SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Finite Fields: An Introduction

av

Niklas Hellberg

2025 - No L4

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Finite Fields: An Introduction

Niklas Hellberg

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Boris Shapiro

2025

Abstract

This paper presents the foundational theory of finite fields through several algebraic perspectives. Our aim is to develop a clear understanding of finite field structure and to illustrate its applications in a pedagogically accessible way. We begin with a historical overview of finite fields, followed by an introduction to the core algebraic concepts. A group-theoretic approach is then used to analyze the cyclic and symmetric properties of finite fields. We subsequently examine the Frobenius map and cyclotomic cosets, emphasizing their role in describing the internal symmetries of finite fields. The theoretical basis connecting finite fields to polynomials is introduced as a basis for computational methods, while linear-algebraic viewpoints connect finite fields to vector space structures and provide the foundation for modern linear coding theory. Finally, we discuss key applications building on these theoretical frameworks and connect the material to the broader research literature.

Den här artikeln presenterar den grundläggande teorin för ändliga kroppar ur flera algebraiska perspektiv. Syftet är att utveckla en tydlig förståelse för ändliga kroppars struktur och att visa hur teorin kan tillämpas på ett pedagogiskt och lättillgängligt sätt. Vi inleder med en historisk översikt över ämnet och går därefter vidare till de centrala algebraiska begreppen. Ett gruppteoretiskt perspektiv används för att analysera de cykliska och symmetriska egenskaperna hos ändliga kroppar. Vidare behandlas Frobeniusavbildningen och cyklotomiska sidoklasser, med fokus på deras betydelse för att beskriva interna symmetrier. Den teoretiska basen som kopplar ändliga kroppar och polynom introduceras som grund för beräkningsmetoder, medan linjäralgebraiska perspektiv kopplar ändliga kroppar till vektorrumsstrukturer och utgör grunden för modern linjär kodningsteori. Avslutningsvis diskuteras centrala tillämpningar som bygger på dessa teoretiska ramar och kopplas till den befintliga forskningslitteraturen.

AI-statement

Large language AI models (LLMs) such as ChatGPT have been used sparingly throughout this project. The two primary purposes for this were first to help concretize some of the abstract proofs that were needed for a complete understanding. Second, LLMs were used to provide a few feedback examples for mathematical syntax in sections of the text.

Contents

1 Introduction **1**

2 History **2**
2.1 Before Finite Fields . . . 2
2.1.1 Gauss . . . 2
2.1.2 Galois . . . 2
2.1.3 Serret . . . 3
2.1.4 Moore . . . 3
2.1.5 Further Reading . . . 3

3 Theory **4**
3.1 Constructing Finite Fields . . . 4
3.1.1 Homomorphisms . . . 9
3.2 Polynomials . . . 12
3.2.1 Cyclotomic Cosets . . . 17
3.2.2 Functions & Irreducible Polynomials . . . 18
3.3 Linear Algebra over Finite Fields . . . 22
3.3.1 Trace & Norm . . . 23

4 Application **26**
4.1 Combinatorics . . . 26
4.1.1 Latin squares . . . 26
4.1.2 Finite Geometries . . . 27
4.1.3 Projective Planes . . . 29
4.2 Algebraic Coding Theory . . . 30

5 Discussion **31**
5.1 Understanding Finite Fields & Their Properties . . . 31
5.2 Multiple Perspectives . . . 31
5.3 Literature . . . 32
5.4 Limitations & Scope . . . 32
5.5 Connection Between Theory & Application . . . 32

1 Introduction

Finite fields are used for many things, from cryptography and algebraic coding theory to polynomial factorization and combinatorcs [15]. In addition to their versatility, their beauty as an algebraic structure has long fascinated mathematicians. Mullen and Panario [15] describe the theory of finite fields as a discipline that has its roots in the middle of the 17th century. Although Gauss was the first to present the complete body of knowledge concerning finite fields of prime orders, there were many before him that wrote about finite fields in various detail. Fermat, Dickson, Euler, and Leibniz are often mentioned when discussing the history of finite field theory [15]. Before discussing the history, let us first define fields.

Fields are algebraic structures that consist of a set of elements under the two binary operations (addition and multiplication) that satisfy a specific set of axioms. Examples of widely known fields include the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, and the complex numbers $\mathbb{C}$, [14].

Forney [8] introduces fields by first rigorously defining the integers, mod-n arithmetics, and groups.

Definition 1.1 *A field is a set $\mathbb{F}$ with at least two elements, and two binary operations $+$ and $\times$, which satisfy the following axioms:*

$\mathbb{F}1$*: The set $\mathbb{F}$ is an abelian group under $+$, with the identity 0.*

$\mathbb{F}2$*: The nonzero elements $\mathbb{F} \setminus \{0\}$ is an abelian group under $\times$, with the identity 1.*

$\mathbb{F}3$*: $+$ and $\times$ are both distributive. For all $a, b, c \in \mathbb{F}$,*

$$a \times (b \times c) = (a \times b) \times c$$
$$a + (b + c) = (a + b) + c$$

[8].

With the definition of a field in place, we can try to understand why finite fields are interesting. A field must satisfy all the group axioms under addition (making $(\mathbb{F}, +)$ an abelian group). It must also form an abelian group under multiplication when 0 is excluded. These axioms include, in particular, the requirements that both are closed.
In a finite field, closure under addition has the consequence that consecutive addition cannot reach infinity like $\mathbb{Q}$ or $\mathbb{R}$. Instead, we must make it so that it "wraps around" and returns to 0. This cyclical nature of addition in finite fields is the first glimpse that finite fields have a very unique and elegant algebraic structure. One way to achieve such a cyclical structure is to make use of modular arithmetic. Finite field structure means that each element in a finite field is an equivalence class of an integer modulo-p, where p is a prime. This means that both binary operations within a finite field are defined modulo-p, thus fulfilling the requirement of closure.
Our goal is to learn about these aspects and, in a digestible manner, introduce them to the reader. Furthermore, an additional aim is to investigate various ways to view finite fields. As such, the research questions this paper aims to answer are:

1. What are finite fields?
2. What properties do finite fields have?
3. What different perspectives can we use to undestand finite fields?
4. What are finite fields used for, both historically and contemporarily?

To begin, let us in Chapter 2 look at the rich history of finite field theory.

2 History

Let us begin by stating the difficulties that arise when writing about the history of a mathematical subject or theory. Brechenmacher [2] says that a common issue is how to select the texts to analyze and where to limit what is relevant to the field. The tension of mathematical discoveries between mathematicians, institutions, and nations is also something to keep in mind as not to strip a mathematical discovery from its context. Both [15] and [2] do this well, and most of the information in this chapter is borrowed from those texts. Since the volume of this paper is limited, a narrow selection of relevant mathematicians and historical context has been made to represent the topic. Additionally this chapter will be structured chronologically for the ease of understanding.

2.1 Before Finite Fields

Some of the earliest work that can be interpreted using the language of finite fields is Fermat's Little Theorem, which says that $x^{p-1} - 1$ is divisible by p when p is prime and x is not divisible by p. Mathematicians in ancient China around 500 BCE already knew the special case of Fermat's Little Theorem that occurs when $x = 2$. In 1640, Pierre de Fermat (1601-1665) sent a formulation same theorem in a letter to Bernard Frénicle de Bessy (1605-1675) without proving it. The proof was later found by Leonard Euler (1707-1783) in his 1736 article [6]. Later investigation of Leibniz (1646-1716) notes revealed that he had also developed a proof in 1680 that remained unpublished. [15]

Mullen and Panario [15] discuss the occurence of theorem's that were expressed in the terms of congurences modulo a prime by Euler, Joseph-Louis Lagrange (1736-1813), and Adrien-Marie Legendre (1752-1833) during the 1700's being precursors to the basic facts of finite fields.

2.1.1 Gauss

Carl Friedrich Gauss (1777-1855) is of immense importance to the theory of finite fields among many others. His 1801 paper *Disquisitiones Arithmeticae* [9] is considered to be Gauss' magnum opus. Mullen and Panario [15] describe how this work far exceeded the criterion of what could be considered a mathematical proof during his time and included a large amount of terminology and symbols, which later became widespread for denoting the respective concepts. Some of these include the symbol $\equiv$ to denote congruence, the use of ϕ to denote Euler's totient function, and the use of the exclamation mark.

Concerning finite fields, the most important is the result in section 2, Art. 14. that if p is prime and a, b are integers not divisible by p, then p does not divide the product of ab. This result essentially shows that the integers (modulo-p) form a field. [15]

After Gauss's death, an omitted eighth section of Gauss' *Disquisitiones Arithmeticae* was found and published in his anthology in 1863 [10]. There, Gauss investigated polynomials modulo a prime and illuminated extensions of a field of prime order. He also introduced the concept of a prime polynomial, now known as an irreducible polynomial, and showed that an arbitrary polynomial can be factored into a product of prime polynomials. [15]

2.1.2 Galois

Évartiste Galois (1811-1832) is the first mathematician to present what is now considered to be a modern view of the theory of finite fields in his paper *Sur la théorie des nombres* published in 1830. Mullen and Panario [15] explain that Galois established the structure of addition and multiplication of the finite extensions of fields of prime order. In other words, Galois established the structure for finite fields of prime power order. Additionally, Galois' paper discusses irreducible integer polynomials (although not using these terms) with the following definition.

Definition 2.1 *An integer polynomial $F(x)$ is irreducible modulo a prime p if it is impossible to find three integer polynomials $\phi(x)$, $\psi(x)$, and $\chi(x)$ such that,*

$$F(x) + p\chi(x) = \phi(x)\psi(x).$$

We can understand this definition by saying that two polynomials are congruent modulo-p if they differ by a multiple of p. This is the same as saying:

$$F(x) - \phi(x)\psi(x) = p\chi(x), \text{ for some } \chi(x) \in \mathbb{Z}[x].$$

Mullen and Panario further point out that Galois' paper had many errors, false assumptions, and poor structure. They also mention the triviality of these errors and say that they in no way diminish the validity of his theory. Galois name became synonymous with finite fields, and nowadays, they are often referred to as Galois fields. [15]

2.1.3 Serret

Joseph-Alfred Serret (1819-1885) was a major contributor to the decoding and reintroduction of Galois's work to the more general mathematical world, as he collected the text into more digestible information for his lectures. These lectures were summarized in the textbook *Cours d'algebre supérieure* [20]. Serret was also responsible for developing an arithmetic approach for defining finite fields which E.H. Moore later brought to the forefront. [2]

2.1.4 Moore

Finally, let us mention Eliakim Hastings Moore (1862-1932) who both Mullen and Panario [15], and Brechenmacher [2] acknowledge as prominent in introducing the abstract theory of finite fields to modern mathematics. He compiled the findings of many mathematicians surrounding the subject into lectures and papers.

2.1.5 Further Reading

This chapter has summarized the history of the mathematical theory of finite fields briefly, and for further reading, we suggest the following texts. Firstly, of course Mullen and Panario [15] and Brechenmacher [2]. Additionally Theodor Schönemann's (1812-1868) paper *Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist* [19] and Camille Jordan's (1838-1922) *Traité des substitutions et des équations algébriques* [12].

3 Theory

3.1 Constructing Finite Fields

This chapter will outline the basic theory of finite fields, i.e. how to construct them. To understand the basic theorems concerning finite fields and their construction, some definitions and theorems are needed. Most of these definitions can be found in Earl and Nicholson's *the Oxford Concise Dictionary of Mathematics* [4] and theorems and proofs are mostly cited from Lidl and Neiderreiter's *Finite Fields* [13] along with Forney's *Introduction to Finite Fields* [8]. We begin by defining some algebraic structures that will be of importance to the later theorems.

Definition 3.1 *Let $n \in \mathbb{N}$. Define a relation $\equiv$ (modulo-n) on $\mathbb{Z}$ by $a \equiv b$ (modulo-n) $\Leftrightarrow \quad n|(a-b)$. A residue class is an equivalence class with respect to this relation. For $a \in \mathbb{Z}$, we write*

$$[a] = \{a + kn \mid k \in \mathbb{Z}\}.$$

A residue class modulo-n can be represented as $[0], [1], [2], ..., [n-1]$ and the binary operations $+$ and $\times$ on them can be represented as

$$[a] + [b] = [a + b] \text{ and } [a] \times [b] = [a] \times [b] \text{ respectively,}$$

[4].

Note that $\mathbb{N}$ does not include 0 in definition 3.1 since divisibility with zero is undefined.

Example: The residue classes modulo 4 can be represented as $[0], [1], [2], [3]$ a where $[2] = -6, -2, 2, 6, 10, 14$ (modulo-4).

We will now look at the concept of ideals. We stress that the reader must understand these concepts.

Definition 3.2 *An ideal is a subring $\mathbf{I}$ of a ring $\mathbf{R}$ where for each $i \in \mathbf{I}$ and for each $r \in \mathbf{R}$ both ir, ri are in $\mathbf{I}$, [4].*

Example: Let $\mathbb{Z}$ be the ring of integers. Take the subring $\mathbf{I} = 3\mathbb{Z} = \{..., -6, -3, 0, 3, 6, ...\}$. $\mathbf{I}$ is closed under addition. $\mathbf{I}$ is also closed under multiplication.

Using the same approach, we can create ideals for any integer $n \in \mathbb{Z}$.

Definition 3.3 *A maximal ideal is an ideal I of a ring R that is maximal with respect to inclusion. This means that if J is an ideal such that $I \subseteq J \subseteq R$, then $I = J$ or $I = R$, [4].*

Definition 3.4 *A principal ideal is an ideal such that a well-defined quotient ring $\mathbf{R}/\mathbf{I}$ can be defined, [4].*

Definition 3.5 *An integral domain is a commutative ring $\mathbf{R}$ with identity and the additional property that for all $a, b \in \mathbf{R}$, $ab = 0$ only if either $a = 0$ or $b = 0$, [4].*

With these definitions we can proceed to the theorems that describe how to construct finite fields. These become the foundations for the rest of the text.

Theorem 3.1 *Every finite integral domain is a field.*

To prove this, we need to prove that every nonzero element has a multiplicative inverse and that the nonzero elements form an abelian group.

Proof: Let $a_1, a_2, ..., a_n$ be elements in a finite integral domain $\mathbf{R}$.
The product of a fixed nonzero element $a \in \mathbf{R}$ and each other element within $\mathbf{R}$ must be distinct due to the properties of an integral domain.
Indeed, otherwise if $aa_i = aa_j$, then since $a \neq 0$ it must be true that either $a_i - a_j = 0$, or $a_i = a_j$. Thus each element in $\mathbf{R}$ is of the form aa_i.

This is particularly true for, $e = aa_i$ for some i with $1 \leq i \leq n$, where e is the identity element of $\mathbf{R}$.
Since $\mathbf{R}$ is commutative, it is also true that $a_i a = e$ and so a_i is the multiplicative invers of a.

As such, the nonzero elements of $\mathbf{R}$ form an abelian group and $\mathbf{R}$ is a field, [13]. □

Theorem 3.2 *The ring $\mathbb{Z}/(p)$ of residue classes of integers modulo the principal ideal generated by a prime p, is a field.*

Proof: With the help of Theorem 3.1 it is enough to prove that $\mathbb{Z}/(p)$ is an integral domain.

Since $\mathbb{Z}/(p)$ consists of the residue classes modulo the principal ideal generated by a prime p it is true that, for every $[a], [b] \in \mathbb{Z}/(p)$, $[a][b] = [ab] = 0$ if and only if, $ab = kp$ for some integer k.

Since p is prime, this can only be true, if p is a divisor to either a or b. If p is a divisor to either a or b, then, due to the properties of modular arithmetic $a = 0$ or $b = 0$, so that $\mathbb{Z}/(p)$ contains no zero divisors. [13] □

To readers who have previous experience in the abstract algebra this may seem trivial. However, for clarity let us present, the arithmetic or constructive viewpoint introduced by Serret, [2].

Theorem 3.3 *For every prime p, the set $R_p = \{0, 1, ..., p-1\}$ forms a field $\mathbb{F}_p$ under $+$ and $\times$ (modulo-p),* [8].

Proof: We already understand that the elements of $\mathbb{F}_p$ form an abelian cyclic group under $+$ modulo-p. Associativity, distributivity, and commutivity follows the properties of ordinary addition and multiplication, and the multiplicative identity is 1.

Let us show that every element in $\mathbb{F}_p \backslash \{0\}$ has a multiplicative inverse using Bézout's identity. Take a nonzero element $a \in \mathbb{F}_p$. Since p is prime $gcd(a, p) = 1$. As such there exists $u, v \in \mathbb{Z}$ that form a linear combination $au + pv = 1$. Reducing (modulo-p) gives $au \equiv 1$. So, u is the multiplicative inverse of a.

Thus $\mathbb{F}_p \backslash \{0\}$ forms a multiplicative abelian group and $\mathbb{F}_p$ is a field. □

With Theorem 3.2 and Theorem 3.3 established, let us look at an example.

Example: Take $p = 5$. Then $\mathbb{Z}/(p)$ consists of [0], [1], [2], [3], and [4]. We can describe the operations in this field by the tables below:

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

×	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

From now on, we will denote the equivalence class $[a]$ simply as a. Keep in mind that when we are discussing finite fields, the elements contained within them are equivalence classes and not numbers.

Definition 3.6 *Let* $\mathbf{G}$ *be a group with a binary operation* $*$*. If* $\mathbf{H}$ *is a subset of* $\mathbf{G}$ *that forms a group under the same operation, then* $\mathbf{H}$ *is a subgroup of* $\mathbf{G}$*, [4].*

Definition 3.7 *Let* $\mathbf{G}$ *be a group. Let* a *be an element in* $\mathbf{G}$ *and* r *an integer. The elements* a^r *forms a subgroup of* $\mathbf{G}$ *generated by* a*. The group* $\mathbf{G}$ *is called cyclic if there exists an element* a *such that* a *generates all the elements in* $\mathbf{G}$*, [4].*

It is very important to note that not every element in a finite field generates the cyclic group $\mathbb{F}_q^\times$. We can note the element 1 as an example.

Definition 3.8 *The generator* a *of a cyclic group* $\mathbb{F}_q^\times$ *is called a primitive element of* $\mathbb{F}_q$*.*

Example: As an example of a cyclic group, we can look at the multiplicative group for the finite prime field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. We denote this multiplicative group as $\mathbb{F}_7^\times$. We can use the element 3 as a generator to construct all the other elements in the group *(Remember that although we write* $0, 1, 2...$ *these elements are indeed still equivalence classes and not numbers, and that we are now working modulo-7).*

$$\begin{aligned}
3^1 &\equiv 3 \\
3^2 &= 9 \equiv 2 \\
3^3 &\equiv 3 \cdot 2 = 6 \\
3^4 &\equiv 3 \cdot 6 = 18 \equiv 4 \\
3^5 &\equiv 3 \cdot 4 = 12 \equiv 5 \\
3^6 &\equiv 3 \cdot 5 = 15 \equiv 1.
\end{aligned}$$

As we can see, every element in $\mathbb{F}_7^\times$ is reached using 3. This means that $\mathbb{F}_7^\times$ is cyclic and 3 is its generator. We can visualize this as a circle with every element in the group in the order of successive powers of three.

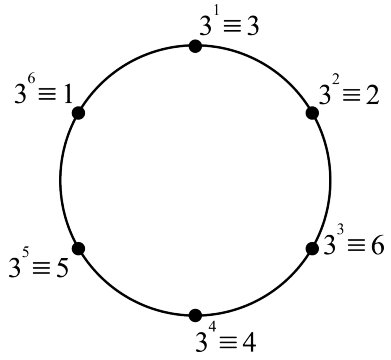

Figure 1: Cyclic multiplicative group $\mathbb{F}_7^\times$. (Adapted and modified from [8])

Remark. Theorem 3.3 defined what we call the prime fields, which are clearly finite since they contain a finite set of elements. These are the simplest finite fields, and with this information, we can now define extention fields.

Definition 3.9 *For a positive integer* n*, let* $\phi(n)$ *be the number of positive integers less than* n *that are coprime to* n*. Then we call* ϕ *Euler's totient function.*

$$\phi(n) = |\{k \in \mathbb{Z} : 1 \leq k \leq n,\ gcd(k, n) = 1\}|.$$

Sometimes Euler's function is written as φ, but we prefer to use ϕ to denote it and to distinguish it from morphisms which we denote by φ. Additionally we will use Φ to denote cyclotomic polynomials.

Example: $\phi(12) = 4$ since $1, 5, 7, 11$ are all coprime to 12.

ϕ is useful for many reasons. One of them is that $\phi(n)$ gives us the number of generators of a cyclic group of order n. Therefore, since $\mathbb{F}_{p^m}^{\times}$ is cyclic of order $p^m - 1$, $\phi(p^m - 1)$ gives the amount of primitive elements in $\mathbb{F}_{p^m}$.

Definition 3.10 *Let* $\mathbf{G}$ *be a group and let* g *be an element of* $\mathbf{G}$*. We say that* g *is of order* n *if* n *is the smallest positive integer such that* $g^n = e$*, where* e *is the identity element of* $\mathbf{G}$*, [4].*

Theorem 3.4 ***(Lagrange's Theorem)*** *Let* $\mathbf{G}$ *be a finite group and let* $\mathbf{H}$ *be any subgroup of* $\mathbf{G}$*. Then the order of* $\mathbf{H}$ *divides the order of* $\mathbf{G}$*. In particular, any element in a finite group divides the order of the group, [14].*

Proof: Let $h \in \mathbf{G}$. Define an equivalence relation on $\mathbf{G}$ as follows. For any $g_1, g_2 \in \mathbf{G}$, we say that g_1 and g_2 are equivalent if there exists an integer n such that:

$$g_1 = h^n g_2.$$

We can verify that this relation satisfies the condition for an equivalence relation, namely.

- reflexive condition: $g = h^0 g$,
- symmetric condition: If $g_1 = h^n g_2$, then $g_2 = h^{-n} g_1$,
- transative condition: If $g_1 = h^m g_2$, and $g_2 = h^n g_3$, then $g_1 = h^{m+n} g_3$.

This means that g_1 and g_2 differ by a power of h. Each equivalence class under this relation can be written as

$$[g] = \{g, hg, h^2 g, h^3 g, \dots\},$$

which corresponds precisely to a left coset of the cyclic subgroup $\langle h \rangle$ generated by h. The number of distinct elements in $\langle h \rangle$ is, by definition, the order of h. Therefore, each equivalence class contains exactly $\text{ord}(h)$ elements.

Since these equivalence classes (cosets) are disjoint and together cover the entire group G, it follows that

$$|\mathbf{G}| = k \cdot \text{ord}(h)$$

for some integer k, representing the number of distinct equivalence classes. Consequently, the order of h divides the order of $\mathbf{G}$, [14]. □

This useful theorem help to prove other results. One of the biggest consequences of this is as follows.

Theorem 3.5 *If* $\mathbb{F}$ *is a field with* q *elements and* a *is a nonzero element in* $\mathbb{F}$*, then* $a^{q-1} = 1$*. Also* $a^q = a$ *for all* $a \in \mathbb{F}$*.*

Proof: The result is immediate when $a = 0$. If $a \neq 0$, we know that a is an element in $\mathbb{F}$. There are $q - 1$ elements in the multiplicative group of nonzero elements of $\mathbb{F}$. Thus, according to Lagrange's Theorem 3.4, the multiplicative order of a in $\mathbb{F}$ divides $q - 1$. Therefore $a^{q-1} = 1$ and $a^q = a$, [14]. □

Definition 3.11 *The characteristic of a field is the smallest integer* n *such that* n *times of the multiplicative identity equals the additive identity. If no such* n *exists, the field is said to have the characteristic* 0*.*

Example: Take the finite field $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. This field has the multiplicative identity 1 and the additive identity 0. The multiplicative identity 1 has to be added 5 times to reach the value 0. Remember that we are working under modulo-5 arithmetic in this field.

Theorem 3.6 *For each prime p and each positive integer $m \geq 1$, there exists a finite field $\mathbb{F}_{p^m}$ with p^m elements. These are called the extension fields of the prime fields $\mathbb{F}_p$ as defined in Theorem 3.3, [8][14].*

This result is only half of the theorem of existence and uniqueness of finite fields. The proof and the second half of the theorem concerning uniqueness will be discussed in Chapter 3.2. It will require some foundations in both homomorphisms and polynomials with the consideration of finite fields. If the proof of the existence feels difficult, it is recommended to return to it after Chapter 3.2.

It is also very important to note that simply because there exists a finite field with p^m elements for every prime p and every positive integer $m \geq 1$ it does not mean that every ring with p^m elements is a field. If such a ring contains a zero divisor it is not a field.

Example: In the case of $p = 3$ and $m = 2$ it is not true that the ring $\mathbf{R}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ is a field. Since $\mathbf{R}_9$ as defined contains $3 \times 3 = 0$ modulo-9 it cannot be a field.

This will also be explored deeper in Chapter 3.2 when we discuss polynomials.

3.1.1 Homomorphisms

To develop a deeper understanding of finite fields, the notion of homomorphisms is essential. It is common in mathematics to use the word isomorphism to refer to two algebraic structures that share the same intrinsic structure. [11]

Egri-Nagy and Hoffman argue that a morphism is commonly used in the sense of a map that preserves every algebraic structure property. They discuss Gauss's view of the perfect map in a cartographical sense and say that morphisms are the functions that fulfill Gauss's criteria. [5]

Definition 3.12 *A homomorphism is a function between two similar algebraic structures that preserves the relational properties of elements in the two structures, [4].*

Example: Let G and H be abelian groups and φ be a homomorphism from G onto H. The homomorphism φ preserves the operation in G in the sense that:

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2), \quad \varphi(-a) = -\varphi(a)$$

More generally to denote that the binary operation within G by $(a; b)$, then

$$\varphi(a_1; a_2) = \varphi(a_1); \varphi(a_2), \quad \varphi(a^{\smile}) = \varphi(a)^{\smile}.$$

Hhere $^{\smile}$ is the inverse, [11].

It is worth to mention that in the case of rings, or perhaps even more pertinent, fields, both binary operations are preserved under a homomorphism. It is useful to view homomorphisms as functions; similarly to how functions have additional properties such as injectives, surjectives, and bijectives, so do homomorphisms.

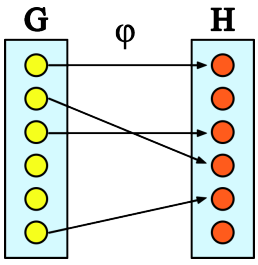

Figure 2: Homomorphism.

Homomorphism does not require the algebraic structures to have the same cardinality. Either the domain or the target algebra may be smaller than the other. One concept which will later be useful when discussing homomorphisms is the kernel.

Definition 3.13 *For a homomorphism $\varphi : G \to H$, the kernel is defined as $ker\varphi = \{g \in G | \varphi(g) = e_H\}$, where e_H is the identity element in H, [4].*

Definition 3.14 *Let $(G, +)$ and $(H, \oplus)$ be groups and φ be their morphism. We say that φ is an monomorphism, if $\varphi(g_1) = \varphi(g_2)$ means that $g_1 = g_2$. Therefore each element in the domain algebra is mapped onto a unique element in the target algebra. In other words, a monomorphism is an injective morphism, [4][11].*

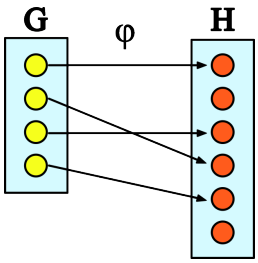

Figure 3: Monomorphism.

Definition 3.15 *Let F,G, and H be groups and $\varphi : F \mapsto G$ be a morphism. We say that φ is an epimorphism, if for every pair of morphisms $\chi, \psi : G \mapsto H$:*

$$\chi(\varphi(f)) = \psi(\varphi(f)) \Rightarrow \chi(g) = \psi(g).$$

Hhere $f \in F$ and $g \in G$. In other words, an epimorphism is a surjective morphism, [4][11].

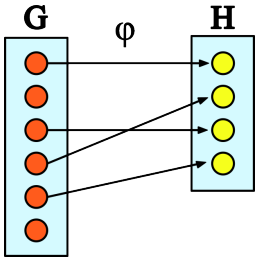

Figure 4: Epimorphism.

Definition 3.16 *Let $(G, +)$ and $(H, \oplus)$ be groups and $\varphi : G \to H$ be a morphism. We say that φ is an isomorphism, if there is a one-to-one correspondence between $(G, +)$ and $(H, \oplus)$. In other words, an isomorphism is a bijective homomorphism. If two groups are isomorphic to each other their relationship is written as $H \cong G$, [4].*

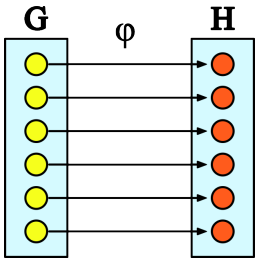

Figure 5: Isomorphism.

Rachel Rupnow [18] discusses the general idea of describing isomorphism as the "sameness", where the only difference is what notation is used to describe the algebraic structures. This is sometimes referred to by mathematicians as "naïve isomorphism". Rupnow brings up some of the implications of the isomorphic structure. If two algebraic structures are isomorphic, it also means that they have the same cardinality and as another way of thinking about isomorphisms, you may consider them as equivalence relations. This also means that algebraic structures are isomorphic to themselves, due to the reflexive property of equivalence relations.

Definition 3.17 *A morphism that maps an algebra to itself is called an endomorphism, [4].*

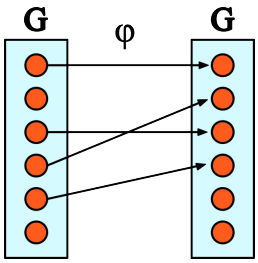

Figure 6: Endomorphism.

Definition 3.18 *A morphism that is both endomorphic, meaning that both its domain and target algebras are the same, and additionally is one-to-one, meaning that every element in the domain and in the target is reached, is called an automorphism.*

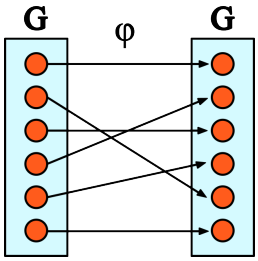

Figure 7: Automorphism.

3.2 Polynomials

This chapter will begin with some initial information that is necessary to understand the proof and continuation of Theorem 3.6. To begin with, we will look at modular arithmetic with consideration to polynomials, which is foundational for operations for polynomials over finite fields. In addition to this, we will learn about splitting fields and subfields, which is another central aspect in finite field theory.

If we look at any two polynomial $f(x)$ and $g(x)$, Euclid's algorithm tells us that $f(x)$ can be expressed as $q(x)g(x)+r(x)$, where $g(x)$ is a monic polynomial of degree m and $r(x)$ is a remainder polynomial. These compositional factors can be found for any given polynomial division. [8]

Whenever we count using polynomial modular arithmetic we say that $f(x) \equiv r(x)$, modulo-$g(x)$. All of the possible remainder polynomials in a field $\mathbb{F}$ form the set $\mathbf{R}_{\mathbb{F},m} = \{r_0 + r_1x + ... + r_{m-1}x^{m-1} | r_j \in \mathbb{F}, 0 \leq j \leq m-1\}$. The size of $|\mathbf{R}_{\mathbb{F},m}| = |\mathbb{F}|^m$. [8].

We can now outline the addition and multiplication rules of modulo-$g(x)$ arithmetic. Let $r(x) = f(x) - q(x)g(x)$ and $s(x) = h(x) - t(x)g(x)$ for some quotient polynomials $q(x)$ and $t(x)$. Furthermore, let $\oplus$ be the symbol for the addition of equivalence classes modulo-$g(x)$ and let $\otimes$ be the symbol for the multiplication of equivalence classes modulo-$g(x)$. Then

$$r(x) \oplus s(x) = (r(x) + s(x)) \; mod - g(x);$$

$$r(x) \otimes s(x) = (r(x)s(x)) \; mod - g(x), \; [8].$$

Now that we understand the modular arithmetic of polynomials, we continue by defining subfields, which will be important for us in the future. We begin with subfields and further move to splitting fields.

Definition 3.19 *Let $\mathbb{F}$ be a field with operations of $+$ and $\times$. If S is a subset of $\mathbb{F}$ that forms a field with the same operations, then S is called a subfield of $\mathbb{F}$, [4].*

Example: A well-known example of a subfield is the field $\mathbb{Q}$ of rational numbers that form a subfield to the field $\mathbb{R}$ of real numbers.

To have a better initial understanding of the splitting field, it is important to note that when we say that $\mathbf{K}$ is a field, the notation $\mathbf{K}[x]$ is referring to a ring of polynomials with coefficients in the field $\mathbf{K}$.

Definition 3.20 *Let $p(x)$ be a polynomial and let r be a number. We say that r is a root of multiplicity k if*

$$p(x) = (x-r)^k q(x), \qquad \text{where } q(r) \neq 0,$$

and k is the largest such integer, [4].

Lemma 3.1 ***(The Derivative Test)*** *Let the polynomial $p(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ be an element of $\mathbb{F}[x]$, where $\mathbb{F}$ is a field. Define the derivative of $p(x)$ as:*

$$p'(x) = na_nx^{x-1} + (n-1)a_{n-1}a^{n-2} + ... + a_1$$

A root r of $p(x)$ has a multiplicity greater than 1 if and only if $p'(r) = 0$, [14][13].

Proof: Suppose that the multiplicity of r is $k \geq 1$. We write $p(x) = (x-r)^k q(x)$. Now we can show that the formal derivative obeys the same algebraic formula as the familiar derivative.

$$D(x^ix^j) = D(x^{i+j}) = (i+j)x^{i+j-1} = ix^{i+j-1} + jx^{i+j-1} = ix^{i-1}x^j + jx^{j-1}x^i, \text{ (Product Rule).}$$

Since multiplication and the operation of derivation are both bilinear, meaning that they are linear with respect to each variable independently [4], we get:

$$D(fg) = D(f)g + fD(g).$$

We know that $D(x-r) = 1$ and $D((x-r)^k) = k(x-r)^{k-1}$ and can immediately see that for $p(x) = (x-r)^k q(x)$ we get

$$D(p(x)) = k(x-r)^{k-1}q(x) + (x-r)^k q'(x).$$

It is then clear that if $k > 1$, then $p'(r) = 0$ and if $k = 1$, then $p'(r) = q(r) \neq 0$, [14]. □

Definition 3.21 *Let $f \in \mathbf{K}[\mathbf{x}]$ be a polynomial of positive degree and let $\mathbb{F}$ be an extension field of $\mathbf{K}$. f is said to split in $\mathbb{F}$ if f can be written as a product of linear factors in $\mathbb{F}[x]$. In other words, if there exists elements $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{F}$ such that*

$$f(x) = a(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n),$$

Where a is the leading coefficient of f. The field $\mathbb{F}$ is called a splitting field of f over $\mathbf{K}$ if f splits in $\mathbf{F}$ and if, $\mathbb{F} = \mathbf{K}(\alpha_1, \alpha_2, ..., \alpha_n)$, [13].

The importance of $\mathbb{F} = \mathbf{K}(\alpha_1, \alpha_2, ..., \alpha_n)$ is related to the fact that it means that $\mathbb{F}$ is the smallest field that contains both the field $\mathbf{K}$ and all the roots of the polynomial f.

Now that we have a definition of splitting fields, we can finally prove Theorem 3.6 that we formulated in Chapter 3.

Proof: Assume that q is of the form p^m where p is a prime. Consider the polynomial $r(x) = x^q - x$ with coefficients in the field $\mathbb{F}_q$ and let $\mathbb{F}$ be a splitting field of $r(x)$ over $\mathbb{F}_q$.
Consider the set $\mathbf{S} = \{a \in \mathbb{F} \mid a^q - a = 0\}$.

We can see that the derivative of $r(x)$ becomes

$$r'(x) = qa^{q-1} - 1$$

and using Lagrange's Theorem 3.4 we realise that $a^{q-1} = 0$, therefore $r'(x)$ is identically -1. The derivative test (Lemma 3.1) then says that $r(x)$ has no multiple roots, meaning that it has no repeating roots.

Since we have no multiple roots we can clearly see that $r(x)$ has q different roots and therefore $|S| = q$. We can now move on to verify that S is a subfield

We can first notice that we only have to check that the operations and identity elements need to be verified for a^q and not for $a^q - a$, since we know that $a^q - a = 0$. Let us verify various axioms and use Lagrange's Theorem 3.4:

- $(a+b)^q = a^q + b^q = a + b$,
- $(ab)^q = a^q b^q = ab$,
- $(-a)^q = -a$,
- $(a^{-1})^q = a^{-1}$

This verifies that S is a subfield and thus S is a finite field with $q = p^m$ elements, [14]. □

The first axiom makes use of the Freshman's Dream, a common mistake in elementary mathematics, where one incorrectly expands a binomial power of 2. However, it is true that this behavior is correct in this instance. Indeed, let us use the binomial theorem. Recall that for any commutative ring, it is true that:

$$(a+b)^q = \sum_{k=0}^{q} \binom{q}{k} a^{q-k} b^k, \text{ for } 0 < k < p^m$$

We can now recall that since $q = p^m$ then every binomial coefficient $\binom{p^m}{k}$ is divisible by p. Therefore $\binom{p^m}{k} \equiv 0$, modulo-p and thus all the binomial coefficients dissapear.

Now we understand the existence part of Theorem 3.6 and may continue with the uniqueness part of the theorem.

Theorem 3.7 *(Theorem 3.6 Continuation) Any finite field with p^m elements is isomorphic to the splitting field of $x^{p^m} - x$ over $\mathbb{F}_p$, [14].*

Proof: We begin by acknowledging that if the field $\mathbb{F}_{p^m}$ has p^m elements, then by Definition 3.11 it must have the characteristic p. Theorem 3.6 states that $\mathbb{F}_{p^m}$ is an extension field of $\mathbb{F}_p$ which in turn means that $\mathbb{F}_p$ is a subfield of $\mathbb{F}_{p^m}$. In fact $\mathbb{F}_p$ is the smallest subfield which behaves exactly like $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

We know that every element of $\mathbb{F}_{p^m}$ is a root of the polynomial $x^{p^m} - x$ as follows from Lagrange's Theorem 3.4 where $a^{p^m} = a$. Conversely $\mathbb{F}_{p^m}$ contains all of the polynomial roots since the polynomial $x^{p^m} - x$ is of degree p^m. Thus there exists exactly one finite field $\mathbb{F}_{p^m}$ for every prime p and integer m up to isomorphism, [14]. □

Example: Let us look at the finite field $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. i.e, let $p = 7$ and $m = 1$.

Each of these elements must be a root to the polynomial $x^{p^m} - x$, and furthermore, they must be all of its roots. To test this we can simply perform the long line of multiplications given by

$$x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6), \text{ modulo-7}$$

This will lead to the cumbersome polynomial

$$x^7 - 21x^6 + 175x^5 - 735x^4 + 1624x^3 - 1764x^2 + 720x \equiv x^7 - x, \text{ modulo-7.}$$

This is exactly the polynomial $x^{p^m} - x$.

We can look at the same concept through a different lens. By continuing from Theorem 3.3 we can instead handle this via residue classes. Consider the polynomial ring $\mathbb{F}_p[x]$, which includes every polynomial modulo the prime p.

Theorem 3.8 *If $g(x)$ is an irreducible polynomial in $\mathbb{F}_p[x]$ of degree m, then the residueclass modulo-$g(x)$ that one gets by considering the quotient*

$$\frac{\mathbb{F}_p[x]}{(g(x))},$$

is a finite field with exactly p^m elements, [8] .

Note that when we write $(g(x))$, we refer to the ideal generated by $g(x)$, which consists of all multiples of $g(x)$. We can write that $(g(x)) = \{h(x)g(x) | h(x) \in \mathbb{F}_p[x]\}$.

Example: For further clarity, we will look at an example.

$$\mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)}$$

Here we take the polynomial ring with coefficients in $\mathbb{F}_2$ and form its quotient modulo the irreducible polynomial $g(x) = x^2 + x + 1$. We know that $g(x)$ is irreducible since it has no roots in $\mathbb{F}_2$. Namely,

$$g(0) = 1 \neq 0$$
$$g(1) = 1 + 1 + 1 = 1 \neq 0.$$

The result is the finite field $\mathbb{F}_4 = \{0, 1, x, x+1\}$ where the elements are the equivalent classes obtained using polynomial division, thereby making operations on coefficients modulo-2 and operations on polynomials modulo-$(x^2 + x + 1)$. From this we get the operation tables:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Definition 3.22 *Let* $\mathbf{I}$ *be an ideal in a ring* $\mathbf{R}$*, then the coset of an element* $r \in \mathbf{R}$ *is defined as*

$$r + I = \{r + i | i \in \mathbf{I}\}, \text{ [4].}$$

Theorem 3.9 *Let* $g(x)$ *be a monic irreducible polynomial over a finite field* $\mathbb{F}$ *with* p^m *elements. The roots of the polynomial is a set of the form* $\{\alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{p^{n-1}}\}$*, where* n *is a divisor of* m*. Moreover,* $g(x)$ *divides* $x^{p^m} - x$*,[8].*

Proof: Let α be a root of $g(x)$. For the same reason as in the proof of Theorem 3.6, where we argued the legitimacy of the freshman's dream using the binomial theorem, $g(\alpha^p) = g^p(\alpha) = 0$. As such, α^p is a root of $g(x)$. Iterating this argument, we find that $\alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{p^i}, ...$ are all roots of $g(x)$.

These roots cannot be distinct since $\mathbb{F}$ is finite. Therefore, let n denote the smallest integer such that $\alpha^{p^n} = \alpha$. As such $\alpha^{p^j} \neq \alpha$ where $1 \geq j < n$. This means that all elements in $\{\alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{n-1}\}$ are distinct and we see that $\alpha, \alpha^p, \alpha^{p^2}, ...$ form a cyclic sequence if and only if n is a divisor of j. Since $\alpha^{p^m} = \alpha$, we see that n must divide m.

We can now show that these roots are all of the roots of $g(x)$. In other words, we say that $g(x)$ is of degree n, which in turn makes the n roots we have found to be the only possible roots of $g(x)$.

Introduce a polynomial $h(x) \in \mathbb{F}[x]$ of degree n as

$$h(x) = \prod_{i=0}^{n-1} (x - \alpha^{p^i}).$$

We can now show that $h^p(x) = h(x^p)$. This can be seen as follows:

$$h^p(x) = \prod_{i=0}^{n-1} (x - \alpha^{p^i})^p = \prod_{i=0}^{n-1} (x^p - \alpha^{p^{i+1}}) = \prod_{i=0}^{n-1} (x^p - \alpha^{p^i}) = h(x^p).$$

Here we once again use the fact that $\alpha^{p^m} = \alpha$. Since, $g(x)$ has no factors in $\mathbb{F}[x]$, $g(x)$ must be equal to $h(x)$ and since the roots of $g(x)$ all satisfy $\alpha^{p^m} = \alpha$, they are all the roots of $g(x)$ and $g(x)$ divides $x^{p^m} - x$, [8]. □

Definition 3.23 *Let* $\mathbf{F}/\mathbf{K}$ *be a field extension and let* $\alpha \in \mathbf{F}$*. The minimal polynomial of* α *over* $\mathbf{K}$ *is the unique monic polynomial* $m_\alpha(x) \in \mathbf{K}$ *of smallest degree, such that* $m_\alpha(\alpha) = 0$*.*
The monic polynomial $m_\alpha(x)$ *is irreducible over* $\mathbf{K}$*, [8][4].*

Definition 3.24 *The endomorphism defined as* $\varphi(x) = x^p$ *that maps* $\mathbb{F} \to \mathbb{F}$ *is called the Frobenius endomorphism, or the Frobenius map. If* $\mathbb{F}$ *is finite it is an automorphism and generates the Galois group of* $\mathbb{F}$ *over the prime subfield, [4].*

The Frobenius map $\varphi(x) = x^p$ acts as an automorphism on any finite field $\mathbb{F}_{p^m}$, transforming its elements while fixing its prime subfield $\mathbb{F}_p$. Frobenius maps also act on the exponents of elements in the multiplicative group $\mathbb{F}_{p^m}^\times$. Multiplication corresponds to the addition of exponents. This means that exponentiation

wraps around when the exponent reaches $p^m - 1$. This means that it acts as addition modulo-$(p^m - 1)$. [14][15]

When we say that an element is fixed under a morphism such as the Frobenius map, we mean that the morphism maps the element to itself. In other words, an element a is fixed if $\varphi(a) = a$. As an example, the reader may note that the Frobenius map fixes all elements in the prime field $\mathbb{F}_p$, since $a^p = a$.

Definition 3.25 *Let $\mathbb{F}_{p^m}$ be an extension of $\mathbb{F}_p$ and let $\alpha \in \mathbb{F}_{p^m}$. Then, $\alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{p^{m-1}}$ are called conjugates of α with respect to $\mathbb{F}_p$, [13].*

3.2.1 Cyclotomic Cosets

As described previously, cyclotomic cosets are orbits under exponentiation. So, whenever, we are studying cyclotomic cosets, we are essentially looking at the orbits generated by applying the Frobenius map.

Definition 3.26 *Let n be a positive integer. The splitting field of $x^n - 1$ over the field $\mathbf{K}$ is called the nth cyclotomic field over $\mathbf{K}$ and is denoted as $\mathbf{K}^{(n)}$.*

Furthermore, the roots of $x^n - 1$ are called the nth roots of unity over $\mathbf{K}$, and these roots are denoted by $\mathbf{E}^{(n)}$, [13].

A beautiful geometrical pattern occurs when you consider the special case when $\mathbf{K}$ is the field $\mathbf{Q}$ of rational numbers. In this case, the nth cyclotomic field $\mathbf{K}^{(n)}$ is a subfield of the field $\mathbf{C}$ of complex numbers.

Definition 3.27 *Let z be a complex number such that $z^n = 1$. It's roots are n distinct nth roots of unity $e^{i2k\pi/n}$, where $k = 0, 1, ..., n-1$.*

They are represented in the complex plane by the n vertices of a regular n-sided polygon that has its vertices on the unit circle and one vetrex is at 1. [4]

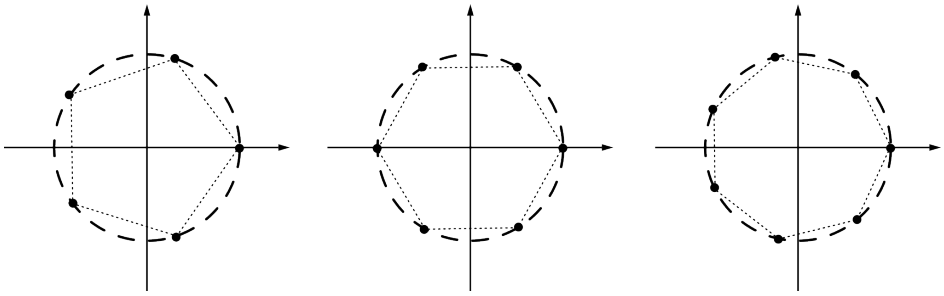

Figure 8: Representation of the roots of unity where $n = 5, 6, 7$. (Adapted and modified from [4])

Since the primitive nth roots of unity are among the roots of $z^n - 1$, there exists a unique monic polynomial whose roots are exactly the primitive nth roots. This polynomial divides $z^n - 1$ and are called the nth cyclotomic polynomial

Definition 3.28 *The nth cyclotomic polynomial $\Phi(x)$ is the monic polynomial with the primitive nth roots of unity as its roots. This means that if α is a primitive nth root of unity over a field $\mathbf{K}$, then the polynomial*

$$\Phi(x) = \prod_{i=1}^{n}(x - \alpha^i).$$

Where $gcd(i, n) = 1$, [4][13].

Example: The 5th cyclotomic polynomial $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

Definition 3.29 *let $q = p^m$ be relatively prime to an integer n, meaning that $gcd(n, q) = 1$. For an integer i, the q-cyclotomic coset modulo-n containing i is $\mathbb{C}_i = \{i, iq, iq^2, ..., iq^{r-1}\}$ where r is the smallest integer such that $iq^r \equiv i$ modulo-n, [15].*

We can make an analogy between r in the cyclotomic coset $\mathbf{C}_i$ and the characteristic of a field. They both denote a sort of operational order, but whereas the characteristic of a field denotes an additive order on a global scale, r instead denotes the local multiplicative order of q within $\mathbf{C}_i$.

3.2.2 Functions & Irreducible Polynomials

In this section, we investigate ways of constructing various polynomials using finite fields. We will begin with polynomials that reach specific points. After this, we will return to the concept of minimal polynomials from Definition 3.23 and primitive elements from Definition 3.8. These will be of use for us when later constructing irreducible polynomials.

The construction of polynomials that reach specific points is based on a property of finite fields. Namely, the property that every function in a finite field can be represented by a polynomial. This property is proven in Theorem 3.11, and it is a distinctive feature to finite fields in the sense that it does not generally hold in other commutative rings with identity. [14] The method itself is well-known in elementary analysis for constructing polynomials with real coefficients that assumes certain assigned values for given values of the indeterminate. [13]

Theorem 3.10 ***(Lagrange's Interpolation Formula)*** *Let $n \geq 0$ and let $a_0, a_1, ..., a_n$ be $n+1$ distinct elements of a field $\mathbb{F}$. Furthemore, let $b_0, b_1, ..., b_n$ be $n+1$ arbitrary elements of $\mathbb{F}$. Then, there exists exactly one polynomial $f(x) \in \mathbb{F}[x]$ of degree at most n such that $f(a_i) = b_i$ for $0 \leq i \leq n$.*

Proof: This polynomial is given by

$$f(x) = \sum_{0 \leq i \leq n} \left(b_i \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - a_j}{a_i - a_j} \right).$$

[14][13]. □

Example: Let us construct a polynomial using Lagrange's interpolation formula. First, we should assign the points that the polynomial should reach. Take the points $(0,1), (1,4), (2,3), (3,4), (4,3)$ and structure them into ordered sets $A = \{a_0, ..., a_4\} = \{0, 1, 2, 3, 4\}$ and $B = \{b_0, ..., b_4\} = \{1, 4, 3, 4, 3\}$. We must remember that the computations are done using modulo-5.

Let us first call

$$\prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - a_j}{a_i - a_j} = L_i(x)$$

We can now calculate the denominator:

$$\prod_{\substack{j=0 \\ j \neq i}}^{n} (a_i - a_j) = (a_i - 0)(a_i - 1)(a_i - 2)(a_i - 3)(a_i - 4).$$

Remember that we ignore $(a_i - a_i)$ due to the $j \neq i$ condition. We get $(-1)(-2)(-3)(-4) \equiv 4 \cdot 3 \cdot 2 \cdot 1 = 24 \equiv 4$. This gives:

$$L_i(x) = 4 \prod_{\substack{j=0 \\ j \neq i}}^{n} (x - a_j) = x^4 + a_i x^3 + a_i^2 x^2 + a_i^3 x + a_i^4,$$

Due to $a^5 = a$ in $\mathbb{F}_5$. This leads to:

$$f(x) = \sum_{0 \leq i \leq n}^{4} b_i L_i(x) = \sum_{0 \leq i \leq n}^{4} (4b_i)(x^4 + a_i x^3 + a_i^2 x^2 + a_i^3 x + a_i^4)$$

This gives us $f(x) \equiv 1 + 2x + x^3$ modulo-5. We can also confirm this by calculating,

$$\begin{aligned} f(0) &= 1, \\ f(1) &= 1 + 2 + 1 = 4, \\ f(2) &= 1 + 4 + 8 \equiv 3, \\ f(3) &= 1 + 6 + 27 \equiv 4, \\ f(4) &= 1 + 8 + 64 \equiv 3. \end{aligned}$$

Theorem 3.11 *Every function $f : \mathbb{F}_q \to \mathbb{F}_q$ can be represented by a unique polynomial over $\mathbb{F}_q$ that at most has the degree $q - 1$, [14][15].*

Proof: We want to show that there is a unique polynomial $P_f(x)$ over $\mathbb{F}_q$ that can represent each $f : \mathbb{F}_q \to \mathbb{F}_q$ such that $P_f(a) = f(a)$.

Define $P_f(x)$ as:

$$P_f(x) = \sum_{a \in \mathbb{F}_q} f(a) \left(1 - (x - a)^{q-1}\right)$$

By Lagrange's Theorem we get that $(b - a)^{q-1} = 1$ if $a \neq b$ and $(b - a)^{q-1} = 0$ if $a = b$. Let us calculate $P_f(b)$.

$$P_f(b) = \sum_{a \in \mathbb{F}_q} f(a) \left(1 - (b - a)^{q-1}\right)$$

We split the sum into two parts.

$$P_f(b) = \sum_{a \in \mathbb{F}_q} f(a) - \sum_{a \in \mathbb{F}_q} f(a)(b - a)^{q-1}.$$

Using Lagrange's Theorem we can now say that:

$$(b - a)^{q-1} = \begin{cases} 0, & a = b, \\ 1, & a \neq b. \end{cases}$$

Applied to the second of our two terms, we see that if $a = b$ then the term is equal to 0 and otherwise the term is equal to $f(a)$. Therefore we can say that our second term is:

$$\sum_{\substack{a \in \mathbb{F}_q \\ a \neq b}} f(a)$$

Thus:

$$P_f(b) = \sum_{a \in \mathbb{F}_q} f(a) - \sum_{\substack{a \in \mathbb{F}_q \\ a \neq b}} f(a) = f(b).$$

[14]. □

Now that we know that each function can be represented by a unique polynomial in $\mathbb{F}_q$, we can look at those polynomials in more detail. Besides, the degree of a polynomial there exists another property that will be of interest to us, namely, the order of a polynomial. [13]

Lemma 3.2 *Let $f \in \mathbb{F}_p[x]$ be a polynomial of degree $m \geq 1$ where $f(0) \neq 0$. Then there exists a positive integer $e \leq p^m - 1$ such that $f(x) | (x^e - 1)$, [13].*

Proof: We know that since $\frac{\mathbb{F}_p[x]}{(f(x))}$ is a finite field with p^m elements, it contains $p^m - 1$ nonzero residue classes *(Remember that when we write $(f(x))$, we refer to the ideal generated by $f(x)$).*
Since $f(0) \neq 0$ we know that x and $f(x)$ are relatively prime and therefore $f(x)$ does not divide any power of x. This means that the p^m residue classes $x^j + (f(x))$, $j = 0, 1, ..., q^m - 1$ are all nonzero.

There exists integers r, s where $0 \leq r < s \leq q^m - 1$ such that $x^r \equiv x^s$ modulo-$f(x)$. Since x and $f(x)$ are relatively prime, it follows that $x^{s-r} \equiv 1$ modulo-$f(x)$. Therefore $f(x)|(x^{s-r} - 1)$ and $e = s - r$, [13][14]. □

Definition 3.30 *Let $f(x) \in \mathbb{F}_q[x]$ be a nonzero polynomial where $f(0) \neq 0$. The least positive integer e such that $f(x)|(x^e - 1)$ is called the order of f and is denoted $ord(f) = e$. Additionally, if $f(0) = 0$, then $f(x) = x^h g(x)$, where $h \in \mathbb{N}$ and $g(x) \in \mathbb{F}_q[x]$ with $g(0) \neq 0$. Then $ord(f) = ord(g)$, [13][14].*

Theorem 3.12 *Let $f(x) \in \mathbb{F}_p[x]$ be irreducible over $\mathbb{F}_p$. Then, $ord(f)$ is equal to the order of any of the roots of $f(x)$ in the multiplicative group $\mathbb{F}_{p^m}^{\times}$*

Proof: Using Theorem 3.7 we see that $\mathbb{F}_{p^m}$ is the splitting field of f over $\mathbb{F}_p$. Let $e = ord(f)$ which means that $f(x)|(x^e - 1)$. Let α be a root of f in $\mathbb{F}_{p^m}^{\times}$, then $f(\alpha) = 0$ and $x = \alpha$ gives $(\alpha^e - 1) = 0$. This then gives that $\alpha^e = 1$.

Let t be the multiplicative order of $\alpha \in \mathbb{F}_{p^m}^{\times}$. Then, we can see that $t|e$.

By Definition 3.10 we see that $\alpha^t = 1$, which conversely gives us that α is a root of $x^t - 1$.

Since $f(x)|x^t - 1$ and $f(x)$ is minimal, we know that $e \leq t$. $e \leq t$ and $t|e$ can only be true if $t = e$. □
[13]

Corollary 3.1 *If $f \in \mathbb{F}_p[x]$ is irreducible of degree m, then $ord(f)|(p^m - 1)$.*

Proof: We saw above that $ord(f)$ equals the multiplicative order of α, when α is a root of f. Since α is an element in the multiplicative group $\mathbb{F}_{p^m}^{\times}$ we know that the order of α divides $p^m - 1$. Therefore $ord(f)|(p^m - 1)$. □
[13]

Theorem 3.13 *The number of monic, irreducible polynomials in $\mathbb{F}_q$ of degree m and order e is given by:*

$$\frac{\phi(e)}{m}$$

if $e \geq 2$ and m is the multiplicative order of q modulo-e. If $m = e = 1$ it is 2 and it is equal to 0 in all other cases.

$$\begin{cases} \frac{\phi(e)}{m}, & \text{if } e \geq 2 \text{ and } m = ord(q), \\ 1, & \text{if } (m, e) = (1, 1), \\ 0, & \text{otherwise.} \end{cases}$$

The degree of an irreducible polynomial in $\mathbb{F}_q[x]$ of order e must be equal to the multiplicative order of q modulo-e.

Proof: Let $f \in \mathbb{F}_q[x]$ be irreducible and let $f(0) \neq 0$. Then Theorem 3.12 tells us that $ord(f) = e$ if and only if all roots of f are the primitive eth roots of unity over $\mathbb{F}_q$. In other words $ord(f) = e$ if and only if f divides the cyclotomic polynomial Φ_e

We can see that by definition $ord(f) = e$ means that $f|(x^e - 1)$ and for $1 \leq d < e$, f does not divide $(x^d - 1)$. If f has a root α in some extention, then $\alpha^e = 1$ and $\alpha^d \neq 1$ for $d < e$. Therefore, α is a primitive

eth root of unity according to Definition 3.26. Thus $f|\Phi_e$.

Let ζ be a primitive eth root of unity in some extension field of $\mathbb{F}_q$. The Frobenius automorphism $\varphi : x \to x^q$ generates the Galois group of the extension:

$$\frac{\mathbb{F}_q(\zeta)}{\mathbb{F}_q}.$$

This Galois group then consists of the set of automorphisms of $\mathbb{F}_q(\zeta)$ that fix every element in $\mathbb{F}_q$, and $\varphi^i(\zeta) = \zeta^{q^i}$.

The size of the Frobenius orbit of ζ is at least $m \geq 1$ with $\zeta^{q^m} = \zeta$. Thus $\zeta^{q^m-1} = 1$. Since $ord(\zeta) = e$ this means that $q^m \equiv 1$ modulo-e. Since the minimal $m = ord(q)$ modulo-e we can see that the minimal polynomial of ζ over $\mathbb{F}_q$ has degree m. We also know that its roots are $\zeta, \zeta^q, ..., \zeta^{q^{m-1}}$.

Due to this, every irreducible factor of $\Phi_e(x)$ over $\mathbb{F}_q$ has degree $m = ord(q)$ modulo-e. This proves that if $m \neq ord(q)$ modulo-e, then there is no irreducible polynomial of order e.

We can use this to determine how many irreducible polynomials there are.

Over any finite field with $gcd(e, q) = 1$, we know that the polynomial $\Phi_e(x)$ has exactly $\phi(e)$ distinct roots which are primitive eth roots. Therefore the degree of $\Phi_e(x) = \phi(e)$ and $\Phi_e(x)$ splits over $\mathbb{F}_q$ as distinct irreducible polynomials with degree $m = ord(q)$ modulo-e. Thus the number of irreducible factors are:

$$\frac{deg(\Phi_e(x))}{m} = \frac{\phi(e)}{m},$$

which gives the count when $e \geq 2$ and $m = ord(q)$ modulo-e.

We can now finally look at the special case where $e = 1$. Here $\Phi_1(x) = x - 1$ which is the only monic irreducible polynomial of order 1. It has degree 1 which is why there is only 1, when $(m, e) = (1, 1)$, and 0 otherwise, [13]. □

3.3 Linear Algebra over Finite Fields

We have viewed finite fields through various lenses. We have defined finite fields using both abstract algebra and the constructivist arithmetic approach; we have seen finite fields used to find and count polynomials. We have explored morphisms and cyclotomic cosets. This chapter will instead use linear algebra as a new viewpoint to analyze finite fields.
To begin, we will introduce a finite field as a vector space, which is a crucial concept used in literature to count the number of elements in a finite field. [13][14]

For linear algebra, we must recall some definitions. We will begin by defining vector spaces.

Definition 3.31 *A vector space* $\mathbb{V} = (\mathbf{V}, +, \times)$ *over a field* $\mathbf{K}$ *consists of a set* $\mathbf{V}$ *with operations of addition* $+ : \mathbf{V} + \mathbf{V} \to \mathbf{V}$*, and scalar multiplication* $\times : \mathbf{K} \times \mathbf{V} \to \mathbf{V}$*, such that* $\mathbf{V}$ *is an abelian group under* $+$ *and further:*

- $\alpha(\beta v) = (\alpha\beta)v$,,
- $(\alpha + \beta)v = \alpha v + \beta v$,
- $\alpha(v + w) = \alpha v + \alpha w$,
- $1v = v$,

where $\alpha, \beta \in \mathbf{K}$ *and* $v, w \in \mathbf{V}$.

Elements of $\mathbf{K}$ *are called scalars and elements of* $\mathbf{V}$ *are called vectors, [4].*

At first glance, this definition appears almost identical to the definition of a field (Definition 1.1). To make sure the reader understands the differences between these definitions, let us point out some differences.

First notice the difference between field multiplication $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and scalar multiplication $\mathbf{K} \times \mathbf{V} \to \mathbf{V}$. Additionally, we note that the definition of a vector space does not require multiplicative inverses in $\mathbf{V}$, but only in $\mathbf{K}$. Now, for this upcoming lemma, we must also understand what the dimension of a vector space is.

Definition 3.32 *The dimension of a vector space* $\mathbb{V}$ *is the number of elements in any basis of* $\mathbb{V}$*, [4].*

Definition 3.33 *A set* $\mathbf{S}$ *of vectors is a spanning set if any vector can be written as a linear combination of elements in* $\mathbf{S}$*. If, in addition, the vectors in* $\mathbf{S}$ *are linearly independent, then* $\mathbf{S}$ *is a basis and any element in* $\mathbf{S}$ *can be referred to as a basis vector, [4].*

Lemma 3.3 *Let* $\mathbb{F}$ *be a finite field with a subfield* $\mathbf{K}$ *that contains* p *elements. Then* $\mathbb{F}$ *is a vector space over* $\mathbf{K}$ *and* $|\mathbb{F}| = p^m$ *where* m *is the dimension of* $\mathbb{F}$ *viewed as a vector space over* $\mathbf{K}$*, [14][13].*

Proof: We begin by verifying that $\mathbb{F}$ is a vector space over $\mathbf{K}$. We do this by ensuring that the vector space axioms are fulfilled.

We can see that the properties of field operations fulfill all of the axioms for vector spaces very easily. The only ones that we have to consider closer is the property of closure under scalar multiplication and the multiplicative identity of scalars.
But, ultimately, these are also fulfilled. closure under scalar multiplication is fulfilled since $\mathbb{F}$ is closed under multiplication and $\mathbf{K} \subseteq \mathbb{F}$. The multiplicative identity of the scalars is fulfilled since $\mathbf{K} \subseteq \mathbb{F}$ means that 1 is the multiplicative identity in both $\mathbf{K}$ and $\mathbb{F}$. In other words $e^{\times}_{\mathbf{K}} = e^{\times}_{\mathbb{F}}$.

Now we can move to proving that the power m is the dimension of $\mathbb{F}$ over $\mathbf{K}$.
Since $\mathbb{F}$ is finite, we can choose a basis $B = \{\beta_1, \beta_2, ..., \beta_m\}$ for $\mathbb{F}$ over $\mathbf{K}$. Therefore, any element $\alpha \in \mathbb{F}$ can be written as a linear combination $\alpha = a_1\beta_1 + a_2\beta_2 + ... + a_m\beta_m$, where every $1 \leq a_i \leq m$ is in $\mathbf{K}$. The sequence of $a_1, a_2, ..., a_m$ is uniquely determined by α. Thus, there are $|\mathbf{K}| = p$ choices for each a_i and thus $|\mathbf{K}|^m = p^m$ distinct coefficient sequences, [14]. □

3.3.1 Trace & Norm

Remember that Lemma 3.3 means that an extension field $\mathbb{F}_{p^m}$ is a vector space over the prime field $\mathbb{F}_p$. With this knowledge, we will now introduce a mapping from $\mathbb{F}_{p^m} \to \mathbb{F}_p$.

Definition 3.34 *For $\alpha \in \mathbf{F} = \mathbb{F}_{p^m}$ and $\mathbf{K} = \mathbb{F}_p$, the trace $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ of α over $\mathbf{K}$ is defined as:*

$$\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + ... + \alpha^{p^{m-1}}.$$

If $\mathbf{K}$ is the prime subfield of $\mathbf{F}$, then $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ is called the absolute trace of α and is simply denoted $\mathbf{Tr}_{\mathbf{F}}(\alpha)$, [13][15].

Note that the trace of α over $\mathbf{K}$ simply is the sum of all conjugates of α as defined in 3.25. [13] We can additionally remark that since $(\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha))^p = \mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ the trace of an element always lies in the base field $\mathbf{K}$. [15] We will continue to use $\mathbf{F}$ to denote the finite extension field $\mathbb{F}_{p^m}$ and $\mathbf{K}$ to denote the finite subfield $\mathbb{F}_p$.

Example: Let us look at the extention $\mathbb{F}_4 = \mathbb{F}_{2^2}$ of the prime field $\mathbb{F}_2$.

- $\mathbb{F}_2 = \{0, 1\}$,
- $\mathbb{F}_4 = \frac{\mathbb{F}_2}{(x^2+x+1)} = \{0, 1, x, x+1\}$.

We can see that in $\mathbb{F}_4$, $x^2 = x + 1$ and after computing the trace of each element as $\mathbf{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\alpha) = \alpha + \alpha^2$, we arrive at:

α	α^2	$\alpha + \alpha^2$	Trace
0	0	0	0
1	1	0	0
x	$x+1$	1	1
$x+1$	x	1	1

Theorem 3.14 *Let $\mathbf{K} = \mathbb{F}_p$ and $\mathbf{F} = \mathbb{F}_{p^m}$. Then the trace function $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}$ satisfies the following properties:*

Tr1 : $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha + \beta) = \mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) + \mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\beta)$ *for all $\alpha, \beta \in \mathbf{F}$;*

Tr2 : $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(c\alpha) = c\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *for all $c \in \mathbf{K}$, $\alpha \in \mathbf{F}$;*

Tr3 : $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}$ *is a linear transformation from $\mathbf{F}$ onto $\mathbf{K}$, where both $\mathbf{F}$ and $\mathbf{K}$ are viewed as vector spaces;*

Tr4 : $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(a) = ma$ *for all $a \in \mathbf{K}$;*

Tr5 : $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha^p) = \mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *for all $\alpha \in \mathbf{F}$.*

Proof:

Tr1 : We already know that in finite fields it is true that $(\alpha + \beta)^a = \alpha^a + \beta^a$ for $\alpha, \beta \in \mathbf{F}$ as we showed in Chapter 3.2 using the binomial theorem. As such we get $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha+\beta) = \alpha+\beta+(\alpha+\beta)^p+...+(\alpha+\beta)^{p^{m-1}} = \alpha + \beta + \alpha^p + \beta^p + ... + \alpha^{p^{m-a}} + \beta^{p^{m-a}} = \mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) + \mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\beta)$ for all $\alpha, \beta \in \mathbf{F}$;

Tr2 : We know that, as a result of Lagrange's Theorem 3.4, $c^{p^j} = c$ for all $j \geq 0$. Therefore we get $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(c\alpha) = c\alpha + c^p\alpha^p + ... + c^{p^{m-1}}\alpha^{p^{m-1}} = c\alpha + c\alpha^p + ... + c\alpha^{p^{m-1}} = c\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ for all $c \in \mathbf{K}$, $\alpha \in \mathbf{F}$;

Tr3 : The properties of **Tr**1 and **Tr**2 in combination with the fact that $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) \in \mathbf{K}$ for all $\alpha \in \mathbf{F}$,

show that the trace map is a linear transformation from $\mathbf{F} \to \mathbf{K}$. To prove that it maps onto, it is sufficient to find an α such that $\mathbf{Tr_{F/K}}(\alpha) \neq 0$. We can rewrite the result into the polynomial $p(x) = x^{p^{m-1}} + ... + x^p + x$ which makes it obvious that $\mathbf{Tr_{F/K}}(\alpha) = 0$ if and only if α is a root of the polynomial $p(x)$. But since the polynomial can have at most p^{m-1} roots and $\mathbf{F}$ has p^m elements, we see that this is a map onto.

Tr4 : This follows immediately from Lagrange's Theorem 3.4.

Tr5 : We can once again use the corollary of Lagrange's Theorem 3.4to show that $\mathbf{Tr_{F/K}}(\alpha^p) = \alpha^p + \alpha^{p^2} + ... + \alpha^{p^m} = \alpha + \alpha^p + ... + \alpha^{p^{m-1}} = \mathbf{Tr_{F/K}}(\alpha)$ for all $\alpha \in \mathbf{F}$.
[13] □

The trace $\mathbf{Tr_{F/K}}$ is not only a linear transformation from $\mathbf{F}$ onto $\mathbf{K}$, but it also describes all linear functions from $\mathbf{F}$ onto $\mathbf{K}$.

Theorem 3.15 *For $\beta \in \mathbf{F}$, let $\mathbf{L}_\beta : \alpha \to \mathbf{Tr_{F/K}}(\beta\alpha)$. Then $\mathbf{L}_\beta \neq \mathbf{L}_\gamma$ as long as $\beta \neq \gamma$. Additionally, the $\mathbf{K}$-linear transformations from $\mathbf{F}$ to $\mathbf{K}$ are exactly the maps of the form $\mathbf{L}_\beta$ as β varies over the elements of the field $\mathbf{F}$, [13][15].*

Proof: By to Theorem 3.14 **Tr**3 we know that each map $\mathbf{L}_\beta$ is a linear transformation. For $\beta, \gamma \in \mathbf{F}$ where $\beta \neq \gamma$, we have $\mathbf{L}_\beta(\alpha) - \mathbf{L}_\gamma(\alpha) = \mathbf{Tr_{F/K}}(\beta\alpha) - \mathbf{Tr_{F/K}}(\gamma\alpha)$. According to Theorem 3.14 **Tr**1 this is equal to $\mathbf{Tr_{F/K}}((\beta - \gamma)\alpha) \neq 0$ for suitable $\alpha \in \mathbf{F}$. Thus $\mathbf{L}_\beta$ and $\mathbf{L}_\gamma$ are distinct. Since $\mathbf{F} = \mathbb{F}_{p^m}$ and $\mathbf{K} = \mathbb{F}_p$ the maps $\mathbf{L}_\beta$ yield p^m different linear transformations from $\mathbf{F}$ into $\mathbf{K}$. Moreover, assigning arbitrary elements of $\mathbf{K}$ to the m elements of a given basis from $\mathbf{F}$ into $\mathbf{K}$ yields every linear transformation from $\mathbf{F}$ into $\mathbf{K}$. Since it can be done in p^m different ways, $\mathbf{L}_\beta$ already exhausts all possible linear transformations from $\mathbf{F}$ into $\mathbf{K}$, [13]. □

Now we have explored the basics of the trace function, which works by linearly compressing extension fields back into their subfields. But since summarizing the conjugates compresses the field linearly, we can also compress fields multiplicatively. This is done using the norm function.

Definition 3.35 *For $\alpha \in \mathbf{F} = \mathbb{F}_{p^m}$ and $\mathbf{K} = \mathbb{F}_p$, the norm $\mathbf{N_{F/K}}(\alpha)$ of α over $\mathbf{K}$ is defined as:*

$$\mathbf{N_{F/K}}(\alpha) = \alpha \cdot \alpha^p \cdot \alpha^{p^2} \cdot ... \cdot \alpha^{p^{m-1}} = \prod_{i=0}^{m-1} \alpha^{p^i} = \alpha^{(q^m-1)/(q-1)}.$$

Furthermore, we can see that the norm is (up to a sign) the constant term of the minimal polynomial (described in Definition 3.23). It follows that $\mathbf{N_{F/K}}(\alpha)$ is always an element of $\mathbf{K}$, [15][13].

Example: To show what we mean when we say that the norm is the constant term of the minimal polynomial up to sign, first take the minimal polynomial of α which is defined as $p_\alpha(x) = (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})...(x-\alpha^{p^{m-1}})$. Let us expand the minimal polynomial:

$$p_\alpha(x) = (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})...(x-\alpha^{p^{m-1}}) =$$
$$x^m - \left(\sum_{i=0}^{m-1} \alpha^{p^i}\right) x^{m-1} + \left(\sum_{i<j} \alpha^{p^i+p^j}\right) x^{m-2} - \left(\sum_{i<j<k} \alpha^{p^i+p^j+p^k}\right) x^{m-3} + ... + (-1)^m \alpha^{1+p+...+p^{m-1}}.$$

If we look closely, we can see that $\alpha^{1+p+...+p^{m-1}}$ is the norm $\mathbf{N_{F/K}}(\alpha)$ which is up to sign due to $(-1)^m$ where m determines if it is a positive or negative constant term. Furthermore, we can see that the term

$$\left(\sum_{i=0}^{m-1} \alpha^{p^i}\right),$$

is the trace function $\mathbf{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$.

Example: Let us also look at an example of the norm of a finite field. Take $\mathbf{K} = \mathbb{F}_5$ and $\mathbf{F} = \mathbb{F}_{25}$. First create $\mathbb{F}_{25}$ as usual:

$$\mathbb{F}_{25} = \frac{\mathbb{F}_5}{(x^2-2)} = \begin{matrix} [0], & [1], & [2], & [3], & [4], \\ [x], & [x+1], & [x+2], & [x+3], & [x+4], \\ [2x], & [2x+1], & [2x+2], & [2x+3], & [2x+4], \\ [3x], & [3x+1], & [3x+2], & [3x+3], & [3x+4], \\ [4x], & [4x+1], & [4x+2], & [4x+3], & [4x+4] \end{matrix}$$

Now that we have the elements of $\mathbb{F}_{25}$, let us choose $\alpha = 3 + 2x$. Additionally we can treat x^2 as 2 within $\mathbb{F}_{25}$ since we are working modulo-$x^2 - 2$ which gives us:

$$\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha) = 3^2 - 2 \cdot 2^2 = 9 - 8 = 1.$$

Thus we see that the norm of the $\alpha = 3 + 2x \in \mathbb{F}_{25}$ is equal to 1.

Theorem 3.16 *$\mathbf{K} = \mathbb{F}_p$ and $\mathbf{F} = \mathbb{F}_{p^m}$. Then the norm function $\mathbf{N}_{\mathbf{F}/\mathbf{K}}$ satisfies the following set of properties:*

N1 : $\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha\beta) = \mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha)\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\beta)$ *for all* $\alpha, \beta \in \mathbf{F}$.

N2 : $\mathbf{N}_{\mathbf{F}/\mathbf{K}}$ *maps* $\mathbf{F}$ *onto* $\mathbf{K}$ *and* $\mathbf{F}^\times$ *onto* $\mathbf{K}^\times$.

N3 : $\mathbf{N}_{\mathbf{F}/\mathbf{K}}(a) = a^m$ *for all* $a \in \mathbf{K}$.

N4 : $\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha^p) = \mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *for all* $\alpha \in \mathbf{F}$, *[13].*

Many parts of the proof for the norm properties are derived immediately from the definition of norms, but some are more difficult, such as **N**2.

Proof:

N1 : **N**1 : $\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha\beta) = \mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha)\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\beta)$ for all $\alpha, \beta \in \mathbf{F}$ follows from the definition of a norm *(Definition 3.35).*

N2 : It has previously been noted that $\mathbf{N}_{\mathbf{F}/\mathbf{K}}$ maps $\mathbf{F}$ into $\mathbf{K}$ and since we know that $\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha) = 0$ if and only if $\alpha = 0$ then we know that $\mathbf{N}_{\mathbf{F}/\mathbf{K}}$ maps $\mathbf{F}^\times$ into $\mathbf{K}^\times$.

Now, we look at the surjectivity of this mapping. Since $\mathbf{F}^\times$ and $\mathbf{K}^\times$ are finite cyclic groups of orders $p^m - 1$ and $p - 1$, and $\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha^{(p^m-1)/(p-1)}$, the image of $\mathbf{N}_{\mathbf{F}/\mathbf{K}}$ consists of the $(p-1)$-th powers in $\mathbf{F}^\times$. Furthermore, since the multiplicative group is cyclic, there exists a generator g. We can then see that:

$$\mathbf{N}_{\mathbf{F}/\mathbf{K}}(g^k) = g^{kp^m-1)/(p-1)}.$$

$p^m - 1)/(p-1)$ is exactly the index between $\mathbf{F}^\times$ and $\mathbf{K}^\times$ *(The number of distinct cosets of* $\mathbf{K}^\times$ *in* $\mathbf{F}^\times$*).* Thus, $\mathbf{N}_{\mathbf{F}/\mathbf{K}}$ produces every element in $\mathbf{K}^\times$.

N3 : This follows from the definition of the norm and since $a \in \mathbf{K}$ the conjugates are all equal to a.

N4 : To show this, we simply need to note that $\mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha^p) = \mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha)^p = \mathbf{N}_{\mathbf{F}/\mathbf{K}}(\alpha)$ due to **N**1, [13][15]. □

4 Application

Now that we have understood some of the elementary properties exhibited by finite fields. Let us look at some old and modern applications of finite field theory.

Below, we will investigate Latin squares and finite geometries. Also, in algebraic coding theory, we will look into linear codes.

4.1 Combinatorics

Combinatorics is a vast and actively used area in mathematics with many practical applications. [14] In this section, we will look at some of the applications of finite field theory in combinatorics.

4.1.1 Latin squares

Definition 4.1 *A Latin square is a square array in which, symbols are arranged such that every symbol occurs exactly once in any given row and column.*

[4][1]

A Latin square can look like this:

$$\begin{array}{cccc} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{array}$$

Dénes and Keedwell [3] discuss the origin of Latin squares and say that it is likely that Latin squares originated as chess problems concerning the movement of chess pieces on a chess board. Richardson [17] notes that in 1723 a version of this problem containing playing cards was introduced to western mathematicians by the French mathematician Jacques Ozanam's (1640-1718) whose 1694 work was republished posthumously [16]. In this article, Ozanam did not discuss the analytical properties of the problem which was postponed until Euler's 1782 paper *Recherches sur une nouvelle espèce de quarrés magiques* [7].

Definition 4.2 *We say that two Latin squares of the same order are orthogonal if there is exactly one position (i, j) for each ordered pair (k, k') where:*

$$L_1(i, j) = k, \quad L_2(i, j) = k'$$

[1]

Euler's Latin squares problem, sometimes referred to as the phalanx problem or the guard problem, was in modern terminology seeking orthogonal Latin squares. [1][3]
We can use finite fields to construct such orthogonal Latin squares. In this theorem we will discuss mutually orthogonal Latin squares. When we say that these squares are mutually orthogonal, we mean that any pair of Latin squares in this set is orthogonal to each other.

Theorem 4.1 *Let $q = p^m$ be a prime power, then it is possible to construct $q - 1$ mutually orthogonal Latin squares.*

[1]

Proof: Define a $q \times q$ array for each of the $q - 1$ nonzero elements t of $\mathbb{F}_q$ as:

$$L_t(i, j) = ti + j, \quad (i, j \in \mathbb{F}_q)$$

We know that L_t is a Latin square since for each (i, j) we have $L_t(i, j) = L_t(i, j')$ if and only if $j = j'$. This can be understood by looking at the components $ti + j = ti + j'$, which of course can only be true if $j = j'$.

Additionally, $L_t(i, j) = L_t(i', j)$ only if $i = i'$, since if we subtract j from both sides we get $ti = ti'$ and since $\mathbb{F}_q$ is a field, we know that every nonzero element has a multiplicative inverse. We already stated that t is a nonzero element of $\mathbb{F}_q$, therefore $i = i'$.

Now consider the two Latin squares L_t and L_u with the same pair of symbols (k, k') in position (i_1, j_1) and (i_2, j_2), then we have:

$$ti_1 + j_1 = k, \quad ui_1 + j_1 = k',$$
$$ti_2 + j_2 = k, \quad ui_2 + j_2 = k'.$$

From that follows that:

$$t(i_1 - i_2) = j_2 - j_1, \quad u(i_1 - i_2) = j_2 - j_1.$$

If $i_1 - i_2 = 0$, then we know that $j_2 - j_1 = 0$ and the two positions are the same, if they are not equal to 0, then we know that $i_1 - i_2$ has a multiplicative inverse in $\mathbb{F}_q$ and

$$t = u = (i_1 - i_2)^{-1}(j_2 - j_1).$$

Therefore $L_t = L_u$ and if $t \neq u$, L_1 and L_2 are orthogonal, and we have a set of $q - 1$ mutually orthogonal Latin squares of order q. □
[1]

4.1.2 Finite Geometries

Finite geometries is another important application of finite fields and allow mathematicians to construct designs. [1]
In this context, design, is used to refer to a way to select a specific subset called a block. [14] But first we need to understand how we construct finite geometries.

Consider an ordinary coordinate plane made up of the set of points (x, y) where both x and y are numbers. Now, construct a finite plane where the axes are in the finite field $\mathbb{F}_q$. In this plane, any point (x, y) acts under modulo-q arithmetic and we can construct a line as

$$ax + by = c,$$

Where $a, b, c \in \mathbb{F}_q$ and a, b cannot both be 0. [1]

Example: Let us look at some lines in the geometry $\mathbb{F}_3^2$. First we can define $\mathbb{F}_3 = \{0, 1, 2\}$. As such, $\mathbb{F}_3^2$ contains every ordered coordinate pair (x, y) where $x, y \in \mathbb{F}$.

$$\mathbb{F}_3^2 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$$

We can imagine this as a 3×3 grid of points.

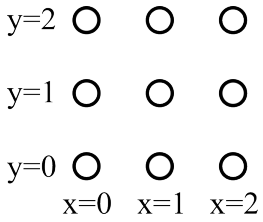

Figure 9: 3×3 grid. (Adapted and modified from [1])

Take any line with the properties defined above, such as $2x + y = 2$. The points that fulfills the equation of this line are $(0, 2), (1, 0), (2, 1)$ (using modulo-3 arithmetic).
We can mark those points and draw a line through them as

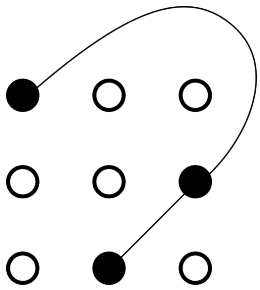

Figure 10: $2x + y = 2$ in the geometry $\mathbb{F}_3^2$. (Adapted and modifier from [1])

We often discuss 2-blocks when talking about finite geometries. Sometimes these are written as $2 - (v, k, \lambda)$ where v is the number of points in the geometry, k is the number of points per block, and λ is the number of blocks containing any given pair of points.

Theorem 4.2 *Let $\mathbb{F}_q$ be a finite field and let points and lines be defined as above. Then, the lines are the blocks of a 2-design on the set of points with parameters:*

$$v = q^2, \quad k = q, \quad \lambda = 1.$$

Proof: We can clearly see that there are q^2 points since there are q elements within $\mathbb{F}_q$ and each point has 2 variables (x, y).

We now need to prove that each line has q points on it. Consider a line $ax + by = c$. Suppose that $b \neq 0$. Each possible of the q values of x determines a unique value $y = b^{-1}(c - ax)$ such that (x, y) is on the line. As such, the line has q points.
In the case that $b = 0$, then $a \neq 0$ and the equation becomes $ax = c$, that is,

$$x = a^{-1}c.$$

In this case, each of the q values of y gives us a unique point $(a^{-1}c, y)$ on the line.

Finally, we need to prove that each pair of points has one unique line that goes through them. Suppose we have two distinct points (x_1, y_1) and (x_2, y_2). We can deduce that $x_2 - x_1$ and $y_1 - y_2$ cannot both be zero at the same time. As such, the equation

$$(y_1 - y_2)x + (x_2 - x_1)y = x_2y_1 - x_1y_2$$

is the equation of a line that contains the two given points. If we have a different line that contains the same two points, we get

$$ax_1 + by_1 = c, \quad ax_2 + by_2 = c.$$

Thus $a(x_2 - x_1) = b(y_1 - y_2)$ and if $x_1 \neq x_2$, then there exists an inverse $(x_2 - x_1)^{-1}$ in $\mathbb{F}_q$.
We can now write $a = \alpha(y_1 - y_2)$, where $\alpha = b(x_2 - x_1)^{-1}$. This gives us $b = \alpha(x_2 - x_1)$ and subsituting for c

$$c = ax_1 + by_1 = \alpha(x_2y_1 - x_1y_2)$$

which is the same line. □
[1]

4.1.3 Projective Planes

Definition 4.3 *A projective plane is a set of elements, called points, along with distinguised sets of points, called lines, as well as a relation incidence I, between points and lines subject to certain conditions:*

(i): Every pair of distinct lines is incident with a unique point. This means that there is one point contained within both of each unique pair of lines called their intersection.

(ii): Every pair of distinct points is incident with a unique line. This means that for every pair of points there is one line that contains both points.

(iii): There exist four points such that no three of them are incident with a single line. This means that there exists four points such that no three of them are on the same line.

[13]
From this definition, we can see that each line must contain at least three points and each point must be contained in at least three lines.
The simplest of the finite projective planes is called the *Fano plane*.

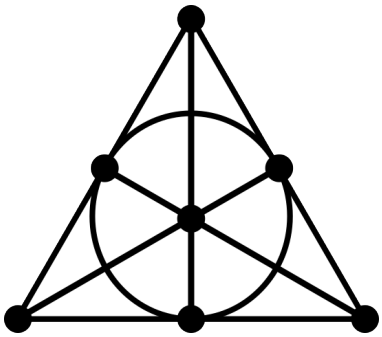

Figure 11: Fano Plane. (Adapted from [13])

For further reading on finite geometries and projective planes we suggest Mullen and Mummert [14], and for a viewpoint from the perspective of coding theory Mullen and Panario [15] provides a very in-depth discussion.

4.2 Algebraic Coding Theory

In the modern world, messages are sent over long distances, and when sending a message over these distances, it is unavoidable that they will travel through various disruptive environments. Mullen and Mummert [14] used an example where solar radiation interferes with message transmissions.
As this is unavoidable, the message that is received often contains missing segments from the originally sent message. How do we then correct this?

Let us assume that there is a set amount of messages that we want to be able to send. We can call that set M. The messages within M can be words or letters.
Then we have an injection from this set of messages to a set of words on a fixed, finite alphabet. A common example to describe this is Morse code. In Morse code we transform the set $M = \{A, B, C, ..., Z, 1, 2, ..., 9, 0\}$ to a series of dots and dashes $\{\cdot.-\}$. *(When we say codes in this context, we do not mean cryptographic codes that are constructed to make the meaning difficult to decode.)*[14]

The goal of coding theory is to make sure that a code allows the reciever to have the highest probability of reconstructing the message that was intended by the sender of the message. Codes that are good at correcting errors are often called error-correcting codes. [14]
A basic idea that emerges in coding theory is to transmit repeating codes or redundant information, which allows the receiver to see what was initially in a lost piece of information due to its repetition.
An alphabet used in coding theory can generally be assumed to be a finite field. A simple model that can be used when coding messages is to assume that both the symbols in the message and in the coded message belong to a finite field $\mathbb{F}_q$ so that the coded message contains more symbols than the original. We can express this as encoding a block of k symbols $m_1m_2...m_k$ where $m_i \in \mathbb{F}_q$ to a code word $c_1c_2...c_n$ where $c_j \in \mathbb{F}_q$ and $k < n$. [13]

The code word can be viewed as an n-dimensional row vector called $c \in \mathbb{F}_q^n$. The function $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$ is called a coding scheme and the function $g : \mathbb{F}_q^n \to \mathbb{F}_q^k$ is called a decoding scheme. We may visualize this process:

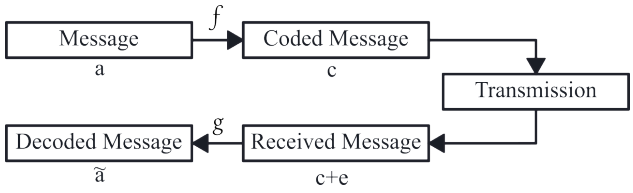

Figure 12: Transmission Model. (Adapted from [13])

$a_1a_2...aa_kc_{k+1}...c_n$ forms a simple coding scheme, where the first k symbols are the original message and the additional $n - k$ symbols are control symbols. We often write these codes as $H = (A, I_{n-k})$ where H is an $(n - k) \times n$ matrix. A is a $(n - k) \times k$ matrix and I_{n-k} is the identity matrix of order $n - k$.

With this, we can now construct a system of equations that gives us the control symbols $c_{k+1}, c_{k+2}, ..., c_n$.

$$Hc^T = 0$$

[13]

5 Discussion

This paper aimed to introduce the theory of finite fields, their structure, and to investigate various mathematical perspectives from which to view them. The research questions concerned in this paper were:

1. What are finite fields?
2. What properties do finite fields have?
3. What different perspectives can we use to undestand finite fields?
4. What are finite fields used for, both historically and contemporarily?

In this discussion, I aim to summarize and analyze the main insights gained throughout my work as well as connect it to the broader literature on finite fields. The chapter will look at the approach and structure of the paper and discuss what could be different and what would be interesting to develop further.

5.1 Understanding Finite Fields & Their Properties

Throughout this paper, finite fields have emerged as rigid, yet deeply organized algebraic structures. Highlighted in Theorem 3.6 and Theorem 3.7, showing that there exist a finite field for every prime power and that they are identical up to isomorphism, was their remarkable symmetry diversifies them from other finite rings where zero divisors commonly prevent their multiplicative inverses from existing.
A fundamental thread throughout the paper is how finite fields merges several layers of algebra. Fundamentally, their additive and multiplicative operations display closed and cyclical properties due to their modular arithmetic, and on a deeper level, we can see that the construction of finite extension fields via the residue quotient

$$\frac{\mathbb{F}_p}{(g(x))},$$

as shown in Theorem 3.8 define a deep connection between finite fields and polynomials. Here, polynomials are shown to define the field structure and concretize how we can think of such an abstract concept, as well as how we may work with them arithmetically.

Understanding the Frobenius map φ and its closely linked cyclotomic cosets, while a structurally dense concept, as an automorphism of the field and as a tool for understanding minimal polynomials, reveals another layer of the internal symmetry found in finite fields, where we see the cycling of the powers of conjugates. Additionally, the counting of polynomials using the totient function showcased a deep connection between the number-theoretic, combinatorial, and algebraic ideas.

5.2 Multiple Perspectives

One of the research questions sought to understand finite fields through different perspectives, and to this end, we looked at them through the group theoretical, polynomial-theoretic, and linear algebraic perspectives. Each of these viewpoints illuminated certain properties and functions of finite fields.
Group theory provided the fundamental relationships found within finite fields, such as the cyclical nature of the multiplicative group $\mathbb{F}_p^\times$. Furthermore, Lagrange's Theorem 3.4 provides the immediate consequence of exponentiation.
While group theory presented relationships and aesthetic beauty of symmetry, polynomial theory instead presented the arithmetic machinery needed for the constructivist understanding of finite fields. Theorem 3.8 clearly provide a reason for the polynomial modular arithmetic used for operations within finite fields and additionally provided a way to visualize the sets within a finite extension field.
Finally, the perspective of linear algebra provided the geometric view of finite fields, whereseeing each finite field as a vector space over its prime field we could see how traces and norms became linear and multiplicative tools.

Although mathematically equivalent, each one of these structures changes the focus on the properties exhibited by finite fields and allows us to better understand them through familiar ways of thinking.

5.3 Literature

Initially it was my assumption that the various sources would tackle finite fields through unique lenses. However, in the process of research I found that most of the information I gathered was synthesized from three major sources. Mullen and Mummert [14], Mullen and Panario [15], and Lidl and Neiderreiter [13] provided large overarching collections of information that each also provided these various perspectives that I sought to filter out.
The thing I most found in common when parcing through the literature is the assumption of clarity in these various, highly abstract, concepts, which made it difficult to understand as a novice in the field. As I strive to become a teacher and as this was meant as an introduction, it became natural to seek out ways to concretely explain the various properties and concepts of finite field theory and this became my driving factor in the selection of theorems and proofs from various sources. Striving to concretize the abstract, I sought imagery that would help visualize the theory to the reader.

To this end, I used Earl and Nicholssons *Oxford Concise Dictionary of Mathematics* [4] to define terminology that was often assumed elementary in other literature on the subject.

5.4 Limitations & Scope

Some limitations of this paper must be acknowledged, primarily due to the breadth of the field. The focus of this paper lay almost solely on the foundational algebra of finite fields. The vast majority of computational theory was left out, such as the algorithms used to construct irreducible polynomials with finite fields. I found that Lidl and Neiderreiter [13] comprehensive section on this subject for the interested reader. These concepts are essential in cryptographic theory and if I were to study the subject further this might be a potential angle.

Furthermore, many of the deeper aspects of finite fields were sorted out of the theoretical foundation chosen to be studied in this paper. Due to the scope of this paper, various theories had to be deprioritized to create a fluent and pedagogical text.
Finally, the historical chapter was intentionally limited. This was not the primary concern of the paper, but the inclusion of the most important and overaching historical background was made to develop an interest and context for the reader.

5.5 Connection Between Theory & Application

The algebraic foundations developed in earlier chapters provide the backbone for various applications of finite fields. In combinatorics, the polynomial construction of extension fields allows for the construction of orthogonal Latin squares and finite geometries. In linear coding theory, mimimal polynomials, the view of finite fields as vector spaces, and the Frobenius automorphism provide the foundations for the defining of linear codes.

We can see that, although the application chapters extend beyond the algebraic foundations, they rest on the theory established in the earlier chapters and clearly show why finite fields are cemented as a central theory within modern mathematics.

References

[1] Norman L. Biggs. *Discrete Mathematics*. Oxford University Press, second edition, 2002.

[2] Frédéric Brechenmacher. A history of galois fields. *Khronos*, 2016.

[3] József Dénes and A. D. Keedwell. *Latin Squares and Their Applications*. Academic Press, London, 1974.

[4] Richard Earl and James Nicholson. *Oxford CONCISE DICTIONARY OF Mathemathics*. Oxford University Press, sixth edition, 2021.

[5] Attila Egri-Nagy and Mikhail Hoffmann. Morphisms (should be) everywhere. *arXiv preprint arXiv:2411.06806*, 2024.

[6] Leonard Euler. Theorematum quorundam ad numeros primos spectantium demonstratio. *Commentarii academiae scientiarum Petropolitanae*, 8:141–146, 1736.

[7] Leonhard Euler. Recherches sur une nouvelle espèce de quarrés magiques. *Mémoires de l'Académie des Sciences de St.-Pétersbourg*, 6:85–239, 1782. Presented in 1779.

[8] George D. Forney. Introduction to finite fields. `https://ocw.mit.edu/course/6-451-principlesofdigital-communication-ii-spring-2005/resources/mit6\_451s05\_fulllecnotes/`, YEAR = 205.

[9] Carl Friedrich Gauss. Disquisitiones arithmeticae. *Leipzig: Fleischer*, 1801.

[10] Carl Friedrich Gauss. Disquisitiones generales de congruentiis. analysis residuorum caput octavum. In *Werke, Band II: Handschriftlicher Nachlass*, pages 212–242. Königliche Gesellschaft der Wissenschaften, Göttingen, 1863.

[11] Steven Givant. *Introduction to Relation Algebras*. Springer International Publishing, 2017.

[12] Camille Jordan. *Traité des substitutions et des équations algébriques*. Gauthier-Villars, Paris, 1870.

[13] Rudold Lidl and Harald Neiderreiter. *ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS 20: FINITE FIELDS*. Cambridge University Press, second edition, 1997.

[14] Gary L. Mullen and Carl Mummert. *Finite Fields and Applications*. American Mathematical Society, 201 Charles Street, Providence, RI 02904-2213 USA, first edition, 2007.

[15] Gary L. Mullen and Daniel Panario. *HANDBOOK OF FINITE FIELDS*. Taylor & Francis Group LLC, 6000 Broken Sound Parkway NW, Suite 300, first edition, 2013.

[16] Jacques Ozanam. *Récréations mathématiques et physiques: qui contiennent plusieurs problêmes d'Arithmétique, de Géométrie, de Musique, d'Optique, de Gnomonique, de Cosmographie, de Mécanique, de Pyrotechnie, de Physique. Avec un Traité des Horloges Élémentaires*. Chez Claude Jombert, Paris, 1723. Nouvelle édition revue, corrigée et augmentée — 4 volumes in-8.

[17] J. T. Richardson. Who introduced western mathematicians to latin squares? *British Journal for the History of Mathematics*, 34(2):95–103, 2019.

[18] Rachel L. Rupnow. Conceptual metaphors for isomorphism and homomorphism: Instructors' descriptions for themselves and when teaching. *Journal of Mathematical Behavior*, 62:100867, 2021.

[19] Theodor Schönemann. Grundzüge einer allgemeinen theorie der höhern congruenzen, deren modul eine reelle primzahl ist. *Journal für die reine und angewandte Mathematik*, 32:93–112, 1846.

[20] Joseph Alfred Serret. *Cours d'algèbre supérieure*, volume 2. Gauthier-Villars, 3e edition, 1866. Volume original provenant de l'Université de Gand et numérisé le 23 janv. 2008.