\mathbb{F}_4$, using the following rule

$$(a + t * b) * (c + t * d) = (ac + b^2 d) + t * (bc + a^2 d + b^2 d^2).$$

We can see that $\mathbb{F}_4 \subseteq S$. Now we will verify the axioms. $(S, +)$ clearly is a group, since addition in $\mathbb{F}_4$ is commutative. Also $1 \in S$ is rather straight-forward, if we take $a = 1$, $b = 0$ then we obtain $1 + t0 = 1 \in S$.

Let us denote left and right multiplication as $L_x(y) = x * y = R_y(x)$. From properties of multiplication in $\mathbb{F}_4$ follows that $L_x(y + z) = L_x(y) + L_x(z)$ holds, analogously for R_y holds $R_y(x + z) = R_y(x) + R_y(z)$ for all x, y, $z \in S$. From the proof of Lemma 3 follows that if left and right multiplication are additive as shown above, then the multiplication is distributive. Hence both distributive laws hold. Since $\mathbb{F}_4$ is a field then the product of any non-zero elements is non-zero.

Now we need to check that this multiplication does not allow zero divisors. Let us suppose that

$$(a + t * b) * (c + t * d) = 0$$

for non-zero $(a, b) \in \mathbb{F}_4 \times \mathbb{F}_4 \backslash \{(0, 0)\}$ and $(c, d) \in \mathbb{F}_4 \times \mathbb{F}_4 \backslash \{(0, 0)\}$. From the definition of multiplication we have that

$$ac + b^2 d = 0, \tag{2.13}$$

$$bc + a^2 d + b^2 d^2 = 0 \tag{2.14}$$

If $a = 0$ then by (2.13) we obtain $b^2 d = 0$. Thus either $b = 0$ or $d = 0$. If $d = 0$ then by (2.14) we get $bc = 0$. Thus either $b = 0$ or $c = 0$. In either case we obtain that either $a = b = 0$ or $c = d = 0$. If $b = 0$ then $ac = 0$ and $a^2 d = 0$. Thus either $a = 0$ or $c = d = 0$.

Now we can suppose that $a \neq 0$ and $b \neq 0$. Then by (2.13) we obtain

$$c = b^2 d a^{-1}.$$

Then by writing $b = b'a$ for some $b' \in \mathbb{F}_4^\times$ and by plugging c into (2.14) we obtain

$$\begin{aligned} bc + a^2 d + b^2 d^2 &= b^3 d a^{-1} + a^2 d + b^2 d^2 \\ &= b'^3 a^2 d + a^2 d + b'^2 d^2 a^2 \\ &= a^2 (b'^3 d + d + b'^2 d^2) \\ &= a^2 (d(b'^3 + 1) + b'^2 d^2) = 0. \end{aligned}$$

For every $x \in \mathbb{F}_4^\times$ we have $x^3 = 1$. Therefore $b'^3 = 1$ and since $ab' \neq 0$ we obtain that $d = 0$ must hold. From $c = b^2 d a^{-1}$ we get that $c = 0$. Hence $c = d = 0$.

Therefore the axiom **S3)** holds.

2.4.3 Penttila-Williams' example

Another more recent example is the Penttila-Williams semifield. This example comes from [Ball and Lavrauw, 2002, p. 6].

Example. The semifield S is of the size $(3^5)^2$ so we view S as a two-dimensional vector space over $\mathbb{F}_{3^5}$, with the multiplication defined as follows

$$(a * t + b) * (c * t + d) = t * \Big[L_1(ac) + bc + ad\Big] + L_2(ac) + bd.$$

From the remark after Lemma 11 we have that

$$L_1^2(x) + 4xL_2(x) = x^6 + x^{28} = x^6(1 + x^{22}).$$

That is we need to show that $(1+x^{22})$ is always a non-square because x^6 is a square.

Now

$$R_{11} = \left\{x^{22} | x \in \mathbb{F}_{3^5}^{\times}\right\} = \left\{y \in \mathbb{F}_{3^5}^{\times} | y^{11} = 1\right\}.$$

Since $11 \times 22 = 242 = 3^5 - 1$. Now we need to show for all $e \in R_{11}$ that $(1+e)$ is non-square. $(1+e)^{121} = -1$ for all $e \in R_{11}$.

Since

$$\frac{3^5-1}{2} = 121 = 1 + 3 + 3^2 + 3^3 + 3^4.$$

The expression

$$(1+e)^{121} = (1+e)(1+e^3)(1+e^9)(1+e^{27})(1+e^{81})$$

holds because the characteristic is 3 and therefore we have that

$$(1+e)^{3^k} = 1 + e^{3^k}$$

in our case $0 \leq k \leq 4$. Therefore

$$\begin{aligned}
(1+e)^{121} &= 1 + e + e^3 + e^4 + e^9 + e^{10} + e^{12} \\
&\quad + e^{13} + e^{27} + e^{28} + e^{30} + e^{31} + e^{36} \\
&\quad + e^{37} + e^{39} + e^{40} + e^{81} + e^{82} + e^{84} \\
&\quad + e^{85} + e^{90} + e^{91} + e^{93} + e^{94} + e^{108} \\
&\quad + e^{109} + e^{111} + e^{112} + e^{117} + e^{118} + e^{120} + e^{121} \\
&= (1+e)(1+e^3)(1+e^9)(1+e^{27})(1+e^{81}) \\
&= \sum_{(a_1,a_2,a_3,a_4,a_5) \in \{0,1\}^5} e^{a_1 1 + a_2 3 + a_3 3^2 + a_4 3^3 + a_5 3^4 \,(\mathrm{mod}\, 11)}.
\end{aligned}$$

Using a computer we observed that running over all

$$(a_1,\, a_2,\, a_3,\, a_4,\, a_5) \in \{0,1\}^5$$

we see

$$a_1 1 + a_2 3 + a_3 3^2 + a_4 3^3 + a_5 3^4 \,(\mathrm{mod}\, 11)$$

takes every non-zero value exactly three times and zero exactly twice. Since the characteristic is three then

$$(1+e)^{121} = 2 = -1.$$

Therefore S is a semifield.

Conclusion

In this thesis we have studied the algebraic objects known as finite semifields. First we went through the preliminaries, the basics of what is necessary to know to study the semifields. In the second chapter we have studied the commutative and non-commutative cases of the semifields and noticed some similarities between these two cases. In both cases we studied those semifields that are rank two over their nuclei.

Bibliography

Simeon Ball and Michel Lavrauw. Commutative semifields of rank 2 over their middle nucleus. In *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, pages 1–21. Springer, Berlin, 2002.

Aart Blokhuis, Michel Lavrauw, and Simeon Ball. On the classification of semifield flocks. *Adv. Math.*, 180(1):104–111, 2003. ISSN 0001-8708. doi: 10.1016/S0001-8708(02)00084-1. URL https://doi.org/10.1016/S0001-8708(02)00084-1.

Stephen D. Cohen and Michael J. Ganley. Commutative semifields, two-dimensional over their middle nuclei. *J. Algebra*, 75(2):373–385, 1982. ISSN 0021-8693. doi: 10.1016/0021-8693(82)90045-X. URL https://doi.org/10.1016/0021-8693(82)90045-X.

Leonard Eugene Dickson. Linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society*, 7(3):370–390, 1906. ISSN 00029947. URL http://www.jstor.org/stable/1986324.

Michael J. Ganley. Central weak nucleus semifields. *European J. Combin.*, 2(4):339–347, 1981. ISSN 0195-6698. doi: 10.1016/S0195-6698(81)80041-8. URL https://doi.org/10.1016/S0195-6698(81)80041-8.

Donald E. Knuth. Finite semifields and projective planes. *J. Algebra*, 2:182–217, 1965. ISSN 0021-8693. doi: 10.1016/0021-8693(65)90018-9. URL https://doi.org/10.1016/0021-8693(65)90018-9.

List of Tables