Scientific Research Publishing

Advances in Pure Mathematics, 2023, 13, 103-132
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

An Introduction to the Theory of Field Extensions

Saviour Chibeti[1*], Iness Kyapwanyama[2], Henry M. Phiri[2], Jeromy Kalunga[2]

[1]Economics Department, University of Lusaka, Lusaka, Zambia
[2]Department of Mathematics, Copperbelt University, Kitwe, Zambia
Email: *saviour@aims.ac.za

How to cite this paper: Chibeti, S., Kyapwanyama, I., Phiri, H.M. and Kalunga, J. (2023) An Introduction to the Theory of Field Extensions. *Advances in Pure Mathematics*, **13**, 103-132.
https://doi.org/10.4236/apm.2023.132006

Received: December 12, 2022
Accepted: February 25, 2023
Published: February 28, 2023

Abstract

This paper unfolds and reviews the theory of abstract algebra, field extensions and discusses various kinds of field extensions. Field extensions are said to be algebraic or transcendental. We pay much attention to algebraic extensions. Finally, we construct finite extensions of $\mathbb{Q}$ and finite extensions of the function field over finite field $\mathbb{F}_p$ using the notion of field completion, analogous to field extensions. With the study of field extensions, considering any polynomial with coefficients in the field, we can find the roots of the polynomial, and with the notion of algebraically closed fields, we have one field, *F*, where we can find the roots of any polynomial with coefficients in *F*.

Keywords

Fields, Extension Fields, Algebraic and Transcendental Extension, Algebraic Closure, Algebraically Closed Field, Absolute Value, Completion, P-Adic Field and Field of Formal Laurent Series

1. Introduction

Much of the history of math is trying to broaden our definition of numbers to help solve more equations. Is it possible to set up another number system? A branch of mathematics called abstract algebra makes it possible to understand this question. The biggest motivation in the history of the expansion of numbers is solving equations. When we consider the natural numbers, the equation $x+1=2$ can be solved, but for the equation $x+2=1$, we encounter the need to define a new number system, the integers, $\mathbb{Z}$ that include the solution of this equation. The same applies with the equation $2x=1$ when we consider the integers, so we define the rationals as a new number system where the solution of $2x=1$ lies. The rationals do not include the solutions of $x^2+1=3$, we define

the real numbers by completing the rationals. The fundamental components of abstract algebra are groups, rings, and fields. In field theory, if we can perform basic arithmetic on a set, addition, subtraction, division and multiplication, the set is referred to as a field ([1]), the real numbers are an example of a field. Now when one takes into account the field of real numbers, $\mathbb{R}$ and the well-known simple equation $x^2+2=1$ with coefficients in $\mathbb{R}$, the solutions of the equation do not lie in $\mathbb{R}$. A natural question that arises is whether there is a larger field where the solutions of this equation lie. The answer proves to be yes, and this larger field is a field of complex numbers. Based on this, we regard the field of complex numbers, $\mathbb{C}$ as a field that extends the field of real numbers, $\mathbb{R}$. We're interested in field extensions because we are assured that given any equation with coefficients in a field, say *L*, the solutions of this equation lie in a larger field if it does not lie in *L*. We briefly give an insight into every chapter and highlight some points in each section.

Chapter 1, underlines some important concepts in our paper. We introduce the concept of a ring, which is key in understanding the concept of a field. Finally, the concept of polynomial rings is introduced, which will be encountered more often in our study of field extension, highlighting only key results.

In Chapter 2, we introduce the concept of field extensions, from which we discuss various kinds of field extensions and some results.

In Chapter 3, we sail through the notion of an algebraic extension, here we discuss what it takes to have an algebraically closed field and an algebraic closure of a field. To complement our discussion of algebraic extension, we briefly discuss transcendental extensions.

Chapter 4 introduces the notion of an absolute value on a field and the criterion for a field to be complete. Here we demonstrate that the notion of completion, is one way to obtain field extensions.

In Chapter 5, we conclude our discussion of field extensions and give suggestions of the possible future work.

Basics and Results

We'll look at some basic ring and field properties in this section. These will come in handy when researching extension fields. Many results, theorems and definitions are taken from [1] and [2].

Definition 1.1. ([1]) Create a set $\mathcal{R}$ with the addition and multiplication binary operations. If the following conditions are met, $\mathcal{R}$ is referred to as a ring.

1) $(\mathcal{R},+)$ is group and for $a_0,a_1\in\mathcal{R}$ we have $a_0+a_1=a_1+a_0$.

2) Multiplication in $\mathcal{R}$ is associative, for all $a_0,a_1,a_2\in\mathcal{R}$,

$$a_0\cdot(a_1a_2)=(a_0a_1)\cdot a_2.$$

3) In $\mathcal{R}$, the two distributive laws apply, for all $a_0,a_1,a_2\in\mathcal{R}$,

$$a_0(a_1+a_2)=a_0a_1+a_0a_2 \quad \text{and} \quad (a_1+a_2)a_0=a_1a_0+a_2a_0.$$

Remark 1.2. Suppose that $\mathcal{R}$ is a ring and $a_0, a_1 \in \mathcal{R}$ be elements. If $a_0 a_1 = a_1 a_0$, $\mathcal{R}$ is considered to be a commutative ring. If a multiplicative identity 1 exists such that for any $a_0 \in \mathcal{R}$

$$a_0 \cdot 1 = 1 \cdot a_0 = a_0,$$

then $\mathcal{R}$ is termed a ring with unity. $\mathcal{R}$ is a finite ring if it has a finite number of elements; otherwise, it is infinite. If $\mathcal{R}_1$ is a subset of $\mathcal{R}$ and a ring with the same operations as $\mathcal{R}$, it is called a subring of $\mathcal{R}$. We'll assume the ring $\mathcal{R}$ is a ring with unity throughout this discussion.

Example 1.3. The set denoted by, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, all contain an element, 1, and they satisfy the axioms stated in Definition 1.1, they are rings with unity and they are infinite.

Definition 1.4. ([1]) Let two nonzero elements a_0 and a_1 be elements of ring $\mathcal{R}$. If $\mathcal{R}$ is commutative, then a_0 is referred to as a zero divisor if $a_0 a_1 = 0$.

Suppose that $\mathcal{R}$ is a commutative ring, If $\mathcal{R}$ contains no zero divisors, it is referred to as an integral domain, say ID. If in an ID, every nonzero element can be expressed uniquely as a product of irreducible elements (or prime elements), it is referred to as a Unique Factorization Domain, and we write (UFD).

Definition 1.5. ([1]) A mapping between two rings $\eta : \mathcal{R} \to \mathcal{R}'$ is referred to as a ring homomorphism if the following conditions are met, for all $a_0, a_1 \in \mathcal{R}$, then

1) $\eta(a_0 + a_1) = \eta(a_0) + \eta(a_1)$
2) $\eta(a_0 a_1) = \eta(a_0)\eta(a_1)$

Elements of a ring $\mathcal{R}$ that map to the additive identity, 0 form a set and it is referred to as the kernel of the ring homomorphism, η. If the mapping in Definition 1.5 is bijective, then it referred to as an isomorphism we write

$$\mathcal{R} \cong \mathcal{R}'.$$

Definition 1.6. ([1]) A subring of a ring $\mathcal{R}$ is said to be an ideal, *I*, of $\mathcal{R}$, if $a_0 r_0, r_0 a_0 \in I$ for ever $r_0 \in \mathcal{R}$ and $a_0 \in I$.

For a ring $\mathcal{R}$ and its ideal *I*, then the following two operations are defined in the quotient group $\mathcal{R}/I$, suppose $a_0, a_1 \in \mathcal{R}$, we have

$$(a_0 + I) + (a_1 + I) = (a_0 + a_1) + I \text{ and } (a_0 + I)(a_1 + I) = (a_0 a_1) + I.$$

$\mathcal{R}/I$ is referred to as the quotient ring of $\mathcal{R}$ by the ideal *I*. It is considered to be a principle ideal if *I* is created by a single element, say a_0, and we write $\langle a_0 \rangle$. We refer to an integral domain that contains ideals that are principal, as a principal ideal domain. Suppose that there are no ideas between the ideal *I* and it's ring $\mathcal{R}$, the ideal is maximal ideal of $\mathcal{R}$.

Definition 1.7. ([1]) A field *F* is a nonzero commutative ring such that $F \setminus \{0\}$ is a group under multiplication.

In any field, we are assured of 0 and 1, and $0 \neq 1$, we therefore have that a field contains at least two elements. A subset of a field, *L* is has the operation of *L* and it is referred to as a subfield. A mapping of fields satisfying the axioms stated

in Definition 1.5 is called a homomorphism of fields and it is injective because its kernel is a proper ideal.

Example 1.8. Since $\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$, $\mathbb{R}$ contains the field $\mathbb{Q}$, hence its a subfield. Also $\mathbb{C}$ contains $\mathbb{R}$, thus, $\mathbb{Q}$ is also subfield of $\mathbb{C}$, by transitivity property.

Suppose the multiplicative identity and the additive identity of a field L are denoted by 1_L and 0 respectively, then the field L contains elements of the additive group generated by 1_L. As we generate the elements of L, we might get an additive identity in the process. Suppose the least number of times we have to add 1_L to get 0 is k, then k is the characteristics of the field, L. If such a positive integer does not exist, the characteristic of, L, is said to be zero.

Definition 1.9. ([1]) Let L be a field. The least positive integer, k that satisfies

$$k\cdot 1_L = 0$$

is referred to as the characteristic of L, and we write $Ch(L)=k$.

$Ch(L)=0$ if such a k does not exist.

Proposition 1.10. ([1]) *Let F be a field. The characteristic of F is either* 0 *or a prime number p.*

Proof. Assume that the characteristic of F, $Ch(F)=k$, assuming $k>1$, then $k\cdot 1=0$. Now let $k=a_0a_1$, where $a_0,a_1<k$, then we have that

$$(a_0a_1)\cdot 1=0\Rightarrow(a_0\cdot 1)(a_1\cdot 1)=0.$$

$(a_0\cdot 1)(a_1\cdot 1)=0$ if and only if $(n\cdot 1)=0$ or $(m\cdot 1)=0$, the fact that k is the lowest positive integer, we have a contradiction. □

Theorem 1.11. ([2]) For a maximal ideal I and the ring $\mathcal{R}$, $\mathcal{R}/I$ is a field.

Proof. See [2]. □

Polynomial Rings

Definition 1.12 [2] Consider a ring $\mathcal{R}$. If $\mathcal{R}$ is commutative and has 1 then an object $s(z)=\alpha_0+\alpha_1 z+\cdots+\alpha_n z^n$ over $\mathcal{R}$, where $a_i\in\mathcal{R}$ is referred to as a polynomial.

From $s(z)$, we call α_n the leading coefficient and $s(z)$ is an n-degree. For $s(z)$ to be monic, $\alpha_n=1$ in $s(z)$ and the collection of all polynomials is denoted by $\mathcal{R}[z]$. The addition is done component-wise and when we consider, $s(z)$ from Definition 1.12 and $r(z)=\beta_0+\beta_1 z+\cdots+\beta_m z^m$, multiplication is defined in this manner,

$$s(z)r(z)=\gamma_0+\gamma_1 x+\cdots+\gamma_{n+m}z^{n+m}$$

where $\gamma_0=\alpha_0\beta_0$, $\gamma_1=\alpha_1\beta_0+\alpha_0\beta_1$, $\gamma_1=\alpha_2\beta_0+\alpha_1\beta_1+\alpha_0\beta_2$, when we generalize, we have $\gamma_i=\sum_{j=0}^{i}\alpha_{i-j}\beta_j$. From the above argument, we have that $\mathcal{R}[z]$, satisfies the axioms stated in Definition 1.1 and hence its a ring and its referred to as a polynomial ring. $\mathcal{R}[z]$ is referred to as an integral domain, provided $\mathcal{R}$ defines a ring [1].

Proposition 1.13. ([1]) *Suppose that L satisfies the axioms of a field. Then its*

polynomial ring, $L[z]$ *qualifies to be to be called a principle ideal domain and hence a unique factorization domain.*

Remark 1.14. For the polynomial $s(\gamma)=\gamma^2+\gamma-6$, the solutions of this polynomial given by $\gamma=2$ and $\gamma=-3$ are referred to as roots of the polynomial. If $r(\gamma)=3\gamma^0=3$ we say, $r(\gamma)$ is a constant polynomial.

Definition 1.15 (contemporary) Suppose that L satisfies the axiom of field and from its polynomial ring, $L[z]$, let $s(z)$ be a nonconstant polynomial. If we cannot write $s(z)$ in the form

$$s(z)=r(z)\cdot k(z)\cdots,$$

where $r(z),k(z),\cdots$ are of degree less than $s(z)$, we say, $s(z)$ is irreducible.

We can express $s(z)=z^2-2$ with coefficients in the rationals as $s(z)=\left(z+\sqrt{2}\right)\left(z-\sqrt{2}\right)$. $s(z)$ is irreducible in the rationals but not in the reals.

Proposition 1.16. ([1]) *Suppose that the non constant polynomial* $s(z)$ *is irreducible, then the ideal,* $\langle s(z)\rangle$ *is a maximal ideal.*

2. Extension Fields

The concepts discussed in the previous chapter help us to introduce extension fields. As the main component of this section, we familiarize ourselves with field extensions by discussing simple extensions, finite extensions, and splitting fields. Many results, definitions, and theorems in this section are those in [1] [2] [3] and [4].

2.1. Construction of Extension Fields

Definition 2.1. ([1]) Suppose that the field L contains the field K, we refer to the field L as extension field of the field that it contains.

The commonly used notations are $L:K$, L/K and a diagram that depicts a the larger field on top of the base field as shown below. We adopt the first notation for our discussion.

We now give an example of field extensions.

Example 2.2. The field $\mathbb{C}$ contains the fields, $\mathbb{R}$ and $\mathbb{Q}$, so we write $\mathbb{C}:\mathbb{R}$ and $\mathbb{C}:\mathbb{Q}$. Similarly the field $\mathbb{Q}$ is contained in the field $\mathbb{R}$, so we have $\mathbb{R}:\mathbb{Q}$.

Definition 2.3. ([1]) Let F, L and K be fields and $F\subset L\subset K$. Then the field L is referred to as a subextension of the K that extends F.

Remark 2.4. From Example 2.2, the field $\mathbb{C}$ extends the fields $\mathbb{R}$ and $\mathbb{Q}$ and since we have the inclusion $\mathbb{C}\supseteq\mathbb{R}\supseteq\mathbb{Q}$ we have that $\mathbb{R}$ is a subextension of the field $\mathbb{C}$ that extends $\mathbb{Q}$.

We now present a statement and demonstration of the Fundamental Theorem of Field Theory, also known as Kronecker's Theorem, which establishes the existence of an extension field.

Theorem 2.5 (Fundamental Theorem of Field Theory). [1] Let L represent a

field. From the polynomial ring $L[z]$, let $s(z)$ be nonconstant. Then there exists a field, K that extends the field E. if $s(\gamma)=0$, then $\gamma \in K$.

Proof. Suppose that L is a field, its polynomial ring $L[z]$ is a *UFD*. From $L[z]$, let $s(z)$ be a non-constant, it can be expressed in terms of some irreducible polynomial in $L[z]$. If one of these irreducible polynomials is, $r(z)$, then the ideal $\langle r(z)\rangle$ is a maximal ideal. And we have that the field

$$K=\frac{L[z]}{\langle r(z)\rangle}.$$

We asserts that L is contained in K and we now define the map

$$\eta: L \to \frac{L[z]}{\langle r(z)\rangle}$$

given by

$$\eta(\beta)=\beta+\langle r(z)\rangle \quad \forall\, \beta \in L.$$

We see that for all $\beta_1, \beta_2 \in L$

$$\eta(\beta_1+\beta_2)=(\beta_1+\beta_2)+\langle r(z)\rangle=\beta_1+\langle r(z)\rangle+\beta_2+\langle r(z)\rangle=\eta(\beta_1)+\eta(\beta_2)$$

and also

$$\eta(\beta_1\beta_2)=(\beta_1\beta_2)+\langle r(z)\rangle=\left(\beta_1+\langle r(z)\rangle\right)\left(\beta_2+\langle r(z)\rangle\right)=\eta(\beta_1)\eta(\beta_2).$$

The map is a ring homomorphism. Because we associate L with its image $\eta(L)$ in K, we'll use β instead of $\beta+\langle r(x)\rangle$ for $\beta \in L$. We have $\eta(\beta)=\beta$, so that s. Since L is contained in K, K is a field that extends L.

For an element γ in K, we write $\gamma=x+\langle r(z)\rangle$. Now from the polynomial ring, $L[z]$, let $r(z)=\beta_0+\beta_1 z+\cdots+\beta_n z^n$ we have

$$\begin{aligned} r(\gamma) &= \beta_0+\beta_1\gamma+\cdots+\beta_n\gamma^n \\ &= \beta_0+\beta_1\left(x+\langle r(z)\rangle\right)+\cdots+\beta_n\left(z+\langle r(z)\rangle\right)^n \\ &= r(z)+\langle r(z)\rangle=0. \end{aligned}$$

Therefore γ satisfies $r(z)$.

Example 2.6. For the field $\mathbb{R}$, Consider the polynomial $\mathbb{R}[z]$, and from $\mathbb{R}[z]$, let $s(z)=z^2+1$, since $s(z)$ is irreducible. The ideal, $\langle s(z)\rangle$ is maximal. so we have the field $K=\frac{\mathbb{R}[z]}{\langle z^2+1\rangle}$. By Theorem 2.5, K is the field that extends $\mathbb{R}$ and contains the solution of $s(z)$. We can write

$$K=\frac{\mathbb{R}[z]}{\langle z^2+1\rangle}=\left\{\beta_0+\beta_1 z+\langle z^2+1\rangle \mid \beta_0,\beta_1\in\mathbb{R}\right\}$$

If γ satisfies $s(z)$ we van write it as $\gamma=z+\langle z^2+1\rangle$ in K then we have,

$$\frac{\mathbb{R}[z]}{\langle z^2+1\rangle}=\{\beta_0+\beta\gamma \mid \beta_0,\beta_1\in\mathbb{R}\}.$$

Then solving for γ in $\gamma^2+1=0$ we have $\gamma=\pm i$ in K and so

$$K = \{\beta_0 + \beta_1 i \mid \beta_0, \beta_1 \in \mathbb{R}\} = \mathbb{C}.$$

Remark 2.7. The example above gives an illustration of the construction of complex numbers with the help of Theorem 2.5. From the construction, we have an isomorphism between the field $\frac{\mathbb{R}[z]}{\langle z^2+1 \rangle}$ and the field $\mathbb{C}$.

2.2. Simple Extension

In the previous section, we have considered a type of field extension obtained by considering a polynomial and an element that is a root of this polynomial. Can we have a construction where we do not consider the polynomial but the element from the larger field? This question is worth exploring. In this section, we consider this kind of construction, where we only consider an element and adjoin it to the base field. Many results, definitions, and theorems in this section are those in [1] [3] and [5]. We now give a lemma which is a motivation of the definition of simple extensions.

Lemma 2.8 ([1]). *Suppose that F is a subfield of E and* $\alpha \in E$. *Then there exists a unique smallest subfield of E containing both F and* α.

Proof. Suppose that $F \subseteq E$ and an element $\alpha \in E$. Then define the set, $\mathcal{S}$ by

$$\mathcal{S} = \{F_i : i \in I\}$$

as the collection of subfields that contains the field F and an element $\alpha \in E$. Define the intersection

$$\mathcal{L} = \bigcap_{i \in I} F_i,$$

then for an element, $x \in \mathcal{L}$, there exists elements $y \in F_i$ and $z \in E$ such that

$$xy = 1 \text{ and } zx = 1.$$

Now

$$z = z \cdot 1 = zxy = 1 \cdot y = yz = y$$

and $z \in F_i$ for all *i*. This implies that $z \in \mathcal{L}$ and by the uniqueness of the inverse, $\mathcal{L}$ turns out to be a subfield of an extension, *E* that contains the field *F* and the element α and it is the smallest such subfield that contains them both. Since $F \subseteq E$, *F* is a subfield and the intersection of these subfields is , *L* is the unique smallest subfield of the extension, *E*.

The lemma above holds true if α is replaced by $\alpha_1, \alpha_2, \cdots$

Definition 2.9 ([1]). For an extension field, $E : F$, consider the elements $\alpha_1, \alpha_2, \cdots$. Then *E* has a subfield with the notation $F(\alpha_1, \alpha_2, \cdots)$ that contains the elements $\alpha_1, \alpha_2, \cdots$ and the field *F*. It is the smallest and it is therefore to referred to as field generated by $\alpha_1, \alpha_2, \cdots$.

Definition 2.10 ([1]). Suppose that the elements $\alpha_1, \alpha_2, \cdots$, in Definition 2.9 are replaced by α and we write $F(\alpha)$. Then $F(\alpha)$ is referred to as a simple extension with the base field *F*. The element, α that generates the field is called

a primitive element.

Remark 2.11. For the fields $L, L(\gamma)$, and K, consider $L \subseteq L(\gamma) \subseteq K$. We have $L(\gamma)$ as the intermediate field. The elements of $L(\gamma)$ are polynomials in γ, for $\gamma \in L(\alpha)$, we consider an n degree polynomial, $r(z)$. Suppose that $r(\gamma) = 0$, we write

$$L(\gamma) = \beta_0 + \beta_1\gamma + \cdots + \beta_{n-1}\gamma^{n-1}$$

where now the coefficients $\beta_0, \beta_1, \cdots, \beta_n \in L$. Some of the elements of $L(\gamma)$ are not polynomials in γ, if $r(\gamma) \neq 0$ in $L[z]$. We can express the field $F(\alpha)$ as a field containing the ratios of the polynomials defined above. We have

$$L(\alpha) = \left\{ \frac{r(\alpha)}{k(\alpha)} \mid r(z), k(z) \in L[z], k(\alpha) \neq 0 \right\}$$

Example 2.12. Consider an extension field, $\mathbb{C} : \mathbb{R}$ and an element i such that $i^2 = -1$, then we have the inclusion

$$\mathbb{R} \subseteq \mathbb{R}(i) \subseteq \mathbb{C}.$$

The field $\mathbb{R}(i)$ contains the element i and $\mathbb{R}$. Since i is a root of some polynomial in $\mathbb{R}[x]$, we can write the elements of $\mathbb{R}(i)$ as,

$$\mathbb{R}(i) = \{a_0 + a_1 i \mid \text{where } a_1, a_1 \in \mathbb{R}\},$$

thus $\mathbb{C} : \mathbb{R}(i) : \mathbb{R}$. The simple extension generated by $\sqrt{2}$ is expressed as

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a_0 + a_1\sqrt{2} \mid \text{where } a_0, a_1 \in \mathbb{Q}\right\}.$$

From the field K that extends the field L, we can construct the smallest field $L(\gamma)$ that contains F and the element γ in the extension field K. By Theorem 2.5, if $r(\gamma) = 0$ for some irreducible polynomial, $r(z) \in L[z]$, there exists a field that extends the field, L and contains γ, and the field is,

$$\frac{L[z]}{\langle r(z) \rangle}.$$

From the field L, we have two extensions field that contains the root γ, $L(\gamma)$ and $\frac{L[z]}{\langle r(z) \rangle}$. We now explore the relationship between the two fields.

Theorem 2.13 ([1]). Suppose that E is a field and the nonconstant polynomial, $r(z)$ with coefficients in E is irreducible. Then if $E \subseteq L$ and $r(\alpha) = 0$, we have $\alpha \in L$. Define $E(\alpha)$ as the simple extension over E. Then

$$\frac{E[z]}{\langle r(z) \rangle} \cong E(\alpha).$$

That is up to isomorphism, the smallest extension of E, $\frac{E[z]}{\langle r(z) \rangle} \cong E(\alpha)$ contains a root of the polynomial $r(z)$.

Proof. Define an evaluation homomorphism

$$\Phi_\alpha : E[z] \to E(\alpha)$$

by $\Phi_\alpha(k(z)) = k(\alpha)$. When we restrict Φ_α on E, we have the identity map, $\Phi_\alpha|_E = I_E$ and Φ_α is a ring homomorphism. Since $r(\alpha) = 0$, $\Phi_\alpha(r(\alpha)) = 0$ and so $r(z) \in \ker \Phi_\alpha$, therefore $\langle r(z) \rangle \subseteq \ker \Phi_\alpha$. We now define the induced homomorphism

$$\widetilde{\Phi_\alpha} : \frac{E[z]}{\langle r(z) \rangle} \to E(\alpha)$$

by $\widetilde{\Phi_\alpha}(k(z) + \langle r(z) \rangle) = \phi_\alpha(k(z))$ where $k(z)$ is any arbitrary polynomial and $\widetilde{\phi_\alpha}$ is well defined. Since any homomorphism between two fields is identically zero or injective, we have that $\widetilde{\phi_\alpha}$ is either a zero map or is injective. Now since

$$\widetilde{\Phi_\alpha}\Big|_E = \phi_\alpha|_E = I_E \tag{1}$$

and $\widetilde{\Phi_\alpha}(z + \langle r(z) \rangle) = \Phi_\alpha(z) = \alpha$ we have that $\widetilde{\Phi_\alpha}$ is injective. We now have

$$\frac{E[z]}{\langle r(z) \rangle} \cong \widetilde{\phi_\alpha}\left(\frac{E[z]}{\langle r(z) \rangle}\right) \subseteq E(\alpha).$$

We now show that $E(\alpha)$ is the image of $\widetilde{\Phi_\alpha}$. From Expression 1,

$$\widetilde{\Phi_\alpha}\left(\frac{E[z]}{\langle r(z) \rangle}\right) \supseteq E \quad \text{and} \quad \alpha \in \widetilde{\Phi_\alpha}\left(\frac{E[z]}{\langle r(z) \rangle}\right)$$

Now $\alpha = \Phi_\alpha(z) = \widetilde{\Phi_\alpha}(z + \langle r(z) \rangle)$, $E(\alpha)$ is the smallest field that contains the field E and α, then we have

$$\widetilde{\phi_\alpha}\left(\frac{E[z]}{\langle r(z) \rangle}\right) \supseteq E(\alpha).$$

But $E(\alpha)$ has $\widetilde{\phi_\alpha}\left(\frac{E[z]}{\langle r(z) \rangle}\right)$ has its subfield, so we have that

$$E(\alpha) = \widetilde{\phi_\alpha}\left(\frac{E[z]}{\langle r(z) \rangle}\right) \cong \frac{E[z]}{\langle r(z) \rangle}.$$

Therefore

$$\frac{E[z]}{\langle r(z) \rangle} \cong E(\alpha)$$

Example 2.14. Consider $s(z) = z^2 - 2 \in \mathbb{Q}[z]$. Since $s(z)$ is irreducible, the quotient, $\frac{K[z]}{\langle s(z) \rangle}$ forms a field. Now if $s(\beta) = 0$, then $\beta = \pm\sqrt{2}$. By Theorem 2.13, we have by taking the positive root of 2 in $\mathbb{R}$

$$\frac{\mathbb{Q}[z]}{\langle z^2 - 2 \rangle} \cong \mathbb{Q}(\sqrt{2}).$$

Remark 2.15. By Theorem 2.13, we have the isomorphism between the field

$\mathbb{Q}\left(-\sqrt{2}\right)=\left\{a_0+a_1\left(-\sqrt{2}\right)\mid \text{where } a_0,a_1\in\mathbb{Q}\right\}$ and the field $\frac{\mathbb{Q}[z]}{\langle z^2-2\rangle}$ and by Example 2.14 we have the relation $\frac{\mathbb{Q}[z]}{\langle z^2-2\rangle}\cong\mathbb{Q}\left(\sqrt{2}\right)$. Transitivity tells us there will be an isomorphism, and we have that

$$\frac{\mathbb{Q}[x]}{\langle z^2-2\rangle}\cong\mathbb{Q}\left(\sqrt{2}\right)\Rightarrow\mathbb{Q}\left(-\sqrt{2}\right)\cong\mathbb{Q}\left(\sqrt{2}\right)$$

under the isomorphism

$$\left(a_0+a_1\sqrt{2}\mapsto a_0-a_1\sqrt{2}\right)$$

Corollary 2.16. *Let* $s(z)$ *be an irreducible polynomial. Isomorphic fields are those generated by adjoining roots of* $s(z)$.

Lemma 2.17 ([1]). *for the field L, the field* $L(x,y)$ *generated by x and y over L is the field* $\left(L(x)\right)(y)$ *generated by y over the simple extension* $L(x)$.

Proof. For an extension field $E:L$, let the elements $x,y\in E$, then by Definition 2.9, the field $L(x,y)\subseteq E$, generated by the elements x and y contains the field L, and the elements x and y, thus it is smallest among the subfields that contains the two elements and the field L, hence contains the simple extension $L(x)$. Since the field contains the simple extension $L(\alpha)$ and the element y it contains the field $\left(L(x)\right)(y)$ and we have

$$L(x,y)\supseteq\left(L(x)\right)(y) \tag{2}$$

Similarly, the field $\left(L(x)\right)(y)$ generated by x is the smallest among the subfields and contains the simple extension $L(x)$ and y and thus contains L, x, and y. we have

$$\left(L(x)\right)(y)\supseteq L(x,y) \tag{3}$$

From Equation (2) and Equation (3), we have the equality of the two fields

$$L(x,y)=\left(L(x)\right)(y).$$

□

Example 2.18. Consider the extension field $\mathbb{C}$ over $\mathbb{Q}$, then the field $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ contains $\sqrt{2}$ and $\sqrt{3}$ and it is the smallest among the subfields of the extension field $\mathbb{C}$ having $\sqrt{2}$, $\sqrt{3}$ and the field $\mathbb{Q}$. Also $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ is an extension over $\mathbb{Q}$ and it is obtained as follows

$$\mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)\supseteq\mathbb{Q}\left(\sqrt{2}\right)\supseteq\mathbb{Q}.$$

2.3. Finite Extension Fields

Since any field say L contains a prime field, the multiplication defined in F makes L into vector space over it's prime field. Similarly when we consider the extension of the field E over L, E is a vector space over L. Most results, definitions, and theorems in this section are those in [1] [3] and [5].

First we give the definition of the degree of an extension before we define finite extension fields.

Definition 2.19. Suppose $K:L$ is an extension field. Then K is vector space over L and the dimension of this vector space is referred to as the degree of the extension, K and we write $K:L$.

Definition 2.20. Let K be a field that extends the field L. If the degree defined in Definition 2.19, is finite, then K is finite, otherwise, K is infinite.

Suppose that for the extension $[K:L]$, $K=L$, then K has degree one. If the degree of the extension is 2 and 3, the extension is called a cubic and quadratic extension respectively. Suppose that γ satisfies a n-degree minimal polynomial, $s(z)$ over a field $\mathbb{F}$, then we write $\deg(\gamma,\mathbb{F})=n$

Theorem 2.21 ([1]). Let K be a field that extends the field L and $\gamma\in K$. If $\deg(\gamma,L)=n$, then the simple extension, $L(\alpha)$ is a vector space over L has the basis $\{1,\gamma,\cdots,\gamma^{n-1}\}$.

Proof. Suppose that $\gamma\in K$ and γ satisfies a polynomial $s(z)$ in the polynomial ring $L[z]$. Then consider the set

$$\ker\Phi_\gamma=\{s\in L[z]:s(\alpha)=0\}.$$

If the set $\{1,\alpha,\cdots,\alpha^{n-1}\}$ were linearly dependent, then there exists some polynomial say $h\in\ker\Phi_\gamma$ with the degree of h less than n. Since $\deg(\gamma,L)=n$ is the minimal degree for a nonzero polynomial in $\ker\Phi_\gamma$. If given $s(z)\in L[z]$, there exist polynomials $q,r\in L[z]$ and when we employ the division algorithm,

$$s(z)=q(z)g(z)+r(z)\text{ and }\deg(r)\le n-1$$

and $g(z)$ is a minimal polynomial of the root γ over the base field L. Clearly $s(\gamma)=r(\gamma)$, and $L(\gamma)$ is the image of $=\ker\Phi_\gamma$ and we write

$$L(\gamma)=\{r(\gamma):r\in L[z],\text{where }\deg(r)\le n-1\}$$

It then follows that $\{1,\gamma,\cdots,\gamma^{n-1}\}$ is a spanning set and therefore a basis of $L(\gamma)$. □

Example 2.22. Consider a field extension $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ then the element $\gamma=\sqrt{2}$ is in the extension $\mathbb{Q}(\sqrt{2})$. We have that $\gamma=\sqrt{2}$ implies $\gamma^2-2=0$, so $s(z)=z^2-2\in\ker\Phi_\gamma$. Therefore the $\deg(\sqrt{2},\mathbb{Q})=2$. By Theorem 2.21, the basis of an extension $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ is $\{1,\sqrt{2}\}$.

Theorem 2.23 ([1]). Suppose that the extensions E and K are finite extensions of the fields L and E respectively, we have the multiplicative relation given by

$$[K:L]=[K:E]\cdot[E:L].$$

Proof. We define a basis for K over E as the set $A=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ and for E as $B=\{\beta_1,\beta_2,\cdots,\beta_m\}$. It suffices to prove that the basis for K over L is the multiplication of the two basis given by

$$BA=\{\beta_j\alpha_i\text{ where }1\le j\le m,1\le i\le n\}.$$

For the elements $\gamma_1,\gamma_2,\cdots,\gamma_n$ and $\eta\in K$, we have a linear combination,

$$\eta = \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n \quad \text{for each } i = 1, 2, \cdots, n.$$

there exist elements $\xi_{i1}, \xi_{i2}, \cdots, \xi_{im} \in F$ and we have the linear combination

$$\gamma_i = \xi_{i1}\beta_1 + \xi_{i2}\beta_2 + \cdots + \xi_{im}\beta_m.$$

Therefore,

$$\eta = \sum_{i=1}^{n} \gamma_i\alpha_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} xi_{ij}\beta_i\right)\alpha_i = \sum_{i,j} \xi_{ij}\left(\beta_j\alpha_i\right)$$

which proves that AB is a spanning set of the $K : L$. We assume that

$$0 = \sum_{i,j} \xi_{ij}\left(\beta_j\alpha_i\right) = \sum_{i}\left(\sum_{j} xi_{ij}\beta_i\right)\alpha_i.$$

Since each $\sum_j \xi_{ij}\beta_i \in E$ and that the basis for an extension $K : L$ is A, $\sum_j \xi_{ij}\beta_i = 0$ for each i. Now we have that each $\xi_{ij} \in L$ and the basis for an extension $E : L$ is B, it implies that each $\xi_{ij} = 0$ which proves we have linearly independent set and it given by AB. □

Remark 2.24. We note that for the extension fields $E : L$ and $K : E$, if $\{\alpha_i \mid i \in I\}$ and $\{\beta_j, j \in I\}$ where I is the indexing set are basis of the extensions respectively, then for fields $L \subseteq E \subseteq K$, the set $\{\alpha\beta_j, i, j \in I\}$ of length mn is a basis for K over L.

Corollary 2.25 ([3]). *Suppose that* $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{r-1} \subseteq K_r$ *are finite field extensions, then*

$$[K_r : K_1] = [K_r : K_{r-1}]\cdots[K_3 : K_2]\cdot[K_2K_1].$$

Proof. When we employ induction, the proof clearly follows from Theorem 2.23,

$$\begin{aligned}[K_r : K_1] &= [K_r : K_{r-1}]\cdot[K_{r-1} : K_1] \\ &= [K_r : K_{r-1}]\cdot[K_{r-1} : K_{r-2}]\cdots[K_3 : K_2]\cdot[K_2 : K_1].\end{aligned}$$

□

Example 2.26. Consider an extension $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$ over $\mathbb{Q}$. Then we have the inclusion

$$\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) \supseteq \mathbb{Q}\left(\sqrt[3]{2}\right) \supseteq \mathbb{Q}.$$

By Theorem 2.23,

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]\cdot\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right].$$

Let $\alpha = \sqrt{3}$. Then $\alpha^2 - 3 = 0$ we have that $s(x) = x^2 - 3 \in \mathbb{Q}\left(\sqrt[3]{2}\right)[x]$ and degree $\left(\sqrt{3}, \mathbb{Q}\left(\sqrt[3]{2}\right)\right) = 2$. By Theorem 2.21, we have that the extension $\mathbb{Q}\left(\sqrt[3]{2}\right)\left(\sqrt{3}\right) : \mathbb{Q}\left(\sqrt[3]{2}\right)$ has a basis $\{1, \sqrt{3}\}$ and $\mathbb{Q}\left(\sqrt[3]{2}\right)\left(\sqrt{3}\right) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$. We now have,

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = \deg\left(\sqrt{3}, \mathbb{Q}\left(\sqrt[3]{2}\right)\right) = 2$$

Similarly, let $\beta = \sqrt[3]{2}$, that is $\beta^3 - 2 = 0$ and $r(x) = x^3 - 2 \in \mathbb{Q}[x]$. So $\deg\left(\sqrt[3]{2}, \mathbb{Q}\right) = 3$. By Theorem 2.21, $\mathbb{Q}\left(\sqrt[3]{2}\right)$ is a 3-dimensional vector space $\mathbb{Q}$.

Now by Theorem 2.23, we have that

$$\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]\cdot\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=2\times 3=6$$

The product of the basis $\left\{1,\sqrt{3}\right\}$ and $\left\{1,\sqrt[3]{2},\left(\sqrt[3]{2}\right)^2\right\}$ gives the basis of an extension $\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}$ and it is given by

$$\left\{1,\sqrt[3]{2},\left(\sqrt[3]{2}\right)^2,\sqrt{3},\sqrt[3]{2}\sqrt{3},\sqrt{3}\left(\sqrt[3]{2}\right)^2\right\}.$$

2.4. Splitting Fields

Theorem 2.5, gives us a criterion to construct extension fields. If the field K extends L and $s(z)$ is a nonconstant polynomial from the polynomial ring $L[z]$, K has a root of $s(z)$. If the root of $s(z)$ is γ, then we have a factor $(z-\gamma)$. For the nonconstant polynomial, $s_1(z)\in K[z]$, we can therefore write $s(z)=(z-\gamma)s_1(z)$. K being a field implies that we can repeat the process, in doing so, we obtain a field E that extends K, and for $s_2(z)\in E[z]$ we have $s(z)=(z-\gamma)(z-\eta)s_2(z)$. In so doing, we can find a field, E_n that extends other fields and this fields contains all the roots of $s(z)$, which can be expressed as a product of linear factor ([1]).

Definition 2.27. Let the field E extend the field L and the nonconstant polynomial $s(z)\in L[z]$. if $s(z)$ can be factored completely into linear factors in the polynomial ring $E[z]$ and over any proper subfields of the base field, $s(z)$ fails to factor completely into linear factors, E is the splitting field for $s(z)$ and is the smallest such extension that contains all the roots of the $s(z)$.

We now give the following example to demonstrate the above definition.

Example 2.28. Consider field $\mathbb{Q}\left(\sqrt{2}\right)$ that extends the field $\mathbb{Q}$. Then the polynomial $s(z)=z^2-2\in\mathbb{Q}[z]$ can be expressed as $s(z)=\left(z-\sqrt{2}\right)\left(z+\sqrt{2}\right)\in\mathbb{Q}\left(\sqrt{2}\right)[z]$. Thus $s(z)$ has been expressed into linear factors, we conclude that the extension field $\mathbb{Q}\left(\sqrt{2}\right)$ is a splitting of the polynomial, $s(z)$. Similarly, for extension field $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ over $\mathbb{Q}$ generated by $\sqrt{2}$ and $\sqrt{3}$ consider the nonconstant polynomial, $r(z)=\left(z^2-2\right)\left(z^2-3\right)\in\mathbb{Q}[z]$, this polynomial can be written as $r(z)=\left(z-\sqrt{2}\right)\left(z+\sqrt{2}\right)\left(z-\sqrt{3}\right)\left(z+\sqrt{3}\right)\in\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)[z]$. We have that $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right):\mathbb{Q}$ is the splitting field for $r(z)$.

Theorem 2.29 (Existence of splitting fields) ([1]) Given any field, say L and the nonconstant polynomial $s(z)$ with coefficients in L, there exists a field, K that extends L. K is the splitting field for $s(z)$.

Proof. It suffices to show first that there is a field, K that extends the field, L in which the polynomial, $s(z)$ of degree n factors completely into linear factors. This is accomplished through induction on the of $s(z)$, if we have that $K=L$, then the degree of $s(z)$ is one. Assume $s(z)$ has degree more than n and F being a field implies that the polynomial ring $L[z]$ is a unique factorization domain and so we can express $s(z)$ into linear factors completely as product

of irreducible polynomial. If all the irreducible factors are of degree 1 again. Otherwise at least one factor say $r(z)$ has degree more than 1. Let the degree be 2. By Theorem 2.5, we have a field K_1 that extends the field L and contains the root of $r(z)$. This implies that over K_1, the two polynomial $r(z)$ and $s(z)$ has a linear factor say $(z-\gamma)$. If $s_1(z)$ is the remaining factor of $s(z)$, $n-1$ is its degree. By induction, we have a field K that extends the field K_1 and $s(z)$ factors completely. Since $\gamma \in K_1 \subseteq K$, this implies that $\alpha \in K$ and K being an extension of L, $s(z)$ has all its roots in K.

Suppose we have a field E that extends all subfields of K and contains L in which $s(z)$ has it's root, then E is the splitting field $s(z)$. □

We now provide the following theorem without proof which tells us that splitting fields are unique.

Proposition 2.30 ([1]). *If there are two splitting fields, they are isomorphic.*

Proof. See ([1]) □

We now present a statement and demonstration of the theorem relating the degree of a nonconstant polynomial, $s(z)$, and that of its splitting field, and a demonstration of the theorem follows.

Theorem 2.31. Suppose that a polynomial, $s(z)$ of degree n splits over the field L, then its splitting field has a degree of at most $n!$.

Proof. Suppose that $s(z)$ is an n-degree polynomial in $L[z]$ and $s(\gamma)=0$. Then the simple extension, $L=L(\gamma)$ is of degree atmost n. If $s(z)$ is irreducible over L_1, then L_1 has degree less than n. Over L_1, $s(z)$ has at least one linear factor, so any other root of $s(z)$ say β satisfies an $n-1$ degree polynomial L_1, thus,

$$\left[L(\beta):L_1\right] \le (n-1)$$

Using Theorem 2.23, if $s(z)$ splits in K, then

$$[K:L]=[K:L_n][L_n:L_{n-1}]\cdots[L_1:L]$$

□

Example 2.32. From Example (2.28), consider an extension field $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, then the polynomial $s(z)=z^2-2$ of degree 2 in the polynomial ring $\mathbb{Q}[z]$ splits in $\mathbb{Q}(\sqrt{2})$. By Example (2.22), $\left[\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right]=2$. Similarly, the polynomial, $s(z)=(z^2-2)(z^2-3)\in\mathbb{Q}[z]$ with coefficients in $\mathbb{Q}$ is of degree 4 and it splits in $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Thus, $\mathbb{Q}(\sqrt{2},\sqrt{3})$ has degree 4.

3. Algebraic Extension

Having set up the theory of field extensions, we have considered different kinds of field extensions. By Theorem 2.5, we where able to find an extension field say E over F by considering a polynomial $s(z)\in L[z]$ and an element γ such that $s(\gamma)=0$. Can we have field, K that extends L containing only those elements that satisfy some polynomial with coefficients in L? In this Chapter, we explore this kind of fields and it's associated properties. Results, definitions and theorems are mostly from [1] [3] [5] and [6].

3.1. Properties of Algebraic Extension

We can classify the elements of an extension field into two categories, and with this classification, we formulate the definition of the algebraic extension.

Definition 3.1 ([1]). Let K be a field that extends L. If $\gamma \in K$ and there exists a nonzero polynomial $s(z) \in L[z]$ such that γ satisfies $s(z)$. then γ is algebraic over L.

We say that γ transcendental if it is does not satisfy any polynomial coefficients in the base field.

Example 3.2. Consider the field $\mathbb{R}$ that extends the base field $\mathbb{Q}$. From the polynomial ring $\mathbb{Q}[z]$, let $s(z) = z^2 - 2$ and since $s(\sqrt{2}) = 0$, $\sqrt{2}$ in $\mathbb{R}$ is algebraic over the base field. Whereas π and e are transcendental over $\mathbb{Q}$ since

$$s(\pi) \neq 0 \quad \text{and} \quad s(e) \neq 0.$$

Remark 3.3. An element from the extension field is algebraic or transcendental, depending on the base field. From Example 3.2, the elements π, and e are transcendental over $\mathbb{Q}$, now for $r(z) = z - \pi$ and $s(z) = z - e$ both in $\mathbb{R}[z]$ they are algebraic over $\mathbb{R}$ since π and e satisfy the polynomial $r(z)$ and $s(z)$ respectively.

Now we'll look at the subfield of algebraic elements.

Corollary 3.4 ([1]). *For a field K that extends L, there exists fields contained in K, that contains the set of all elements of K defined in Definition* 3.1.

Proof. Suppose that the field K that extends L contains elements defined in Definition 3.1 and these elements are π and $\gamma \neq 0$. We now show that

$$\pi \pm \gamma, \pi\gamma \text{ and } \pi/\gamma,$$

are elements defined in Definition 3.1. To do this, it suffices to show that the field $L(\pi, \gamma)$ has a finite degree since it contains all these elements. By Theorem 3.22, we have

$$[L(\pi,\gamma)] = [F(\pi,\gamma) : L(\gamma)] \cdot [L(\gamma) : L].$$

Now since the element π is an element defined in Definition 3.1, it is algebraic the simple extension $L(\gamma)$. Therefore, we have that the field, $L(\pi, \gamma)$ that extends the field $L(\gamma)$ and the $L(\gamma)$ that extends L are of finite degree.

□

The subfield of elements from Corollary 3.4 defines what we call a relative algebraic closure of field within a field that extends it and this, we'll present in the preceding section. With the tools at handy we describe the notion of an algebraic extension and find it's relation with finite extension.

Definition 3.5 ([1]). Suppose that field K that extends the field L contains elements defined in Definition 3.1, then K is referred to as an algebraic extension of L.

Note that if the field that extends the base field is a not an extension defined in Definition 3.5, it is said to be a transcendental extension.

Example 3.6. Consider the element i such that $i^2 = -1$ in the field, $\mathbb{C}$ that extends $\mathbb{R}$ and the polynomial ring $\mathbb{R}[z]$. From $\mathbb{R}[z]$ define

$$s(x) = 2z^2 + 2.$$

We now have that $s(i) = 0$, hence i defines an element in Definition 3.1. However not all elements of $\mathbb{C}$ are algebraic over the base $\mathbb{R}$, e.g. $(2+2i) \in$, hence $\mathbb{C}$ is a field defined in Definition 3.5. From Example 3.2, we have that over $\mathbb{Q}$, neither $\mathbb{C}$ nor $\mathbb{R}$ is a field defined in Definition 3.5 .

Definition 3.7 ([3]). Let K be the field that extends the field L and let $\gamma \in K$ be an element defined in Definition 3.1. From the polynomial ring $L[z]$, let $s(z)$ be an irreducible monic polynomial and $s(\gamma) = 0$. Then the polynomial $s(z)$ is said to be minimal.

Proposition 3.8 ([3]). *Over the field L and element $\gamma \in L$, define a finite simple extension generated by γ, $L(\gamma)$. Then the element γ is algebraic over L.*

Proof. Suppose that the element γ satisfies some polynomial with coefficients in L, then over L, let $s(z)$ be a polynomial defined in Definition 3.7, the degree of this polynomial is equivalent to that of $L(\gamma)$. Hence the field extension is finite, and has degree at most n if the element γ satisfies a polynomial of degree k. Conversely, suppose now that over L, γ is an element of a k-degree simple extension. Then the extension $L(\gamma)$ has $k+1$ roots and they are linearly dependent. Suppose the roots are

$$1, \gamma, \gamma^2, \cdots, \gamma^k,$$

and for all $\beta_i \neq 0$ in L, we have a linear combination,

$$\sum_{i=0}^{k} \beta_i \gamma^i = 0.$$

For a nonzero polynomial, $s(z)$ of degree at most n with coefficients in L, $s(\gamma) = 0$, thus γ is algebraic over L. □

The next theorem shows that finite implies algebraic.

Theorem 3.9 ([3]). Let K be a field that extend the field L. If $K : L$ algebraic extension, then $K : L$ is finite.

Proof. Suppose that the field K extends the field L and contains the element γ. Over L, the simple extension $L(\gamma)$ is contained in the field K and defines a subspace of the vector space K. Hence the field $L(\gamma)$ has degree at most the degree of the K. By Proposition 3.8, the element α satisfies some polynomial with coefficients in L. □

Theorem 3.10 ([1]). The extension field E over the field F is finite if and only if E is generated by a finite number of algebraic elements over F.

Proof. See [1]

□

In our next theorem, we prove the statement that algebraic over algebraic is Algebraic

Theorem 3.11 ([1]). Suppose that over the field L, the field K is an algebraic

extension and over the field E, the field L is an algebra algebraic extension . Then over E, L is an algebraic extension.

Proof. Let the field K, contain the element γ. Then γ satisfies some polynomial, $s(x)$ with coefficients in L,

$$s(\gamma)=a_k\gamma^k+a_{k-1}\gamma^{k-1}+\cdots+a_1\gamma+a_0=0 \tag{4}$$

where $a_i\in K$. Now over E, consider the field $E(\gamma)$ generated by γ the coefficients a_i's of the polynomial $s(x)$.

Since over E, L is an algebraic extension, the elements a_i's satisfies some polynomial with coefficients in E, and so the extension $E(a_i)$, $i=0,1,\cdots,k$ is finite by Theorem 3.10. Now by Equation 4, we have that the element α generates an extension field of degree at most k, since it's minimal polynomial over this field is a divisor of the polynomial above, we have that

$$\left[E(\alpha,a_i):E\right]=\left[E(\alpha,a_i):E(a_i)\right]\cdot\left[E(a_i):E\right] \text{ where } i=0,1,\cdots,k$$

is also finite and we have that over E, K is an algebraic extension since the element γ satisfies some polynomial with coefficients in E. □

3.2. Algebraic Closure of a Field and Algebraically Closed Fields

Definition 3.12. [1] Let L and $\tilde{L}$ be two fields. Then if over L, $\tilde{L}:L$ is an algebraic extension field and from the polynomial ring, $L[x]$, all polynomials splits completely. $\tilde{L}$ is said to the algebraic closure of L.

We can also define an algebraic closure in terms of a set.

Definition 3.13. Suppose that the field K extends the field of the L. We define the algebraic closure of L in the field K as

$$\bar{L}=\{\gamma\in E\}.$$

The element γ satisfies some polynomial with coefficients in L, thus all elements contained in $\bar{L}$ are algebraic over the base field, L.

Definition 3.14 ([1]). Suppose that L is field and from the polynomial ring, $L[x]$, every nonconstant polynomial has a root and this root is contained in K. Then K is referred to as an algebraically closed.

Lemma 3.15. *Suppose that the field L equals to its algebraic closure* $\tilde{L}$, *then L is algebraically closed.*

Proof. When we assert that L is algebraically closed, then from the polynomial ring $L[x]$, we can choose any polynomial, $s(x)$. Suppose that $s(\gamma)=0$, then $(x-\gamma)$ is a factor contained in $L[x]$. For $r(x)\in L[x]$, we can now express $s(x)$ as

$$s(x)=(x-\gamma)r(x),$$

All the roots are in L. Thus, over L, $s(x)$ splits completely and hence L equals $\tilde{L}$. Conversely, if we assert that $L=\tilde{L}$, it follows immediately that L is algebraically closed. □

Corollary 3.16. *Suppose that the field* $\tilde{L}$ *is the algebraic closure of the field L. Then we have that it is algebraically closed.*

Example 3.17. Consider the field, $\mathbb{C}$ that extends the field $\mathbb{R}$, then, $\mathbb{C}$ algebraic closure of $\mathbb{R}$, and hence its algebraically closed. The $\mathbb{R}$ is not an algebraic closure of itself, since when we consider the polynomial $s(x)=x^2+4\in\mathbb{R}[x]$ has roots $\pm 2i$ which are not contained in $\mathbb{R}$, hence its not algebraically closed.

From the uniqueness of splitting fields, we have that algebraic closure of a field is unique up to isomorphism and we know that that if the field $\tilde{L}$ is an algebraic closure of the field L, then $L=\tilde{L}$ and this field is algebraically closed. Now, the question that may arise is, can we have an algebraically closed field for an given field? Our next proposition helps us understand this question.

Proposition 3.18 ([1]). *Suppose that L is a field, then exists an algebraically closed field, K that extends the field L.*

Proof. See [1] □

Example 3.19. Consider the field $\mathbb{C}$, that extends the field, $\mathbb{Q}$ and $\mathbb{R}$. $\mathbb{C}$ is the algebraic closure of $\mathbb{Q}$ and $\mathbb{R}$, hence its algebraically closed.

Proposition 3.20. *Suppose that the field K contains the field L. If K is algebraically closed, then we call the set $\tilde{L}$ an algebraic closure of L and its defined as*

$$\tilde{L}=\{\gamma\in K:\gamma \text{ is algebraic over } L\}.$$

Proof. Suppose that $\tilde{L}$ contains the elements that satisfy some polynomial with coefficients in *L*. Over *L*, Definition 3.5 implies that $\tilde{L}$ is algebraic. From the polynomial ring $L[x]$, every polynomial, say $s(x)$ factors completely into linear factors over *K*. This also holds true for every polynomial in the polynomial ring $K[x]$. Now γ is algebraic over *L* since $s(\gamma)=0$. We have that γ is contained in $\tilde{L}$. We now have that all linear factors have coefficient in $\tilde{L}$, which implies that that $s(x)$ factors completely in $\tilde{L}$ and this means that we have an algebraic closure, $\tilde{L}$ of *L*. □

Algebraic Closure of Finite Fields

In order to describe the algebraic of finite fields, we first presents some results on finite fields. If the elements in a field, $\mathbb{F}_p$ are of a finite number, we say that $\mathbb{F}_p$ is a finite field. Consider the following set of integers $2\mathbb{Z},3\mathbb{Z},5\mathbb{Z},7\mathbb{Z}$, these set of integers are maximal ideal of the ring of integers and when we get the quotient with ring $\mathbb{Z}$, we have the fields $\mathbb{Z}/k\mathbb{Z}$ for $k=2,3,5,7$. The fields obtained have a finite number of elements $2,3,5,7$ respectively. From the construction, we see that if we consider any prime we can construct these fields and we write $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ to denote these kind of fields.

Lemma 3.21 ([1]). *Suppose that the field $\mathbb{F}$ contains the field $\mathbb{L}$. If $\mathbb{L}$ has q number of elements and over $\mathbb{L}$, k is the degree of $\mathbb{F}$. We have that $\mathbb{L}$ has q^k elements.*

Proof. Suppose that $\mathbb{F}$ has a finite number of elements, then over $\mathbb{L}$, $\mathbb{F}$ is a finite extension field and hence a vector space with a finite dimension. Assume that over $\mathbb{L}$, *k* is a dimension of $\mathbb{L}$ that is $[\mathbb{F}:\mathbb{L}]=k$. We have that over $\mathbb{L}$, the set $\{\gamma_1,\gamma_2,\cdots,\gamma_k\}$ is basis and the γ_i's are linearly independent. For any

$\beta \in \mathbb{L}$ and $\alpha_i \in \mathbb{F}$ we have a linear combination of the basis, and we write

$$\beta = \sum_{i=1}^{k} \alpha_i \gamma_i.$$

There are q choices for each α_i and there are $k\alpha_i$'s. We have that β has q^k choices and we conclude that the finite field F must have q^k elements. □

Theorem 3.22 ([1]). Suppose that the field $\mathbb{L}$ has a finite number of elements and let the prime p denote its characteristic. Over its prime subfields, let k be the degree of $\mathbb{L}$, then $\mathbb{L}$ has p^k elements.

Proof. Suppose that $\mathbb{L}$ has a finite number of elements, then its characteristic is a prime, p. There is an isomorphism between $\mathbb{F}_p$ that contains p number of elements and the prime subfield that has characteristic p. Then we have that $\mathbb{F}_p \subseteq F$ and $\left|\mathbb{F}_p\right| = p$. By Lemma 3.21, we have that the field F must have p^n elements. Hence we conclude that all finite fields must have prime power orders. □

Remark 3.23. From Theorem 3.22, a finite field cannot have 6 elements because the number 6 is not a power of any prime.

Lemma 3.24 ([1]). *Suppose that the field* $\mathbb{L}$ *has* q *elements and for any* $\gamma \in \mathbb{L}$. *Then*

$$\gamma^q - \gamma = 0.$$

Proof. For the case $\gamma = 0$, it follows that $\gamma^q = 0$. Under multiplication, the nonzero elements of $\mathbb{L}$ forms a group and its order is $q-1$. We denote this group by $\mathbb{L}^*$ and we have that $\left|\mathbb{L}^*\right| = q-1$. From group theory, we have that $\gamma^{q-1} = 1$ which implies that $\gamma^q = \gamma$ and we conclude that the lemma holds. □

Lemma 3.25 ([1]). *Suppose that the field* $\mathbb{L}$ *has* q *elements and contains the field* $\mathbb{F}$. *From the polynomial ring,* $\mathbb{L}[z]$, *let the polynomial* $s(z) = z^q - z$. *Then* $s(z)$ *splits in* $\mathbb{L}$, *and for* $\gamma \in \mathbb{L}$, *we write*

$$z^q - z = \prod (z - \gamma).$$

Proof. Suppose that $s(z)$ splits in $\mathbb{L}$, $\mathbb{L}$ is a splitting field of $s(z)$. There are at most q roots in $\mathbb{L}$ since $s(z)$ is a q-degree polynomial. By the previous lemma, Lemma 3.24, the polynomial, $s(z)$ is satisfied by all the elements of $\mathbb{L}$. Therefore for $\gamma \in \mathbb{L}$, we write

$$z^q - z = \prod (z - \gamma).$$

Over a proper subfield of $\mathbb{L}$, that contains $\mathbb{F}$ the $s(z)$ does not split, as such a field would have fewer than q elements. □

Theorem 3.26 (Existence and Uniqueness of Finite Fields). [1] Consider an integer $k \geq 1$ and prime number p there exists a field with p^k elements and its referred to as a finite field. Let $q = p^k$ and from the polynomial ring $\mathbb{F}_p$, let $s(z) = z^q - z$. Then there is an isomorphism between the splitting field of $s(z)$ and the field $\mathbb{F}_q$.

Proof. See [1]

Theorem 3.27 (Subfield Criterion for finite fields). Let $\mathbb{F}_q$ be a finite field

with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m where m is a positive divisor of n then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.

Proof. see [1].

□

Example 3.28. The subfield of the field $\mathbb{F}_{2^{30}}$ are $\mathbb{F}_{2^{30}}$, $\mathbb{F}_{2^{15}}$, $\mathbb{F}_{2^{10}}$, $\mathbb{F}_{2^5}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^2}$ and $\mathbb{F}_2$ since 30, 15, 10, 5, 3, 2 and 1 are positive divisors of 30.

Lemma 3.29. *Suppose that the field* $\mathbb{L}$ *is finite with k elements. Then not a every polynomial with coefficients in* $\mathbb{L}$ *has a root, that is* $\mathbb{L}$ *is not algebraically closed.*

Proof. We asserts that $\mathbb{L}$ has k elements, then $\mathbb{L}$ is finite. Let the elements be $\gamma_1, \gamma_2, \cdots, \gamma_k$. From the polynomial ring $\mathbb{L}[z]$ define the polynomial $s(z)$ by

$$s(z) = \sum_{i=1}^{k} (z - \gamma_i) + 1.$$

Then for all $i < k+1$, $s(\gamma_i) \neq 0$. Therefore, there is no element of $\mathbb{L}$ that is a root of $s(z)$. Since $s(z)$ exists, we conclude that $\mathbb{L}$ is not algebraically closed. □

For a finite field of prime order. We consider an integer $k \geq 1$ and a prime p. Suppose that $q = p^m$, we have the field $\mathbb{F}_q$. Since $\mathbb{F}_q$ is a field, it has an algebraic closure, say $\mathbb{L}$ and so, $\mathbb{L}$ contains $\mathbb{F}_q$ by definition. $\mathbb{F}_q$ that contains $\mathbb{F}_q$. Also since there is a unique field extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $\mathbb{F}_q^n$ is contained in $\mathbb{L}$. There is an isomorphism between the $\mathbb{F}_q^k$ and one field contained in $\mathbb{L}$. If we assume that this subfield is isomorphic to $\mathbb{F}_{q^n}$, we have the inclusion

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^n} \subseteq \mathbb{L}.$$

The union

$$F = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$$

is an algebraic closure of $\mathbb{F}_q$. This field is a countable union of arbitrarily large finite fields ([7]).

3.3. Transcendental Extensions

The previous section introduced an algebraic extension in which all its elements are algebraic over the base field. If an extension field is not algebraic, then it's said to be transcendental, and in this section, we introduce this type of field extension. Results, definitions and theorems are similar to those in [8] and [9].

Definition 3.30 ([10]). Let the field $\mathbb{L}$ extend the field $\mathbb{K}$. Then we say that $\mathbb{L}:\mathbb{K}$ is a transcendental extension if there exists at least one element, γ that is not a root some polynomial with coefficients in $\mathbb{K}$.

Example 3.31. Consider the two extensions $\mathbb{R}$ over $\mathbb{Q}$ and $\mathbb{Q}(e)$ over $\mathbb{Q}$, then $\mathbb{R}$ and $\mathbb{Q}(e)$ are transcendental extension of $\mathbb{Q}$ since from Remark 3.3, the elements π and e are transcendental over $\mathbb{Q}$.

Definition 3.32 ([10]). Suppose X is a transcendental element over a field $\mathbb{L}$. Then the rational function field over $\mathbb{L}$ in one variable Z is the field containing all rational functions and it is defined as

$$\mathbb{L}(Z)=\left\{\frac{s(z)}{r(z)}\,|\,s,r\in\mathbb{L}[z],r(z)\neq 0\right\}.$$

Definition 3.33 ([10]). Suppose the field $\mathbb{L}$ extends the field $\mathbb{K}$. We define an algebraically dependent set if from the extension $\mathbb{L}$, a subset $\mathcal{S}=\{\gamma_1,\gamma_2,\cdots,\gamma_n\}$ satisfies some polynomial, $r(z)$ in $\mathbb{K}[z_1,z_2,\cdots,z_n]$, that is,

$$r(\gamma_1,\gamma_2,\cdots,\gamma_n)=0.$$

A subset S is said to algebraically independent over $\mathbb{K}$ if it not algebraically dependent over $\mathbb{K}$. A given set of elements is said to algebraically independent if it does not satisfy some algebraic relation and it is said to be algebraically dependent if it satisfies a polynomial or some algebraic relation.

Example 3.34. Consider the two sets $\{\pi^2,\pi\}$ and $\{\sqrt{2}\}$, then over the field $\mathbb{Q}$, these two sets are algebraically dependent, since they satisfy the polynomials $f(x,y)=x-y^2$ and $g(x)=x^2-2$ respectively from the polynomial ring $\mathbb{Q}[x,y]$. But the sets $\{\pi\}$ and $\{x^2+y^2,x+y\}$ are algebraically independent over $\mathbb{Q}$ and $\mathbb{R}$ respectively.

Remark 3.35. If an element say α is transcendental over any given field, then the set containing α is algebraically independent over the given field. If the set S is algebraically independent over any given field, then it's subset is also algebraically independent. Thus, we can say that an empty set is algebraically independent over any given field. On the other hand, if S is any set that contains an algebraically dependent set, then S is algebraically dependent.

Corollary 3.36 ([10]). *Suppose that* $\mathbb{K}$ *is a field and over* $\mathbb{K}$, *define the set* $\mathcal{S}=\{\gamma_1,\gamma_2,\cdots,\gamma_n\}$. *If* $\mathcal{S}$ *is algebraically independent, then we have an isomorphism defined by*

$$\mathbb{K}(\gamma_1,\gamma_2,\cdots,\gamma_n)\cong\mathbb{K}(x_1,x_2,\cdots,x_n)$$

Definition 3.37 ([11]). Suppose that the field $\mathbb{L}$ extends the field $\mathbb{K}$ and the set $\mathcal{S}=\{\gamma_1,\gamma_2,\cdots,\gamma_n\}$. If $\mathcal{S}$ is the maximum of all the algebraically independent subsets of $\mathbb{L}$, we say that $\mathcal{S}$ is a transcendental basis of $\mathbb{L}$ over $\mathbb{K}$.

If the basis of an extension defined above is empty, $\mathbb{L}$ is an algebraic extension.

Example 3.38. Consider the extension field $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, then set defined by $\mathcal{S}=\{\varnothing\}$ is a basis of this extension. over $\mathbb{L}$, the function field $\mathbb{L}(X)$, has the set $\{X\}$ has its transcendental basis.

Proposition 3.39 ([11]). *Suppose that the field* $\mathbb{L}$ *extends the field* $\mathbb{K}$ *and over* $\mathbb{K}$, *define an algebraically independent set,* $\mathcal{S}$. *Over* $\mathbb{L}$, *the set* $\mathcal{S}\cup\gamma$ *is algebraically independent* $\Leftrightarrow$ *an element* $\gamma\in\mathbb{L}$, *is transcendental over* $\mathbb{K}(\mathcal{S})$.

Proof. We assert that over $\mathbb{L}$, the set $\mathcal{S}\cup\gamma$ is algebraically independent and γ satisfies some polynomial with coefficients in $\mathbb{K}(\mathcal{S})$. We therefore

have for $r_i(\beta_1,\cdots,\beta_n)\in\mathbb{K}(\beta_1,\cdots,\beta_n)$

$$r_0(\beta_1,\cdots,\beta_n)+r_1(\beta_1,\cdots,\beta_n)\gamma+\cdots+r_{n-1}(\beta_1,\cdots,\beta_n)\gamma^{n-1}+r_n(\beta_1,\cdots,\beta_n)\gamma^n=0.$$

The relation shows that $\mathbb{K}(\mathcal{S})$ is algebraically dependent which is a contradiction. Conversely, suppose that over $\mathbb{K}(\mathcal{S})$, γ satisfies some polynomial, $r(x)$. Now each coefficient of this polynomial is an element of $\mathbb{K}(\mathcal{S})$, Clearing denominators yields a nonzero polynomial $r_i(\beta_1,\cdots,\beta_n)\in\mathbb{K}(\beta_1,\cdots,\beta_n)$. Therefore this polynomial yield and algebraic dependence in $\mathbb{K}(\mathcal{S})$, and over $\mathbb{K}$, we have that $\mathbb{K}(\mathcal{S})$ is algebraically independent if and only if γ is transcendental.

Corollary 3.40 ([10]). *Suppose that the field* $\mathbb{L}$ *extends the field* $\mathbb{K}$ *and over* $\mathbb{K}$, *define an algebraically independent set,* $\mathcal{S}$. *If* $\mathbb{L}$ *is algebraic over* $\mathbb{K}(\mathcal{S})$, $\mathcal{S}$ *is a transcendental basis.*

Theorem 3.41. [11] Suppose that $\mathcal{S}$ and $\mathcal{S}_2$ are two transcendental basis. Then cardinality of $\mathcal{S}_1$ equals the cardinality of $\mathcal{S}_2$.

Proof. See [11] □

Definition 3.42. Suppose that the field $\mathbb{L}$ extends the field $\mathbb{K}$ and $\mathcal{S}$ defines a transcendental basis over $\mathbb{K}$. If $\mathbb{L}=\mathbb{K}(\mathcal{S})$ we say that $\mathbb{L}$ is purely transcendental.

Definition 3.43 ([10]). Suppose that the field $\mathbb{L}$ extends the field $\mathbb{K}$ and $\mathcal{S}$ defines a transcendental basis over $\mathbb{K}$. Then the cardinality of $\mathcal{S}$ is referred to as the transcendental degree of $\mathbb{L}$ over $\mathbb{L}$. We write $\operatorname{tra\,deg}(L:K)$ to denote the transcendental degree.

Example 3.44. From Example 3.38, the transcendental basis of the extension field $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is the empty set $\varnothing$ which implies that the transcendental degree of $\mathbb{Q}(\sqrt{2})$ is zero. In general, the transcendental degree of an algebraic extension is zero and we can conclude that all extensions are transcendental extensions.

Theorem 3.45. Suppose that $\mathbb{L},\mathbb{K}$ and $\mathbb{E}$ are fields and the inclusion $\mathbb{K}\supseteq\mathbb{L}\subseteq\mathbb{E}$ be a tower of fields. Then

$$\operatorname{tra\,deg}(\mathbb{K}:\mathbb{E})=\operatorname{tra\,deg}(\mathbb{K}:\mathbb{L})+\operatorname{tra\,deg}(\mathbb{L}:\mathbb{E})$$

Proof. See [11] □

4. Absolute Values and Completions

In the previous chapters, we have considered different kinds of field construction in which the base field is taken to be any arbitrary field. In this chapter, we consider two kinds of base field, $\mathbb{Q}$ and $\mathbb{F}_q(t)$ and introduce the notion of an absolute value on these base field and use this concept to construct an extension field. Most results, definition and theorems are taken from [12] [13] [14] [15].

4.1. Absolute Value over $\mathbb{Q}$ and Completion of Fields

Definition 4.1. [14] Let E be a field. A mapping $\phi:E\to\mathbb{R}_{\geq 0}$ defined by

$$\phi(\alpha)=|\alpha| \quad \text{where} \quad \alpha \in E,$$

is called an absolute value over *E*, if it has the following properties;

1) $|\alpha|=0$ and $|\alpha|\geq 0$ if, and only if, $\alpha=0$
2) $|\alpha\beta|=|\alpha||\beta|$, for all $\alpha,\beta\in E$
3) $|\alpha+\beta|\leq|\alpha|+|\beta|$ for all $\alpha,\beta\in E$ (Triangle inequality).

Definition 4.2. [14] Suppose the absolute value in Definition 4.1 has an extra property called the strong triangle inequality for any $\alpha,\beta\in E$ given by,

$$|\alpha+\beta|\leq \max\{|\alpha|,|\beta|\},$$

then, it is called nonarchimedean. If an absolute value is not nonarchimedean, it is said to be archmedean.

Example 4.3. Consider the usual absolute value defined by

$$|\alpha|_0=\begin{cases}0, & \text{if } \alpha=0\\ 1 & \text{if } \alpha\neq 0,\end{cases}$$

which is called the trivial absolute value. For real numbers and rational numbers, we have the mappings $|.|_\infty:\mathbb{R}\to\mathbb{R}_{\geq 0}$ and $|.|_\infty:\mathbb{Q}\to\mathbb{R}_{\geq 0}$ both defined by

$$|\alpha|_\infty=\begin{cases}\alpha & \text{if } \alpha\geq 0\\ -\alpha & \text{otherwise}\end{cases}$$

Remark 4.4. The absolute value on the complex numbers is defined as

$$|\alpha+\beta i|=\sqrt{\alpha^2+\beta^2}.$$

If we assume that both *a* and *b* are the same, then the strong triangle inequality is not satisfied in each case and we therefore have that these absolute values we have defined are all archimedean.

We now present the general properties of absolute values on a field.

Lemma 4.5. [13] *For a field F. Let* $|.|$ *be the absolute value on F. Then we have*,

1) $|1|=1$
2) $|\lambda^{-1}|=|\lambda|^{-1}$
3) $\big||\lambda|-|\gamma|\big|\leq|\lambda-\gamma|$

Proof.

1) $|1|^2=|1^2|=|1|\Rightarrow|1|=1$
2) $1=|\lambda\lambda^{-1}|=|\lambda||\lambda^{-1}|\Rightarrow|\lambda^{-1}|=|\lambda|^{-1}$
3) We assert that $\alpha=\lambda-\gamma$ and $\beta=\gamma$, so that

$$|\alpha+\beta|\leq|\alpha|+|\beta|$$

we obtain,

$$|\lambda|-|\gamma|=|\alpha+\beta|-|\beta|\leq|\alpha|=|\lambda-\gamma|.$$

Definition 4.6. Suppose that $\mathbb{L}$ is a field and on $\mathbb{L}$, define the two nontrivial absolute values $k_0=|.|_0$ and $k_1=|.|_1$. we say that k_0 and k_1 are equivalent if, and only if, for every $\gamma\in\mathbb{L}$ there is a positive real number, τ such

that,

$$|\gamma|_0 = |\gamma|_1^r .$$

An immediate result from Definition 4.6 is the following corollary.

Corollary 4.7. *For a field* $\mathbb{L}$, *two nontrivial absolute values* $|.|_0$ *and* $|.|_1$ *on* F *are equivalent if for all* $\gamma \in \mathbb{L}$ *we have,*

$$|\gamma|_0 < 1 \Rightarrow |\gamma|_1 < 1$$

We now introduce the notion of a metric space, convergence of a sequence and Cauchy sequence.

Definition 4.8. Suppose $\mathcal{X}$ is a set. A mapping $\delta : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ satisfying the following axioms, for every $\alpha, \beta, \gamma \in \mathcal{X}$;

1) $\delta(\alpha, \beta) \geq 0$ and $\delta(a,b) = 0 \Leftrightarrow \alpha = \beta$
2) $\delta(\alpha, \beta) = \delta(\beta, \alpha)$
3) $\delta(\alpha, \gamma) \leq \delta(\alpha, \beta) + \delta(\beta, \gamma)$

is called the metric on $\mathcal{X}$.

Remark 4.9. A metric space denoted by $(\mathcal{X}, \delta)$ is a set $\mathcal{X}$ equipped with a metric δ. The Definition 4.1 of an absolute value on a field looks similar to Definition 4.8 of a metric and thus we can employ the notion of an absolute value together with a field to form a metric space. Let us consider an ordinary absolute value on $\mathbb{Q}$, then we have a metric space $(\mathbb{Q}, |.|)$ and we can define the metric on the rational numbers $\delta : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}_+$ as

$$\delta(a,b) = |a-b|.$$

Definition 4.10. [15] Suppose a field F is equipped with $|.|$. A sequence (s_n) with its elements taken from F converges to a limit ι, if there is an element $\iota \in F$ such that for any $\varepsilon > 0$ there exists a natural number M, for all $n \geq M$ we have,

$$|s_n - \iota| < \varepsilon.$$

If the limit in the above definition exists, it is unique.

We now provide a theorem below without proof.

Lemma 4.11. [15] *Suppose* F *is a field and the sequences* (s_n) *and* (t_n) *in* F *converge to* s *and* t *respectively. Then, the sequence* $(s_n + t_n)$ *and* $(s_n t_n)$ *converges to* $s+t$ *and* st respectively.

Proof. See [15].

Definition 4.12. Suppose F is a field and (s_n) a sequence in F. (s_n) is called a Cauchy sequence if for every $\varepsilon > 0$, there is a positive integer M such that for any $m, n \geq M$,

$$|s_m - s_n| < \varepsilon.$$

The notion of a Cauchy sequence can be thought of as a sequence in which elements are closer to each other, that is, the difference between the elements is minimal. We now find the relation between a sequence that converges and Cauchy sequence.

Theorem 4.13 ([15]). Suppose that the sequence (s_n), then (s_n) is Cauchy sequence.

Proof. Suppose the sequence (s_n) converges to a limit say s, then for every $\varepsilon > 0$ there exists a positive integer M such that for all $n \geq M$

$$|s_n - s| < \frac{\varepsilon}{2}.$$

Now for any $m, n \geq M$, we have,

$$|s_m - s_n| = |s_m - s + s - s_n| \leq |s_n - l| + |l - s_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

□

The converse does not necessarily hold true, it depends on the field.

Definition 4.14. [15] Two sequences (s_n) and (t_n) are equivalent if for every $\varepsilon > 0$, there is a natural number M such that for every natural number $n \geq M$,

$$|s_n - t_n| < \varepsilon.$$

From Definition 4.14, we can derive the definition of an equivalence relation on the set of all sequences in the field F. We denote the equivalence classes of the sequence, (s_n) by $[(s_n)]$.

Definition 4.15 ([15]). Let L be a field. The field $\hat{L}$ whose elements are equivalence classes of Cauchy sequences in L is called the completion of L.

Remark 4.16. The field we have just defined is indeed a field since we have all the operations, that is

1) $0_{\hat{F}} = [(0_F, 0_F, 0_F, \cdots)]$
2) $1_{\hat{F}} = [(1_F, 1_F, 1_F, \cdots)]$
3) $[(a_n)] + [(b_n)] = [(a_n + b_n)]$
4) $[(a_n)][(b_n)] = [(a_n b_n)]$

5) for any nonzero element $[(a_n)]$ of the completion field, we define another element say $[(b_n)]$ in the completion field by

$$b_n = \begin{cases} a_n^{-1} & \text{if } a_n \neq 0 \\ 0 & \text{if } a_n = 0 \end{cases}$$

such that $[(a_n)][(b_n)] = [(a_n b_n)] = 1$.

Definition 4.17. [15] Let S be any subset of a field L equipped with $|.|$. The set S is dense in L if for every element $x \in L$ and every $\varepsilon > 0$, there exists an element $s \in S$ such that

$$|x - s| < \varepsilon.$$

Theorem 4.18 ([15]). Let L be a field equipped with $|.|$ and $\hat{L}$ it's completion. Then L is dense in $\hat{L}$.

Proof. Let $a \in \hat{L}$ be the equivalence class of Cauchy sequences (s_n) in L. Then for every $\varepsilon > 0$, there exists an s_m such that for all $n \geq m$ we have the property $|s_m - s_n| < \varepsilon$. It follows that $|a - \hat{s}_m| < \varepsilon$, where $\hat{s}_m \in L \subseteq \hat{L}$ is just the equivalence class of $(s_m, s_m, s_m, \cdots)$. □

Theorem 4.19. [15] Every Cauchy sequence in the completion field $\hat{F}$ is equivalent to a Cauchy sequence whose elements lie in *F*.

Proof. Let (c_n) be a Cauchy sequence in $\hat{F}$. Since *F* is dense in $\hat{F}$, for each c_n we pick $a_n \in F \subseteq \hat{F}$ so that

$$|c_n - a_n| < \frac{1}{n}.$$

Then for any $\varepsilon > 0$, we pick *M* such that for all $m, n \geq M$,

$$|c_m - a_m| < \frac{\varepsilon}{3} \quad |c_n - a_n| < \frac{\varepsilon}{3} \text{ and } |c_m - c_n| < \frac{\varepsilon}{3}.$$

It then follows from the triangle inequality that for any $m, n \geq M$,

$$|a_m - a_n| < \varepsilon.$$

thus, the sequence (a_n) is Cauchy. □

Theorem 4.20. [15] Suppose *L* is a field equipped with $|.|$. Then there is a complete field $\hat{F}$ with $|.|'$ that extends *L*. This completion $\hat{F}$ is unique up to isomorphism. Moreover on *L*, $|.|'$ restricts to $|.|$. Lastly, *L* is dense in $\hat{F}$.

Proof. (Sketch of the proof) Since some Cauchy sequence in *L* does not have a limit, the limit should exits in the completion field. So general idea is for each element of the completion field $\hat{F}$ to be a limit of Cauchy sequence of elements in *L*. □

Throughout our discussion, we have been talking about the ordinary absolute and the trivial absolute value and we have shown that the ordinary absolute value is archimedean. Can we have a nonarchimedean absolute value on the field of rational numbers? The definition below helps us understand this question.

Definition 4.21. [12] For a prime *p*, define an absolute value on the rational numbers $|.|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ as follows, for all $x \in \mathbb{Q}$, let $\alpha, \beta, m \in \mathbb{Z}$ with $\gcd(\alpha, \beta) = 1$, *p* divides neither α nor β and $x = p^m \frac{\alpha}{\beta}$ then,

$$|x|_p = p^{-m}$$

is the p-adic absolute value on the rational numbers $\mathbb{Q}$.

The p-adic absolute value is indeed an absolute value and it also satisfies the strong triangle inequality condition for absolute values and hence it is nonarchimedean.

Example 4.22. Consider a prime number say $p = 11$ and $x = \frac{968}{9} \in \mathbb{Q}$. Then we have that

$$\left|\frac{968}{9}\right|_{11} = \left|11^2 \frac{8}{9}\right|_{11} = 11^{-2}.$$

We now have an idea of a p-adic absolute value on $\mathbb{Q}$. Does there exist another absolute value on $\mathbb{Q}$ apart from the p-adic absolute value and the ordinary absolute value? The next theorem tells us more about this question.

Theorem 4.23 (Ostrowski). [10] Let ψ be an absolute value on the rational numbers. Then ψ is trivial or it's either equivalent to the usual absolute value

or some p-adic absolute value.

Proof. See [10] □

The Theorem 4.23 tell us that we can only find two absolute values on $\mathbb{Q}$, namely the ordinary and the p-adic absolute value.

4.2. Finite Extension of $\mathbb{Q}$

After establishing the notion of completion and absolute value on $\mathbb{Q}$, we can think of completion of a field as an extension of a field.

Example 4.24. The rational numbers with the ordinary absolute value $\left(\mathbb{Q},|.|\right)$ is not complete. Consider a sequence $a_n = \{3, 3.1, 3.14, 3.141, \cdots\}$. The sequence a_n is a Cauchy sequence in $\mathbb{Q}$ but it is not convergent as the limit of this sequence is π which is not in $\mathbb{Q}$.

With the tools at hand, we can now complete the rationals with respect to the ordinary absolute value and the p-adic absolute value.

Remark 4.25. Consider the rational numbers $\mathbb{Q}$ and the ordinary absolute value $|.|$ on $\mathbb{Q}$, we have a metric space $\left(\mathbb{Q},|.|\right)$. From Example 4.24, we see that π is not in $\mathbb{Q}$ so we now get a set of all Cauchy sequence of rational numbers. For π to be included and all the missing limit, we use the equivalence class of a Cauchy sequence with respect to the equivalence relation. We now obtain a new field which we call the field of real numbers.

Corollary 4.26. [14] $\left(\mathbb{R},|.|\right)$ *is the completion of* $\left(\mathbb{Q},|.|\right)$.

Remark 4.27. From Corollary 4.26, we have the statements below:

1) The field $\mathbb{R}$ of real numbers with respect to the ordinary absolute value is complete,

2) Real numbers $\mathbb{R}$ are an extension field of rational numbers $\mathbb{Q}$,

3) $\mathbb{Q}$ is dense in $\mathbb{R}$.

Instead of the ordinary absolute value, we now consider the p-adic absolute value and run through the same process of constructing the completion field.

Corollary 4.28. $\left(\mathbb{Q},|.|\right)_p$ *is not complete*

Corollary 4.29. [14] *The completion of* $\left(\mathbb{Q},|.|\right)_p$ *is the field* $\mathbb{Q}_p$ *called the p-adic field.*

Remark 4.30. From Corollary 4.29, we have the following statements:

1) the p-adic field with respect to the p-adic absolute value is complete,

2) $\mathbb{Q}_p$ is an extension field of $\mathbb{Q}$,

3) $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

The elements of the above obtained field can be written as,

$$\sum_{n=k}^{\infty} a_n p^n,$$

where $k \in \mathbb{Z}$ and $a_n \in \{0, 1, \cdots, p-1\}$ for all $n \geq k$.

Example 4.31. Consider the 7-adic field, then we can write two as

$$|2| = 2 \cdot 7^0 + 3 \cdot 7^1 + 2 \cdot 7^2 \text{ in } \mathbb{Q}_7.$$

We have constructed the p-adic field, $\mathbb{Q}_p$, this field has a lot of properties

and they discussed in [14]. We now give the general definition of all finite field extensions over the rational numbers $\mathbb{Q}$.

Definition 4.32. [14] An algebraic number field is a finite extension of $\mathbb{Q}$.

If F is an algebraic number field over $\mathbb{Q}$, then F has finite degree.

Example 4.33. The field $\mathbb{Q}$ is a finite extension of itself. Gaussians $\mathbb{Q}(i)$ and all simple extension of $\mathbb{Q}$.

Definition 4.34. We call the complex number, γ an algebraic number if it satisfies some monic polynomial with coefficients in $\mathbb{Z}$.

4.3. Finite Extension of $\mathbb{F}_p(t)$

In the previous section, we considered $\mathbb{Q}$ as the base field, and from this consideration, we constructed algebraic number fields. In this section, we take the rational function field over the finite field as our base field.

Definition 4.35. Let $p>1$ be a prime, $q=p^n$ and $g\in\mathbb{N}\,|\,\{0\}$. We define the rational function field as

$$\mathbb{F}_q(t)=\left\{\frac{h(t)}{f(t)}\,|\,h(t),\ f(t)\in\mathbb{F}_q[t],\ f(t)\neq 0\right\}.$$

Definition 4.36. [12] A formal Laurent series $f(T)$ is an infinite series of the form

$$f(T)=\sum_{j=-r}^{\infty}a_jT^j$$

with $r,j\in\mathbb{Z}$, $a_j\in\mathbb{L}_p$ for all j.

Definition 4.37. [12] Given $x\in\mathbb{F}_p(t)$ and for polynomials $g,h\in\mathbb{L}_p[t]$ let $x=t^r\dfrac{g}{h}$ such that t divides neither g nor h, then an absolute value $|.|_t$ is defined by,

$$|x|_t=\left|t^r\frac{g}{h}\right|_t=p^{-r}.$$

The above absolute is called the t-adic absolute value and it is nonarchimedean like the p-adic absolute value. The t-adic absolute value can also be defined in terms of other parameters than p.

Theorem 4.38. [12] The field $\mathbb{F}_p(t)$ is the completion field of the field $\mathbb{L}_p(t)$ with respect to $|.|_t$.

Proof. Consider the set T of distinct limits of Cauchy sequences in $\mathbb{L}_p(t)$. We represent each element in T as a unique Cauchy series of the form

$$a_{-n}t^{-n}+\cdots+a_0+a_1t+\cdots+a_nt^n+\cdots=\sum_{i=-m}^{\infty}a_it^i$$

with $m,i\in\mathbb{Z}$, $a_i\in\mathbb{L}_p$ for all i. Thus the completion of $\mathbb{L}_p(t)$ is the field of formal Laurent series denoted by $\mathbb{F}_p(t)$. □

Remark 4.39. From the two previous sections, we can draw some important

conclusions about the fields that we have constructed. Since $\mathbb{Q}_p$ is an extension of $\mathbb{Q}$ which has characteristic zero, the field $\mathbb{Q}_p$ is of characteristic zero. Similarly, since $\mathbb{F}_p(t)$ is an extension of the finite field $\mathbb{F}_p$, it is of characteristic *p*. The other notable thing is that both fields are constructed with the respect to a nonarchimedean absolute value. The elements are written in form of power series in these fields.

5. Conclusion

In conclusion, we have shown that with the study of field extensions, considering any polynomial with coefficients in the field, we can find the roots of the polynomial. With the notion of algebraically closed fields, we have one field, *F*, where we can find the roots of any polynomial with coefficients in *F*. We have also shown that the concept of field extensions can be accounted for by field completion.

Acknowledgements

The authors wish to acknowledge the support of the University of Lusaka and the refereed authors for their helpful work towards this paper. They are also grateful to the anonymous peer-reviewers for their valuable comments and suggestions towards the improvement of the original manuscript.

Conflicts of Interest

Regarding the publication of this paper, the authors declare that, there is no conflict of interest.

References

[1] Dummit, D.S. and Foote, R.M. (2004) Abstract Algebra. Vol. 3, Wiley, Hoboken.

[2] Gallian, J. (2016) Contemporary Abstract Algebra. Cengage Learning, Boston.

[3] Hungerford, T.W. (2012) Abstract Algebra: An Introduction. Cengage Learning, Boston.

[4] Li, L. and Zhao, K. (2022) Extension Fields. In: *Introduction to Abstract Algebra*, EDP Sciences, Les Ulis, 141-164. https://doi.org/10.1051/978-2-7598-2916-3.c008

[5] Fraleigh, J.B. (2003) A First Course in Abstract Algebra. Pearson Education India, Delhi.

[6] Moy, S. (2014) An Introduction to the Theory of Field Extensions.

[7] Boxall, G. (2020) Primitive Elements Notes. Stellenbosch University, Cape Town.

[8] Kodrnja, I. and Muic, G. (2021) On Primitive Elements of Algebraic Function Fields and Models of $X_0(N)$. *The Ramanujan Journal*, **55**, 393-420. https://doi.org/10.1007/s11139-021-00423-w

[9] Chambert-Loir, A. (2021) Field Extensions. In: (*Mostly*) *Commutative Algebra*, Springer, Berlin, 157-201. https://doi.org/10.1007/978-3-030-61595-6_4

[10] Salvador, G.D.V. (2006) Topics in the Theory of Algebraic Function Fields. Springer Science & Business Media, Berlin.

[11] Dummit, E. (2020) Fields and Galois Theory (Part 2).

[12] Brown, J., Hasmani, A., Hiltner, L., *et al*. (2015) Classifying Extensions of the Field of Formal Laurent Series over the Finite Field. *The Rocky Mountain Journal of Mathematics*, **45**, 115-130. https://doi.org/10.1216/RMJ-2015-45-1-115

[13] Crivelli, F., Pink, R., *et al*. (2008) Absolute Values, Valuations and Completion.

[14] Fernando, Q. (2020) P-adic Numbers: An Introduction. Springer International Publishing, Berlin.

[15] Sutherland, A. (2013) 18.782 Introduction to Arithmetic Geometry, Fall 2013. Massachusetts Institute of Technology, Cambridge.