university of groningen / faculty of science and engineering / mathematics and applied mathematics

Analysis of Kneser's Root Finding Algorithm for Polynomials in a Constructive Setting

Bachelor's Project Mathematics

July 2018

Student: G.A. Gamboa Quintero

First supervisor: Prof. dr. G.R. Renardel de Lavalette

Second assessor: Prof. dr. J. Top

Abstract

This Bachelor thesis reproduces the proof of the Kneser Algorithm which is used to find roots of nonconstant polynomials as well as providing an analysis of the algorithm in a constructive setting. At first, the motivation for Mathematical Constructivism is presented. Second, the real numbers are constructed through Cauchy sequences and equivalence classes. This leads to an axiomatization of the real numbers in the proof assistant Coq through the construction of a real number structure that is composed of Cauchy sequences of rationals. This will be proven in the first part of the thesis. The second part contains a detailed proof of the Kneser Algorithm. Finally, it contains a brief section that treats an alternative method of proving the algorithm.

Acknowledgements

Thanks to everyone that contributed to these project and to my accomplishment of this Bachelor title.

I want to thank Dr. Renardel who supervised me through this thesis and helped me with all the doubts I had since the beginning. Also, for providing me with a topic that was completely new for me and for his availability throughout all this term.

I am grateful for my parents that have provided me with the support, both mentally and economically, to be here in Groningen and finish my studies in a university like the University of Groningen. I have learnt a lot about myself in the last three years and it could not have been without them.

I also want to mention Janis Norden, who has been one of my closest and dearest friends in Groningen and who helped me in countless occasions in situations related to both university and personal matters. I can only say this: thank you very much sir, you are a gentleman and a scholar. Also, I want to thank Fernanda Fortini for being one of my closest friends and providing me with all the support I needed through these years. For all those days of standing by my side through thick and thin, and for putting a smile on my face every single day.

To everyone, thanks for all your encouragement and support!

Contents

1 Introduction

Mathematical Constructivism was founded by L.E.J. Brouwer in the late 1910's. It first attained the name of Mathematical Intuitionism but later it was name Mathematical Constructivism. This approach towards mathematics consists on considering as valid mathematical objects only those concepts that can be thought of as "mental" constructions. To understand what elements we consider valid in Constructivism, let us introduce the three main tenets of Constructive Mathematics as stated in [1]:

1. Mathematics consists of mental constructions that are present in our minds. The manipulation of mathematical symbols is just a tool we use to communicate mathematics to each other, and since this way of communication is conditioned by our limitations, mathematics should not be focused on it.

2. A mathematical statement is true when there exist a proof of it and false if, assuming there is a proof of it, leads to a contradiction. Thus, for an arbitrary mathematical statement, it does not make sense to discuss its truth value unless one of the before mentioned situations takes place.

3. Mathematics does not focus on mentally reconstructing what has been already constructed, nor it is about determining the truth value of mathematical objects. It is a free creation of the mind.

The first principle clarifies that mathematical language should not be the focus for us, instead we use it to communicate and store mathematical knowledge. The second principle is very important too, since it gives as consequence one of the most important characteristics of constructive mathematics: the law of excluded middle does not necessarily hold. In Classical Mathematics, that is what we will call the approach of mathematics from the Classical Logic point of view, a statement such as "there exists an x such that $A(x)$ holds" can be proven to be true without explicitly stating an algorithm to construct this x. In Constructivism, this is not a valid proof for the existence of this x. That is why, when we say in constructivism that x exists, we really mean that there is an algorithm to construct this x we talk about. Thus, for any mathematical statement, truth follows if and only if there is a proof for a statement and falsity follows if and only if the assumption the existence of a proof leads to a contradiction.

The third principle is a more philosophical statement and it will not be discussed very thoroughly in this thesis. It does have an important consequence, and this is that choice sequences are valid mathematical objects. These will not play an important role in any of the further sections of this thesis, but more on them can be read in [2] .

Now that we have stated and discussed the principles of Constructivism, we need to start defining mathematical notions within this new approach towards mathematics. Our main goal is to reproduce and analyze Kneser's proof of the Fundamental Theorem of Algebra in its main context. This theorem states that every polynomial with complex coefficients of degree greater than 0 has a root in the complex numbers. It was first proven by Carl Gauss in the 18^{th} century by means of contradiction, but there was no statement of an explicit method to find a root for any polynomial. In this thesis, we first focus on a constructive definition of the real numbers. Between the many methods of defining the real numbers, we want to mention two main ones and discuss just one of these two. The first one is the approximation of a real number through Cauchy sequences. This method is presented in [1]. It consists of defining the real numbers as a set of equivalence classes of Cauchy sequences, which gives way to the name *Cauchy reals*. We will stick to the usual terms, and refer to the *Cauchy Reals* simply as *Reals*. The second method that is very important and recognized in Constructivism is the Dedekind approach. In this thesis we will not discuss this approach, but it is also properly introduced in [1].

After defining the real numbers constructively, we will move on to constructively defining some algebraic structures that are necessary for the analysis of Kneser's proof. This will gives us way into the axiomatization of the real numbers in Coq. Coq is the formal proof management system that was used in [3] to axiomatize the algebraic structures previously defined constructively and

construct a real number structure from an axiomatization of the rationals and the field of Cauchy sequences in the rationals.

Finally, we will reproduce and analyze Kneser's proof in the context of Constructivism. Since this proof is constructive, we obtain an algorithm from it. This algorithm called *Kneser's Algorithm* will be analyzed and discussed in the last part of this thesis.

Before we start with the main topic of this thesis, it is important to understand why the Kneser Algorithm, and many other root finding algorithms are important in today's mathematical context. When proving a theorem, it is not enough to provide a proof if implementing the solution is necessary for the use of the theorem. This is why we require root finding algorithms, to contruct roots that we do not get from any non-constructive proof of the Fundamental Theorem of Algebra. For now, we focus only on the Kneser Algorithm because the proof of it and the axiomatization of the reals on Coq serve as an example of how to implement constructive notions and algorithms into proof assistants such as Coq.

2 Construction and Axiomatization of the Real Numbers

In this section, we will look at the main definitions and characteristics of Constructive Mathematics that will help us understand the context under which the Kneser algorithm was invented and proven as well as being able to analyze it properly. Constructive Mathematics have a different and weaker axiomatic system than that of Classical Mathematics. This has as consequence that some mathematical statements which are proven to be true in Classical Mathematics, often cannot be proven neither true nor false in Constructivism. We will first follow the Cauchy approach in defining the real numbers and some of the algebraic structures needed to complete Kneser's proof. This is mainly how it is presented in [1], and concludes with Kneser's proof. For a slightly different approach on the constructive definition of the real numbers, look at [4]. After, we will present the Coq axiomatization of the real numbers and mathematical structures as a complement and formalization of what is done by Cauchy in Coq. This will provide the proper tools to be able to follow Kneser's proof on the next chapter.

In the introduction, we mentioned the three tenets of Constructivism but we did not give any examples of what a "mental" construction might illustrate. Before introducing the definitions and notions of the real numbers, let us begin with understanding properly what a "mental" construction is through a basic yet very important example.

2.1 The Natural Numbers as a mental construction

We have already mentioned the three main principles of Constructivism in the introduction. These principles give way into Constructive Mathematics which are Mathematics that deal only with mental constructions. To get a grasp of what mental constructions are, let us consider this example.

Example. The set $\mathbb{N}$ of natural numbers is a mental construction. Start by thinking of an abstract unit by itself. After this, think of another abstract unit different from the first one and combine them. Doing this repetitively generates the natural numbers.

2.2 Constructive Definitions

2.2.1 Real Numbers

After having defined the natural numbers constructively, we can extend our line of thought to define the sets $\mathbb{Z}$ and $\mathbb{Q}$ which are constructed by thinking about pairs of natural numbers module their respective equivalence classes. Although this is already an important progress towards defining our complete number system, we now need to define constructively the set $\mathbb{R}$ of real numbers.

In order to define real numbers constructively, we must consider fundamental sequences (Cauchy sequences).

Definition 2.1. A fundamental sequence $(r_n)_n$ is a sequence of rationals, together with a function $\beta : \mathbb{N} \to \mathbb{N}$ called the modulus, such that

$$\forall knm(|r_{\beta(k)+n} - r_{\beta(k)+m}| < 2^{-k})$$

Remark. Although we will focus manily on fundamental sequences, one very important aspect of Constructive Mathematics is the admission of choice sequences. Since these are not the focus of this thesis, we will just acknowledge their existence.

Remark. For now, we consider $<$ as an unproblematic relation between rationals. When defined for reals, we have to pay closer attention in order to avoid problems.

Before continuing with the process of defining the set $\mathbb{R}$ of real numbers, it is necessary to understand the role of the modulus function β in the definition of fundamental sequences. In simpler terms, when we input an integer k into the function β, this function will let us know from which term on of our fundamental sequence, namely $r_{\beta(k)}$, we have that every pair of terms after $r_{\beta(k)}$ has at most a distance of 2^{-k}.

Definition 2.2. Two fundamental sequences $(r_n)_n$ and $(s_n)_n$ coincide, that is $(r_n)_n \approx (s_n)_n$, when

$$\forall k \exists n \forall m (|r_{n+m} - s_{n+m}| < 2^{-k})$$

We must also define an ordering relation $<$ between fundamental sequences. This will allow us to introduce an ordering relation later on to the real numbers.

Definition 2.3. Let $(r_n)_n$ and $(s_n)_n$ be fundamental sequences. We define an order $<$ for $(r_n)_n$ and $(s_n)_n$ as:

$$(r_n)_n < (s_n)_n := \exists k n \forall m (r_{n+m} + 2^{-k} < s_{n+m})$$

Finally, having defined fundamental sequences and $\approx$, we arrive to the definition of the real numbers.

Definition 2.4. The set $\mathbb{R}$ of real numbers is the set of equivalence classes of fundamental sequences with respect to $\approx$.

Remark. When we refer to a real number x in constructive mathematics, we refer to the equivalence class of *fundamental sequences* with respect to x. Thus, it makes sense to write $(r_n)_n \in x$ when we wish to refer to a fundamental sequence $(r_n)_n$ in the equivalence class of x.

Two of the most important characteristics of Intuitionism are the exclusion of the Principle of Excluded Middle and the Double Negation Elimination. Within Intuitionism, a statement A is true if and only if there is a proof for A and a statement A is false if and only if the assumption that there is a proof for A leads to a contradiction. Thus, in Mathematical Intuitionism, it is allowed to think of mathematical statements that have no assigned truth value. In other words, the principle of excluded middle is not conserved. This has as consequence one of the most important tenets of Intuitionistic Mathematics: the undecidability of equality in the real numbers. Let us reproduce an example from [1] that illustrates this principle.

Example. Consider a mathematical statement that has not beeen proven true nor false. For example, Goldbach's conjecture: every even number greater than 2 is the sum of two prime numbers. Let us call this statement $A(n)$ for $n \in 2\mathbb{N}_{>0}$ and let us define a real number x^A through the following fundamental sequence:

$$r_n^A := \begin{cases} 2^{-n} & \text{if } \forall k \leq n,\ A(n) \\ 2^{-k} & \text{if } \neg A(k) \wedge k \leq n \wedge \forall l < k\ A(l) \end{cases}$$

It is easy to see this is a fundamental sequence and also we see that $x^A = 0 \leftrightarrow \forall n A(n)$ holds. (We want to clarify that by the definition of $\mathbb{R}$, equality in this set is between equivalence classes, and if two equivalence classes intersect, then they are the same). The direction from right to left is obvious from the definition of the sequence. If $x^A = 0$, then $r_n^A < 2^{-(n-1)}$ for all $n \in 2\mathbb{Z}$ so $A(n)$ holds for every n. Thus, we have that if $A(n)$ is true, then $x^A = 0$. Otherwise, $x^A \neq 0$. Thus, since we do not know the truth value of $\forall n A(n) \ \vee \ \neg \forall n A(n)$, we do not know the truth value of $x^A = 0 \ \vee \ x^A \neq 0$. This yields an example of the undecidability of equality between x^A and 0.

From now on, we will use the letters x, y and z to refer to real numbers in Constructive Mathematics, which means they will indicate equivalence classes of fundamental sequences as these are the elements of $\mathbb{R}$. It is also the case in Constructive Mathematics that the real numbers have three operations that are shared with Classical Mathematics: addition, subtraction and distance from 0 (absolute value). Let us define these operations.

Definition 2.5. Let $(r_n)_n \in x$ and $(s_n)_n \in y$, where x and y are two real numbers. We define:

$$x + y := (r_n + s_n)_n / \approx,\ x - y := (r_n - s_n)_n / \approx,\ |x| := (|r_n|)_n / \approx$$

It is necessary to introduce an ordering relation to the real numbers to be able to compare them, just as we do in Classical Mathematics. Let this be our next definition.

Definition 2.6. Let x and y be two real numbers. We define:

$$x < y := \exists (r_n)_n \in x\ \exists (s_n)_n \in y\ ((r_n)_n < (s_n)_n)$$

Remark. Since the set of real numbers contains conjugacy classes, the definition of $<$ has as consequence $\forall(r_n)_n \in x\ \forall(s_n)_n \in y\ ((r_n)_n < (s_n)_n)$.

Until now, we have seen the arithmetic between real numbers in Constructivism. This is very important since we can compare and combine real numbers, but we still do not know how to determine whether two real numbers are equal or not. Since we are considering Constructive Mathematics, and as shown in the example before, it is not possible to decide whether two numbers are equal or not. To be able to compare real numbers, we can introduce a different notion that tell us if two real numbers are *apart*. This notion is called *apartness* and let it be our next definition.

Definition 2.7. Let $x, y \in \mathbb{R}$. We define:

$$x \# y := (x < y) \ \vee \ (x > y)$$

Apartness plays a very important role in constructive mathematics. Let us prove the properties of apartness.

Proposition 2.8. *Let $x, y, z \in \mathbb{R}$. The apartness relation $\#$ has the following properties:*

1. $\neg(x \# y) \ \leftrightarrow \ x = y$
2. $x \# y \ \leftrightarrow \ y \# x$
3. $x \# y \ \leftrightarrow \ (x \# z \ \vee \ z \# y)$
4. $x \# y \ \leftrightarrow \exists k n \forall m(|r_{n+m} - s_{n+m}| > 2^{-k})$

Proof. Since the proof of this proposition is very technical and it does not contribute much to this thesis, let us prove only the first statement: $\neg(x \# y) \ \leftrightarrow \ x = y$.

$\neg(x \# y) \ \leftarrow \ x = y$ follows directly from the definition of $\#$, so we have to prove $\neg(x \# y) \ \rightarrow x = y$. Let $\neg(x \# y)$ and $(r_n)_n \in x,\ (s_n)_n \in y$. From the previous proposition, we have that

$$\neg(\exists k n \forall m(|s_{n+m} - r_{n+m}| > 2^{-k}))$$

This is rewritten as

$$\forall k n \neg \forall m(|r_{n+m} - s_{n+m}| > 2^{-k}). \tag{1}$$

Let α, β be the moduli of $(r_n)_n, (s_n)_n$ respectively. Then, we also have

$$\forall k n m(|r_{\alpha(k)+n} - r_{\alpha(k)+m}| < 2^{-k}). \tag{2}$$

$$\forall k n m(|s_{\beta(k)+n} - s_{\beta(k)+m}| < 2^{-k}). \tag{3}$$

For k, take $k+2$ and $\max\{\alpha(k+2), \beta(k+2)\}$ for n in (1), then

$$\neg \forall m(|r_{n+m} - s_{n+m}| > 2^{-k-2}). \tag{4}$$

Now, suppose that for some k and m $|r_{n+m} - s_{n+m}| > 2^{-k}$, then

$$|r_{n+m'} - s_{n+m'}| \geq |r_{n+m} - s_{n+m}| - |r_{n+m'} - r_{n+m}| - |s_{n+m'} - s_{n+m}| \geq 2^{-k} - 2 \cdot 2^{-k-2} = 2^{-k-1} \tag{5}$$

for all m'; this is a contradiction with (4), thus $\forall m k(|r_{n+m} - s_{n+m}| \leq 2^{-k})$. We conclude $x = y$. $\square$

So far in this section, we have defined real numbers, their properties and the relations that can be established between them. Now, we move on to a topic that is more specific to the main objective of this thesis: algebraic structures.

2.2.2 Algebraic Structures

We will define the algebraic structures needed for a proper understanding of Kneser's proof from a constructive point of view. For now, we will step aside from the introduction of the real numbers and define the algebraic structures for an arbitrary set with arbitrary operations.

Definition 2.9. A group with apartness is a structure $(G, \cdot, e, \#, ^{-1})$ that satisfies the following axioms:

- $x \cdot e = e \cdot x = x$ $(Unit\ element)$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ $(Associativity)$
- $x \cdot x^{-1} = x^{-1} \cdot x = e$ $(Existence\ of\ Inverses)$
- $xy \# x'y' \ \rightarrow x \# x' \ \vee \ y \# y'$
- $x^{-1} \# y^{-1} \rightarrow x \# y$

For every $x, x', y, y' \in G$.

Notation. In the fourth axiom, we abbreviate $x \cdot y$ as xy. Let this be our usual notation from now on.

Remark. The last two axioms are referred to as the *strong extensionality* of $\cdot$ and $^{-1}$. In other words, $\cdot$ and $^{-1}$ cannot distinguish between two indistinguishable elements via $\#$.

Groups themselves do not play a big role on this thesis, so we skip their properties and their proofs. If the reader is interested in Group Theory from a constructive point of view, refer to [1]. Instead, we move on to defining commutative rings with apartness.

Definition 2.10. A unitary commutative ring with apartness is a structure $(R, +, \cdot, -, 0, 1, \#)$ that satisfies the following axioms:

$x + 0 = x$
$x + y = y + x$
$x + (y + z) = (x + y) + z$
$x + (-x) = 0$
$x \cdot 1 = x$
$xy = yx$
$x(yz) = (xy)z$
$x(y + z) = xy + xz$
$x + y \# x' + y' \ \rightarrow x \# x' \ \vee \ y \# y'$
$xy \# x'y' \ \rightarrow x \# x' \ \vee \ y \# y'$
$1 \# 0$

If we add an extra axiom to the definition of ring, we obtain a field. Let this be our next definition.

Definition 2.11. A field with apartness F is a unitary commutative ring with apartness that satisfies the following axiom: $x \# 0 \rightarrow \exists y(xy = 1)$

For now, we have defined the structures of group, ring and field. After this, we move on to defining polynomial rings, as these are the main object of study in this thesis. In Classical Mathematics, polynomials are defined as the finite sum of powers of a variable or "unknown" X multiplied by coefficients in a field. This is very closed to the definition of polynomial in Constructive Mathematics, the only difference being that since we cannot determine whether an element of a field is equal to 0 or not, we have to find another way of defining the degree of a polynomial. Our two next definitions takes care of this.

Definition 2.12. A polynomial f with coefficients from a field F, is a sum of the form:

$$f(X) = \sum_{k=1}^{n} a_k X^k = a_n X^n + \ldots + a_1 X + a_0, \text{ where } f(k) = 0 \text{ for } k > n$$

Definition 2.13. Let $f = a_n X^n + \ldots + a_1 X + a_0$ be a polynomial with coefficients in a field F.

1. f has degree n if $a_n \# 0$. $(\deg f = n)$
2. f has degree at *least* m if $a_m \# 0$, for $0 \leq m \leq n$. $(\deg f \leq m)$

The rest of the theory of polynomial rings in Constructivism does not contribute much to this thesis since we will focus on a constructive proof. More of the theory of polynomials can be read on [1].

2.3 Coq Axiomatization

As stated before, in the Coq axiomatization of the reals, the first step is to define the algebraic structures that are needed for Kneser's proof, and at the end, axiomatize the real numbers. It is important to consider the Coq axiomatizatoin of the reals for this thesis because it is one of the main tools used in [3] in order to formalize the constructive proof by Kneser. Although this approach of axiomatizing the reals follows the reverse order, it is also based on the same concept as before: defining the reals trhough Cauchy sequences.

2.3.1 Structures in Coq

For now, we do not know how to axiomatize the reals, so we first define a constructive set with an apartness relation and then extend this definition to defining a constructive commutative ring. We will include the Coq axioms instead of the Coq code to facilitate the reading of this thesis, the Coq code is present in Appendix A. These approach to axiomatizing the reals through Coq can be followed from [5].

Definition 2.14. The following axioms correspond to Constructive Set C with apartness relation $\# \subset C \times C$ and equality relation $= \subset C \times C$:

1. *Irreflexivity:* $\forall x \in C(\neg(x \# x))$.
2. *Symmetry:* $\forall xy \in C(x \# y \to y \# x)$.
3. *Cotransitivity:* $\forall xy \in C((x \# y) \to \forall z \in C(x \# z \vee z \# y))$.
4. *Tightness:* $\forall xy \in C(\neg(x \# y) \to x = y)$.

Now that we have a constructive set defined through Coq, we must extend this to axiomatize a constructive ring. As it is the case of the previous axiomatization, the following one is also very close to the definition given from the previous section.

Definition 2.15. The following axioms correspond to a constructive commutative unitary ring R with operations $+ : R \times R \to R$, $- : R \to R$ and $* : R \times R \to R$ and relations of apartness $\# \subset R \times R$ and equality $= \subset R \times R$:

1. $0 \in R$
2. *Strong Extensionality of* $+$: $\forall xyzw \in R(x + z \# y + w \to (x \# y \vee z \# w))$.
3. *Associativity of* $+$: $\forall xyz \in R((x + y) + z = x + (y + z))$.
4. *Additive Identity Element:* $\forall x \in R(x + 0 = x)$.
5. *Commutativity of* $+$: $\forall xy \in C(x + y = y + x)$
6. *Strong Extensionality of* $-$: $\forall xy \in R(-x \# -y \to x \# y)$.
7. *Property of* $-$ *and* $+$: $\forall x \in R(x + -x = 0)$.
8. $1 \in R$.
9. *Strong Extensionality of* $*$: $\forall xyzw \in R(x * z \# y * w \to (x \# y \vee z \# w))$.
10. *Associativity of* $*$: $\forall xyz \in R((x * y) * z = x * (y * z))$.
11. *Multiplicative Identity Element:* $\forall x \in R(x * 1 = x)$.
12. *Commutativity of* $+$: $\forall xy \in C(x * y = y * x)$
13. *Distributive Law:* $\forall xyz \in C(x * (y + z) = (x * y) + (x * z))$.
14. $1 \# 0$.

The operation $(-)$ is not introduced as an operation between two members of R, but it is axiomatized as the negative inverse of a member of R.

From this step of axiomatizing a ring R, it makes sense to move on to axiomatizing a field since the real numbers are one. A field is a commutative ring with a multiplicative inverse partial function. It is partial since the element 0 does not have an inverse. In order to properly axiomatize a field, we must first select the elements from R which we want to define the inverses for and then axiomatize the inverse function for these elements. This process cannot be done all at once, we have to start by defining the subset S of a set C for which we can apply a function without coming into trouble. This will serve for selecting the elements of R for which we can apply the inverse function. Since this is done in Coq explicitely, but in mathematical notation we know how to define the set of invertible elements, we leave the Coq code in the appendix and assume we already have the set S we want (in the appendix, this set S is renamed as `NonZeros F`). Finally, we move on to defining the reciprocal function *rcpcl* for this subset S which will give us way into axiomatizing a field F. This will consist in uniting the axioms of our ring R and *rcpcl*.

Definition 2.16. The following axioms correspond to the reciprocal partial function $rcpcl : F \to F$ for a field F.

1. *Strong Extensionality of rcpcl:* $\forall xy \in R(rcpcl(x) \# rcpcl(y) \to x \# y)$.
2. *Property of rcpcl:* $\forall xy \in R(rcpcl(x) * x = 1)$

Remark. The reciprocal function *rcpcl* is defined for $x \in F$ if and only if $x \# 0$. This comes from the fact that in the rationals, the number 0 does not have a multiplicative inverse.

As we did on the previous section, it is necessary to introduce an order ($<$) to the real numbers. We introduce this order to our field F, this will result in an ordered field which we will call OF. Let this be our next definition.

Definition 2.17. The following axioms correspond to an ordered field OF with an order $<$.

1. *Strong Extensionality of* $<$: $\forall xyzw \in OF(x < z \to (y < w \vee x \# y \vee z \# w))$.
2. *Transitivity of* $<$: $\forall xyz \in OF((x < y \wedge y < z) \to x < z)$.
3. *Irreflexivity of* $<$: $\forall x \in OF(\neg(x < x))$.
4. *Asymmetry of* $<$: $\forall xy \in OF(x < y \to \neg(y < x))$.
5. *Addition respects* $<$: $\forall xy \in OF(x < y \to \forall z \in OF(x + z < y + z))$.
6. *Multiplication respects* $<$: $\forall xy \in OF(0 < x \wedge 0 < y \to 0 < x * y)$.
7. *Property of* $\#$ *and* $<$: $\forall xy \in OF(x \# y \leftrightarrow (x < y \vee y < x))$.

Looking at what we have now, we are very close to defining a real number structure, which is our main goal for this section. A real number structure is an Archimedean and Cauchy complete ordered field. The characteristic Archimedean means that for every real number, there is a natural number greater that it. Cauchy complete means that every Cauchy sequence converges. In order to define the Archimedean property in Coq, we make use of the set `nat` which is the set of Natural numbers and we make use of the inductive function $nreal : \texttt{nat} \to F$ which is defined as follows:

$$nreal(n) := \begin{cases} 0 & \text{if } \ n = 0 \\ nreal(n-1) + 1 & \text{if } \ n > 0 \end{cases}$$

Now, for the Cauchy completeness, we have to define a Cauchy sequence s over our field F, which is almost the same definition from Subsection 2.2.1 (Definition 2.1), but instead, we consider the terms of s as elements of F and not rationals, since we have not axiomatized the rationals in Coq yet. Also, we do not use the Cauchy modulus of a sequence since we assume the Axiom of Choice and this automatically generates one. Because of this, we use the ϵ-definition of Cauchy sequences. Thus, we have to axiomatize the following logical statement:

$$\forall \epsilon \in F_{>0} \exists N \in \mathbb{N} \ \forall m \geq N(|s_m - s_N| < \epsilon)$$

In order to axiomatize the previous statement, we have to introduce the absolute value property and the Cauchy condition on F. Normally, the absolute value is considered as a function, but for our field F, it is a property between two members of F. These will be our next definitions.

Definition 2.18. Let $\epsilon, x \in F$. We define the absolute value property $AbsSmall(\epsilon, x)$ as follows:

$$AbsSmall(\epsilon, x) := -\epsilon < x \wedge x < \epsilon$$

Remark. In more familiar terms and using the Classical Mathematics absolute value function $|\cdot|$, the elements $\epsilon, x \in F$ satisfy the previous property if $|x| < \epsilon$, for $\epsilon > 0$. If $\epsilon < 0$, then $-\epsilon, x$ satisfy $AbsSmall$.

Definition 2.19. Let us introduce the Cauchy condition on F for a sequence $g : \texttt{nat} \to F$. Let $\epsilon > 0$, then

$$\exists N \in \texttt{nat}(\forall m \in \texttt{nat}(N < m) \to AbsSmall(\epsilon, g_m - g_N)$$

Finally, after introducing all the notions required to axiomatize the logical statement from the previous paragraph, we will introduce a function `lim` that will have as input Cauchy sequences in F and as output, the respective limit for each sequence. This will complete the process of axiomatizing F as a real number structure.

Definition 2.20. For a Cauchy sequence $s : \texttt{nat} \to F$ converging to a limit l, the function `lim` is defined as follows:

$$\texttt{lim}(s) := l$$

Remark. When we say a Cauchy sequence $s := (s_n)_n$ converges to a limit l, we define convergence in the same way as in Classical Mathematics. That is $\forall k\ \exists N\ \forall m \geq N(|s_m - l| < 2^{-k})$.

Remark. This function is necessary in Coq because it is the way we construct the real numbers through equivalence classes of Cauchy sequences. Since our field F will be defined in the next section as the field of Cauchy sequences in $\mathbb{Q}$, it is necessary to have a function that lets us know which real numbers is represented by which sequence.

With the last definition, we conclude the axiomatization in Coq of the structures we will use for Kneser's proof. In the next subsection, we will describe how the rationals are constructed in Coq, and how we can define the real numbers through this definition of the rationals.

2.3.2 Rationals and Reals in Coq

The introduction of the rationals in Coq is based on the approach followed in [5], and it is more technical than the one presented in the previous section when we were following the approach in [1]. This will then be used to construct the real numbers from Cauchy sequences, just as we did in subsection 2.2.1. This is why we can consider section 2.3 as a formalization in Coq of section 2.2.

The rational numbers are not defined in Coq, so we need to to construct them. The natural numbers are implemented in Coq as an inductive type `nat` as we said before, but this is almost of no help with what we want to do. Let us use the following representation for the rationals: the pair $\langle p, n\rangle$ represents the rational number $\frac{p}{n+1}$, where $p \in \mathbb{Z}$ and $n \in \mathbb{N}$. This is a better way of representing the rationals, than the more intuitive way of setting $\langle p, n\rangle$ to represent $\frac{p}{n}$. This is because we can easily avoid the case of $n = 0$. Since equality is decidable on $\mathbb{Q}$, we define it in the following way:

$$\langle p, n\rangle =_{\mathbb{Q}} \langle q, m\rangle \ := \ p(m+1) = q(n+1)$$

This way of defining equality works very well in Coq, since Coq is equipped with `ZArith` and can easily verify arithmetical statements in the integers. We define *apartness* in the following way:

$$\langle p, n\rangle \ \# \ \langle q, m\rangle \ := \ \neg(\langle p, n\rangle =_{\mathbb{Q}} \langle q, m\rangle)$$

Finally, we define addition and multiplication as:

$$\langle p, n\rangle + \langle q, m\rangle := \langle p(m+1) + q(n+1), nm + n + m\rangle \qquad \langle p, n\rangle \cdot \langle q, m\rangle := \langle pq, nm + n + m\rangle$$

With this, we complete the arithmetics definitions on Coq. The additive inverse, that is multiplication by -1 can be defined simply since the integers' arithmetic is already included in Coq. Let us move on to the definition of the multiplicative inverse which is a much more challenging aspect.

In the previous subsection, we defined the reciprocal function in Coq for our previously constructed field F. We cannot define the multiplicative inverse of $\langle p, n\rangle$ as $\langle n+1, p-1\rangle$ since $p-1$ has to be natural. Thus, we define the inverse of $\langle p, n\rangle$ on $\mathbb{Q}_{\#0}$ as:

$$\langle p, n\rangle^{-1} := \begin{cases} \langle n+1, p-1\rangle & \text{if } p > 0 \\ \langle -(n+1), -(p+1)\rangle & \text{if } p < 0 \end{cases}$$

We have constructed the rational numbers $\mathbb{Q}$ such that they satisfy all of the axioms from our field F in Coq. We must also introduce an ordering for the rationals and prove that $\mathbb{Q}$ is Archimedean and we obtain an Archimedean ordered constructive field. First, we focus on the ordering. We introduce $<$ through the following definition:

$$\langle p, n\rangle <_{\mathbb{Q}} \langle q, m\rangle := p \cdot (m+1) <_{\mathbb{Z}} q \cdot (n+1)$$

where $<_{\mathbb{Z}}$ is the usual ordering in the integers. Moreover, we can easily prove that $\mathbb{Q}$ is Archimedean so we can conclude that $\mathbb{Q}$ is a constructive ordered field.

Our main goal for this subsection is to construct a real number structure. This will be done by proving that the field of Cauchy sequences over the rationals, or *fundamental sequences* as we referred to them in 2.2.1., forms a constructive ordered field. After that, we will prove that this field of Cauchy sequences is Archimedean and complete. Through this, we would have showed that the field of Cauchy Sequences over $\mathbb{Q}$ forms a real number structure. For now, we will not focus anymore on Coq syntax, but we focus more on the constructive arguments and the proofs of the theorems that will let us state our desired final result. The following theorem is our final goal for this section.

Notation. We denote the set of Cauchy sequences over $\mathbb{Q}$ by $CauchySeq_{\mathbb{Q}}$.

Theorem 2.21. *$CauchySeq_{\mathbb{Q}}$ is a real number structure.*

This theorem will be split up between two theorems to facilitate the readability of its proof.

Theorem 2.22. *$CauchySeq_{\mathbb{Q}}$ is a constructive ordered field.*

Theorem 2.23. *$CauchySeq_{\mathbb{Q}}$ is Archimedean and Cauchy complete.*

The first proof to come will be that of Theorem 2.22. In order to prove this theorem, we must first introduce some additional notions to $CauchySeq_{\mathbb{Q}}$. First, we must give $CauchySeq_{\mathbb{Q}}$ a field structure with apartness. We will not focus too much on the proof of the field axioms since they do not contribute much to this thesis. From then on, we will introduce an order to $CauchySeq_{\mathbb{Q}}$ and conclude that it is a constructive ordered field. In the end, to prove Theorem 2.23 we will use a lemma which will be introduced later on to prove the Archimedean property and a diagonalization argument to prove the Cauchy completeness. This will conclude into a proof of Theorem 2.21.

Definition 2.24. For $CauchySeq_{\mathbb{Q}}$, we define the 1-element as $\mathbb{1} := (1, 1, 1, \ldots)$. The 0-element is defined as $\mathbf{0} := (0, 0, 0, \ldots)$. Addition and Multiplication $(+, \cdot)$ are defined via pointwise addition and multiplication in $\mathbb{Q}$, as in Definition 2.5.

For the inverses in $CauchySeq_{\mathbb{Q}}$ we have the following definition

Definition 2.25. Let f be the nonzero Cauchy sequence in $CauchySeq_{\mathbb{Q}}$ and let N be such that for $m \geq N$, $f_m \# 0$. We define the sequence f^{-1} as follows:

$$f_m^{-1} := \begin{cases} f_m^{-1} & \text{if } m \geq N \\ 0 & \text{if } m < N \end{cases}$$

Now, we can introduce an order $<$ as this will give us way for introducing apartness later.

Definition 2.26. Let $f, g \in CauchySeq_{\mathbb{Q}}$, we define $f < g$ as

$$\exists \epsilon \in \mathbb{Q}_{\geq 0}\ \exists N \in \mathbb{N}\ \forall m \geq N (\epsilon + f_m <_{\mathbb{Q}} g_m)$$

Before proving that our order $<$ satisfies the axioms from Definition 2.17, let us define apartness and equality in $CauchySeq_{\mathbb{Q}}$.

Definition 2.27. We define $\#$ and $=$ for f, g in $CauchySeq_{\mathbb{Q}}$ as follows:

$$f \# g := f < g \vee g < f \qquad f = g := \neg(f \# g)$$

We can now prove that $<$ is an order in $CauchySeq_{\mathbb{Q}}$.

Lemma 2.28. *$<$ satisfies the axioms of an order for the field $CauchySeq_{\mathbb{Q}}$.*

Proof.
1. (*Strong extensionality*) Let $f, g, h, l \in CauchySeq_{\mathbb{Q}}$. Assume $f < g$. By definition, we have $\exists \epsilon \in \mathbb{Q}_{\geq 0}\ \exists N \in \mathbb{N}\ \forall m \geq N(\epsilon <_{\mathbb{Q}} g_m - f_m)$. If $f \# h$, then we are done. Using that $\#$ is decidable, we can consider three cases. If $g \# l$, we are also done. The last case is if $f = h$ and $g = l$, so let us assume this. We have that $h = f < g$, so $h < g$. By definition, we get $\exists \gamma \in \mathbb{Q}_{\geq 0}\ \exists M \in \mathbb{N}\ \forall m \geq M(\gamma <_{\mathbb{Q}} g_m - h_m)$. Nos, since we assumed $g = l$, we can see that for $\mu := \min\{\epsilon, \gamma\}$ and $K := \max\{N, M\}$, it holds that $\forall m \geq K(\mu <_{\mathbb{Q}} l_m - h_m)$, which is the definition of $h < l$.

2. (*Transitivity*) Let $f, g, h \in CauchySeq_{\mathbb{Q}}$. Assume $f < g$ and $g < h$. By definition we have that $\exists \gamma \in \mathbb{Q}_{\geq 0}\ \exists M \in \mathbb{N}\ \forall m \geq M(\gamma <_{\mathbb{Q}} g_m - f_m)$ and $\exists \epsilon \in \mathbb{Q}_{\geq 0}\ \exists N \in \mathbb{N}\ \forall m \geq N(\epsilon <_{\mathbb{Q}} h_m - g_m)$. Thus, we conclude that for $\mu := \max\{\epsilon, \gamma\}$ and $K := \min\{N, M\}$, $\forall m \geq K(\mu <_{\mathbb{Q}} h_m - f_m)$.

3. (*Irreflexivity*) Let $f \in CauchySeq_{\mathbb{Q}}$. then $\forall m \in \mathbb{N}(f_m - f_m = 0)$. Thus, $\neg(f \# f)$. $\exists \epsilon \in \mathbb{Q}\ \exists N \in \mathbb{N}\ \forall m \geq N(\epsilon + f_m <_{\mathbb{Q}} g_m)$

4. (*Asymmetry*) Let $f, g \in CauchySeq_{\mathbb{Q}}$. Assume $f < g$. By definition, this means $\exists \epsilon \in \mathbb{Q}_{\geq 0}\ \exists N \in \mathbb{N}\ \forall m \geq N(\epsilon + f_m <_{\mathbb{Q}} g_m)$. We must prove that $\neg(g < f)$. This will be done by contradiction. Assume $g < f$. This means that $\exists \gamma \in \mathbb{Q}_{\geq 0}\ \exists M \in \mathbb{N}\ \forall m \geq N(\gamma + g_m <_{\mathbb{Q}} f_m)$. Let $K := \max\{N, M\}$. Then, $\forall m \geq K(\epsilon + f_m \geq g_m)$ by definition of K. Also, $\forall m \geq K(\gamma + f_m \geq g_m)$ by definition of K. Thus, we get $\forall m \geq K(f_m + \epsilon < g_m < g_m + \gamma < f_m < f_m + \epsilon)$. This is a contradiction. So, $\neg(g < f)$.

5. (*Addition respects* $<$) This is a consequence of the previous four points.

□

We move on to the proof of Theorem 2.22.

Proof. (Theorem 2.22) Definitions 2.24, 2.25, 2.26 and 2.27 make $CauchySeq_{\mathbb{Q}}$ a field with an apartness relation. Moreover, Lemma 2.28 and its proof show that $CauchySeq_{\mathbb{Q}}$ is an ordered field. Thus, we conclude that $CauchySeq_{\mathbb{Q}}$ is a constructive ordered field. □

Now, we move on to proving Theorem 2.23. For this theorem, we have to prove that $CauchySeq_{\mathbb{Q}}$ is Archimedean and Cauchy Complete. For the first characteristic, we introduce the following lemma.

Lemma 2.29. *Let $f \in CauchySeq_{\mathbb{Q}}$. Then, there exists an upper bound for every sequence term of f. Formally, this translates to $\exists K \in \mathbb{Q}_{\geq 0}\ \forall m \in \mathbb{N}(|f_m| < K)$.*

Proof. Pick $\epsilon > 0$, then $\exists N \in \mathbb{N}$ such that $\forall n, m \in \mathbb{N}(|f_m - f_n| < \epsilon)$. Now, let us define $M := \max\{f_0, f_1, \ldots, f_N\}$. We have the following $\forall m \geq N$:

$$|f_m| = |f_m - f_N + f_N| \leq |f_m - f_N| + |f_N| < \epsilon + M$$

Thus, picking $K := M + \epsilon$ gives us our desired result. □

For any sequence $f \in CauchySeq_{\mathbb{Q}}$, if our $K \in \mathbb{N}$ then we are done and we pick the constant sequence $\mathbf{K} := (K, K, K, \ldots)$. If not, we know from before that $\mathbb{Q}$ is Archimedean so for K there is a $K' \in \mathbb{N}$ such that $K < K'$. Thus, we pick the sequence **K'** $:= (K', K', K', \ldots)$. This gives us a bound for f in $CauchySeq_{\mathbb{N}}$. Thus, we have that $CauchySeq_{\mathbb{Q}}$ is Archimedean. For the Cauchy completeness property, we pick an arbitrary Cauchy sequence of Cauchy sequences $\{f_n^i\}_{i=0}^{\infty}$ and show it converges to a limit sequence g that we will construct. First, we introduce the notion of strong Cauchy for a sequence and prove two lemmas for sequences of this type.

Definition 2.30. A sequence f is strong Cauchy if it satisfies

$$\forall n \forall m > n(|f_m - f_n| < 2^{-n})$$

Lemma 2.31. *For every Cauchy sequence (f_n) there exists a subsequence (f_{n_k}) that is strong Cauchy. Moreover, (f_n) and (f_{n_k}) share the same limit.*

Proof. Let (f_n) be a Cauchy sequence. We will construct the subsequence (f_{n_k}). For this, we will use the modulus of convergence α of f_n. Now, let us define our subsequence in the following manner

$$f_{n_k} := f_{\alpha(k)}$$

We have to prove that f_{n_k} is strong Cauchy. For this, fix $k \in \mathbb{N}$. Now, for any $m \in \mathbb{N}$ we have that

$$|f_{n_k} - f_{n_{k+m}}| = |f_{\alpha(k)} - f_{\alpha(k+m)}| < 2^{-k}$$

So, we have that f_{n_k} is strong Cauchy.

Now, for the second part of the proposition, fix $K \in \mathbb{N}_{>0}$. We have that

$$|f_{n_k} - l| = |f_{n_k} - f_{n_k+m} + f_{n_k+m} - l| \leq |f_{n_k} - f_{n_k+m}| + |f_{n_k+m} - l| < 2^{-n_k} + 2^{-K} < 2^{-K+1}$$

Thus, pick $N := n_k + 1$ and we obtain our desired result. □

Now that we have defined the strong Cauchy condition for a sequence, we go back to our initial problem and consider the Cauchy sequence of Cauchy sequences $\{f_n^i\}_{i=0}^{\infty}$. Consider the sequence $(f_n^i)_{n\in\mathbb{N}}$ with modulus of convergence α_i for some $i \in \mathbb{N}$ and a respective subsequence $(f_{n_k}^i)$ which is strong Cauchy. This subsequence $(f_{n_k}^i)$ exists as we can construct it using its modulus of convergence in the following way:

$$(f_{n_k}^i) := (f_{\alpha_i(k)}^i).$$

By the previous lemma, we have that this subsequence shares the same limit than that of (f_n^i). Thus, our problem translates to showing that $(f_{n_k}^i)_{i=0}^{\infty}$ converges to a limit g in $CauchySeq_{\mathbb{Q}}$. We claim that the sequence $(g_n) := (f_{\alpha_n(n)}^n)$ is the limit of $(f_{n_k}^i)_{i=0}^{\infty}$. Let us first prove that this limit sequence $g \in CauchySeq_{\mathbb{Q}}$, and we will conclude with the proof of convergence.

Lemma 2.32. *The sequence $(g_n) := (f_{\alpha_n(n)}^n)$ is in $CauchySeq_{\mathbb{Q}}$.*

Proof. Let $k > 0$. We have that for $n, m \in \mathbb{N}$

$$|g_n - g_{n+m}| = |f_n^n - f_{n+m}^{n+m}| \leq |f_n^n - f_\infty^n + f_\infty^n - f_\infty^{n+m} + f_\infty^{n+m} - f_{n+m}^{n+m}| \leq$$

$$|f_n^n - f_\infty^n| + |f_\infty^n - f_\infty^{n+m}| + |f_\infty^{n+m} - f_{n+m}^{n+m}| < 2^{-k}$$

for an $N \in \mathbb{Z}$. □

Lemma 2.33. *The sequence $(f_{n_k}^i)_{i=0}^{\infty}$ converges to (g_n).*

Proof. Let $k > 0$ and fix $i \in \mathbb{N}$. This will be a proof of pointwise convergence. We have that for $n \in \mathbb{N}$

$$|f_{\alpha_n(i)}^n - f_{\alpha_n(n)}^n| = |f_{\alpha_n(i)}^n - f_\infty^n + f_\infty^n - f_\infty^i + f_\infty^i - f_{\alpha_n(n)}^n| \leq$$

$$|f_{\alpha_n(i)}^n - f_\infty^n| + |f_\infty^n - f_\infty^i| + |f_\infty^i - f_{\alpha_n(n)}^n| \leq 2^{-k}$$

for an $N \in \mathbb{Z}$. □

In this last proof, we conclude that for an arbitrary sequence $\{f^i\}_{i=0}^{\infty}$ of Cauchy sequences $f^i \in CauchySeq_{\mathbb{Q}}$, the sequence converges to a limit in $CauchySeq_{\mathbb{Q}}$. This means that $CauchySeq_{\mathbb{Q}}$ is Cauchy complete and Archimedean, which concludes the proof of Theorem 2.23. Having proved this, we can conclude that $CauchySeq_{\mathbb{Q}}$ is a real number structure according to Theorem 2.21. Thus, we have constructed the real numbers in Coq. In the next section, we will start the analysis of Kneser's algorithm taking into account all of the notions introduced in this chapter.

3 Kneser Algorithm

Manfred Kneser provided a proof for his root finding algorithm in 1981 inspired by a proof of his father, Hellmuth Kneser. This proof relies heavily on the rational numbers and not on an axiomatization of the reals, as we defined on the previous chapter. The original proof by M. Kneser can be found in [6] and an English translation of his proof can be found in [1]. The proof provided by his father was published in [7]. In this thesis we will reproduce and analyze the proof provided in [3], since this is the proof that uses the Coq axiomatization of the Real Numbers we introduced in the previous chapter. For simplicity, Kneser's Algorithm is first presented in terms of Classical Mathematics in [3], but we will not focus on this as our main objective is the Constructive version of the Kneser Algorithm that involves the apartness relation $\#$ in the real numbers. The proof is composed of six steps which, when put together, will prove the Fundamental Theorem of Algebra through Kneser's Algorithm for any polynomial of degree $n > 0$.

The idea of the algorithm is to use properties of the coefficients of a given polynomial to construct a Cauchy sequence that converges to a root of the polynomial. It is worthy to clarify that we will be using the rationals, unlike what M. Kneser did when he proved his algorithm, but we use the real number structure axiomatized in the previous chapter. Also, since we are working with the axioms of Constructive Mathematics, we still have to be aware of the undecidability of the equality in $\mathbb{R}$ (and as a consequence in $\mathbb{C}$). Because of this, we have to pay close attention in some stages of our proof to avoid ambiguity. Let us now start the proof with the first lemma.

The first section of the proof is a Lemma that allows us to determine the maximum element of a finite sequence "up to ϵ". Let us state and prove this.

Lemma 3.1. *Let $n \in \mathbb{N}$, $\epsilon > 0$ and $c_1, \ldots, c_n \in \mathbb{R}$, then there is a k such that for all $i \in \{1, \ldots, n\}$ we have $c_k > c_i - \epsilon$. Formally, this translates to*

$$\forall n \in \mathbb{N}\ \forall \epsilon > 0\ \exists k\ \forall i \in \{1, \ldots, n\}(c_k > c_i - \epsilon)$$

Proof. This proof is done by induction on n. Let $\epsilon > 0$

1. *(Base Step)* Trivial.
2. *(Inductive Hypothesis)* Assume for some $n \in \mathbb{N}$ and $c_1, \ldots, c_n \in \mathbb{R}$ that $\exists k \forall i (c_k > c_i - \epsilon)$.
3. *(Inductive Step)* Consider $c_1, \ldots, c_n, c_{n+1} \in \mathbb{R}$. We already have that $\exists k (c_k < c_i - \frac{\epsilon}{2})$ for all $i \in \{1, \ldots, n\}$ from the Inductive Step, so we have two possibilities $c_k - \frac{\epsilon}{2} < c_{n+1} \vee c_{n+1} - \epsilon < c_k$. If $c_{n+1} - \epsilon < c_k$, pick c_k. Otherwise, if $c_k - \frac{\epsilon}{2} < c_{n+1}$, then by the cotransitive property of $<$, we have that $c_k - \epsilon < c_{n+1} \vee c_k - \frac{\epsilon}{2} < c_k - \epsilon$. Of which the only possible case is the first one, which is $c_k - \epsilon < c_{n+1}$.

□

This lemma introduces the preorder $\leq_\epsilon$ for $\epsilon > 0$, which will be useful in the Kneser algorithm. This preorder $\leq_\epsilon$ is not antisymmetric, which is why it is not a partial order. For two numbers x, y, we have that $x \leq_\epsilon y := x < y + \epsilon$. Conversely, it can also be expressed as $x \leq_\epsilon y := x - \epsilon < y$. With this notion and by the cotransitivity of $<$, we have $\forall x, y \in \mathbb{R}(x \leq_\epsilon y \vee y \leq_\epsilon x)$. The decidability for the partial order $\leq_\epsilon$ facilitates the comparison of two real numbers, as was not the case for $<$, where for any $x, y \in \mathbb{R}$ we had to determine between three cases $x < y \vee x = y \vee y < x$.

Now, we present two propositions that give us a specific properties about a set of positive numbers and we will apply these to the coefficients of a given monic polynomial in order to generate our desired Cauchy sequence that converges to a zero of the polynomial. We start with the first of these propositions.

Proposition 3.2. *Let $n > 0, \epsilon > 0, a_0 > \epsilon, a_1, \ldots, a_{n-1} \geq 0, a_n = 1$. We can construct an $r_0 > 0$ and $k_0 \in \{1, \ldots, n\}$ such that*

$$a_{k_0} r_0^{k_0} = a_0 - \epsilon$$

Moreover, for all $j \in \mathbb{N}$ there exists a $k_j \in \{1, \ldots, n\}$ with $k_0 \geq k_1 \geq \ldots \geq k_j \geq \ldots$ such that for all $i \in \{1, \ldots, n\}$

$$a_{k_j} \left(\frac{r_0}{3^{-j}}\right)^{k_j} > a_i \left(\frac{r_0}{3^{-j}}\right)^{i} - \epsilon$$

Formally, this statement translates to

$$\forall n \in \mathbb{N}\ \forall \epsilon > 0((a_0 > \epsilon \wedge a_1, \ldots, a_n \geq 0) \rightarrow (\exists r_0 > 0 \exists k_0 \in \{1, \ldots, n\}(a_{k_0} r_0^{k_0} = a_0 - \epsilon)\ \wedge \forall j \in \mathbb{N}_{>0}$$

$$\exists k_j \in \{1, \ldots, n\}(k_0 \geq k_1 \geq \ldots \geq k_j \geq \ldots\ \wedge\ \forall i \in \{1, \ldots, n\}(a_{k_j} \left(\frac{r_0}{3^{-j}}\right)^{k_j} > a_i \left(\frac{r_0}{3^{-j}}\right)^{i} - \epsilon)))).$$

Proof. The proof is divided into two parts. In the first part, we must determine the appropriate choice for k_0 and r_0 to be able to prove the equality of the proposition. This will be done by taking initial values for both k_0 and r_0 and updating them through an algorithm that will be described below, considering in turn for i the values $n-1$ until 1, in this order. We will consider these two following invariants:

$$a_{k_0} r_0^{k_0} = a_0 - \epsilon \tag{1}$$

$$a_{k_0} r_0^{k_0} > a_l r_0^l - \epsilon \quad \textit{for all } l \in \{i, \ldots, n\} \tag{2}$$

In the second part, we will focus on generating the sequence of k_j's and proving the inequality of the proposition.

1. Let us start by taking $k_0 = n$ and $r_0 = \sqrt[n]{a_0 - \epsilon}$. For now, this choice satisfies (1). We will start updating k_0 and r_0 as follows (running i from $n-1$ to 1):

   - If $a_i r_0^i < a_0$, do nothing since $a_i r_0^i - \epsilon < a_0 - \epsilon = a_n(\sqrt[n]{a_0 - \epsilon})^n = a_{k_0} r_0^{k_0}$. So both invariants are respected.
   - If $a_0 - \epsilon < a_i r_0^i$, set k_0 to i and r_0 to $\sqrt[i]{\frac{a_0 - \epsilon}{a_i}}$. By assumption, r_0 decreases. This still respects (1). Now, we must show that our new choice for k_0 and r_0 respect (2). This is the case because for every l such that $i < l \leq n$ it holds that $a_i r_0^i = a_0 - \epsilon > a_l r_0^l - \epsilon$.

   After applying this algorithm, we have the proper choice of k_0 and r_0.

2. In this step, we will first determine the sequence $k_0 \geq k_1 \geq \ldots$. This will be done through an inductive algorithm, which at the same time, will satisfy the inequality of the proposition. Assume we have k_j for some $j \in \mathbb{N}$ and define $r_j := 3^{-j} r_0$. Consider the sequence

   $$a_1 \left(\frac{r_j}{3}\right), a_2 \left(\frac{r_j}{3}\right)^2, \ldots, a_{k_j} \left(\frac{r_j}{3}\right)^{k_j}$$

   Applying the previous lemma for $\frac{\epsilon}{2}$ to this sequence, we obtain k_{j+1}. We have to show that this satisfies the proposition. The fact that $k_j \geq k_{j+1}$ is trivial. We now must show the inequality. We have to consider two cases for i: $i \leq k_j \vee i > k_j$.

   - For $i \leq k_j$, we have that $a_{k_{j+1}}(r_{j+1})^{k_{j+1}} = a_{k_{j+1}} \left(\frac{r_j}{3}\right)^{k_{j+1}} > a_i \left(\frac{r}{3}\right)^i - \epsilon = a_i (r_{j+1})^i - \epsilon$ by the way we chose k_{j+1}.
   - For $i > k_j$ we have:

     $$a_{k_j} \left(\frac{r_j}{3}\right)^{k_j} = 3^{-k_j} a_{k_j} (r_j)^{k_j} > 3^{-k_j}(a_i (r_j)^i - \epsilon) = 3^{-k_j} a_i (r_j)^i - 3^{-k_j}\epsilon > a_i (r_{j+1})^i - \frac{\epsilon}{2}$$

     So, it is the case that

     $$a_{k_{j+1}}(r_{j+1})^{k_{j+1}} = a_{k_{j+1}} \left(\frac{r_j}{3}\right)^{k_{j+1}} > a_{k_j} \left(\frac{r_j}{3}\right)^{k_j} - \frac{\epsilon}{2} > a_i \left(\frac{r_j}{3}\right) - \epsilon$$

   This concludes the proof of the inequality in the proposition.

□

Now, let us state and prove the second proposition.

Proposition 3.3. *Let $n > 0, \epsilon > 0, a_0 > \epsilon, a_1, \ldots, a_{n-1} \geq 0, a_n = 1$. We can construct an $r > 0$ and a $k \in \{1, \ldots, n\}$ such that they satisfy the three following properties:*

$$r^n < a_0$$

$$3^{-2n^2} a_0 - 2\epsilon < a_k r^k < a_0$$

$$\sum_{i=1}^{k-1} a_i r^i + \sum_{i=k+1}^{n} a_i r^i < (1-3^{-n})a_k r^k + 3^n\epsilon$$

Formally, this translates to

$$\exists r > 0 \exists k \in \{1,\dots,n\}(r^n < a_0 \ \wedge \ 3^{-2n^2}a_0 - 2\epsilon < a_k r^k < a_0 \ \wedge$$
$$\sum_{i=1}^{k-1} a_i r^i + \sum_{i=k+1}^{n} a_i r^i < (1-3^{-n})a_k r^k + 3^n\epsilon).$$

Proof. We apply the previous proposition to obtain the sequence $k_0 \geq k_1 \geq k_2 \geq \dots$ and we define $r_j = 3^{-j}r_0$ for $j \in \mathbb{N}$. We have that k_j for $j \in \mathbb{N}$ is non-increasing in $\{1,\dots,n\}$, then there is a j' such that $k_{j'-1} = k_{j'} = k_{j'+1}$. Let us define $k = k_{j'}$ and $r = r_{j'}$. By the previous proposition, we also have that for all $i \in \{1,\dots,n\}$:

$$a_i r^i = a_i (r_{j'})^i = \frac{a_i (r_0)^i}{3^{ij'}} \leq a_i (r_0)^i < a_{k_0}(r_0)^{k_0} + \epsilon = a_0$$

Thus, for $i = n$, we have that $a_n r^n = r^n < a_0$, which is the first inequality we had to prove was satisfied. For $i = k$, we have that $a_k r^k < a_0$. This proves the first part of the second inequality. For the second part of the inequality, we use the following fact:

$$a_{k_0} r^{k_0} = 3^{-j'k_0} a_{k_0}(r_0)^{k_0} \geq 3^{-j'n} a_{k_0}(r_0)^{k_0} = 3^{-j'n}(a_0 - \epsilon) \geq 3^{-j'n}a_0 - \epsilon$$

Having this and combining it with the previous proposition, we also can conclude that

$$a_k r^k > a_{k_0} r^{k_0} - \epsilon \geq 3^{-j'n} a_0 - 2\epsilon > 3^{-2n^2} a_0 - 2\epsilon$$

This finishes the proof for the second inequality. We move on to proving the third inequality. Since $k = k_{j'+1}$, we have that for all $i \in \{1,\dots,n\}$

$$a_k \left(\frac{r}{3}\right)^k = a_{k_{j'+1}} \left(\frac{r_{j'}}{3}\right)^{k_{j'+1}} = a_{k_{j'+1}} (r_{j'+1})^{k_{j'+1}} > a_i (r_{j'+1})^i - \epsilon = a_i \left(\frac{r_{j'}}{3}\right)^i - \epsilon$$

Adding ϵ and multiplying by 3^i yields:

$$a_i r^i < 3^{i-k} a_k r^k + 3^i \epsilon$$

Summing over $1,\dots,k-1$ yields:

$$\begin{aligned}\sum_{i=1}^{k-1} a_i r^i &< \sum_{i=1}^{k-1} 3^{i-k} a_k r^k + \sum_{i=1}^{k-1} 3^i \epsilon \\ &= \frac{(1-3^{1-k})}{2} a_k r^k + \frac{(3^k - 3)}{2}\epsilon \\ &< \frac{(1-3^{1-k})}{2} a_k r^k + \frac{3^n}{2}\epsilon\end{aligned}$$

Also, since $k = k_{j'-1}$, we have that for all $i \in \{1,\dots,n\}$

$$a_k (3r)^k = a_{k_{j'-1}} (3r_{j'})^{k_{j'-1}} = a_{k_{j'-1}} (r_{j'-1})^{k_{j'-1}} > a_i (r_{j'-1})^i - \epsilon < a_i (3r)^i - \epsilon$$

Adding ϵ and dividing by 3^i yields:

$$a_i r^i < 3^{k-i} a_k r^k + 3^{-i}\epsilon$$

Summing over $k+1,\dots,n$ yields:

$$\sum_{i=k+1}^{n} a_i r^i < \sum_{i=k+1}^{n} 3^{k-i} a_k r^k + \sum_{i=k+1}^{n} 3^{-i}\epsilon < \frac{1-3^{-n}}{2} a_k r^k + \frac{3^n}{2}\epsilon$$

If we put together both results from the sums above, we conclude our last inequality

$$\sum_{i=1}^{k-1} a_i r^i + \sum_{i=k+1}^{n} a_i r^i < (1-3^{-n})a_k r^k + 3^n\epsilon$$

□

For this next section of the proof, we introduce the Kneser Lemma. This part of the algorithm that is attributed to Kneser and it sets its mark, and hence it is named after him. Although the Kneser Lemma does not have as immediate consequence the Fundamental Theorem of Algebra, it does give way into proving a special case of the Fundamental Theorem of Algebra that considers monic polynomials. In the Kneser Lemma, we use the results from the previous two propositions.

Proposition 3.4 (**Kneser Lemma**). *For every $n > 0$ there is a $q \in (0,1)$ such that for every monic complex polynomial $f(z)$ of degree n and for all $c > 0$ satisfying $|f(0)| < c$, there exists a $z' \in \mathbb{C}$ with $|z'|^n < c$ and $|f(z')| < qc$.*

Proof. For $n > 0$, define $q := 1 - 3^{-2n^2-n}$. It is obvious that $0 < q < 1$. Now, we have to determine z'. Let us write our polynomial $f(z)$ as $f(z) = b_n z^n + \ldots + b_1 z + b_0$. We assumed $f(z)$ to be monic, so $b_n = 1$. Also, $f(0) = b_0$ so when we consider all c's such that $|f(0)| < c$, we really mean all c's such that $|b_0| < c$. We will consider an arbitrary c that satisfies $|b_0| < c$. Since $0 < qc$, then by the cotransitive property of $<$, we can determine:

$$|f(0)| < qc \vee 0 < |f(0)|$$

If we have that $|f(0)| < qc$, then pick $z' = 0$ and we are done. If $0 < |f(0)|$ holds, then proceed as follows to find z'.

Define $a_i := |b_i|$ for $i \in \{1, \ldots, n\}$ and choose $\epsilon > 0$ such that the following holds

$$2\epsilon < 3^{-2n^2} a_0 \tag{3}$$

$$(3^n + 1)\epsilon < q(c - a_0) \tag{4}$$

By (3), $\epsilon < 2\epsilon < 3^{-2n^2} a_0 < a_0$ holds. Thus, we have $a_1, \ldots, a_{n-1} \geq 0$, $a_0 > \epsilon$ and $a_n = 1$. This means we can apply the Proposition 3.3 to obtain $r > 0$ and $k \in \{1, \ldots, n\}$ that satisfy:

$$r^n < a_0$$

$$3^{-2n^2} a_0 - 2\epsilon < a_k r^k < a_0$$

$$\sum_{i=1}^{k-1} a_i r^i + \sum_{i=k+1}^{n} a_i r^i < (1 - 3^{-n}) a_k r^k + 3^n \epsilon$$

We claim that $z' = r \sqrt[k]{-\frac{b_0/b_k}{a_0/a_k}}$ satisfies the properties to be proven. This choice of z' is based on (3) and the result of applying the Proposition 3.3 in the step before, since this assures that $a_k > 0$. Let us verify the first condition that z' has to satisfy, that is, $|z'| < c$. For this, consider that $|b_0| = a_0$ and $|b_k| = a_k$. So, we have

$$|z'| = \left| r \sqrt[k]{-\frac{b_0/b_k}{a_0/a_k}} \right| = r \left| \sqrt[k]{\frac{b_0/b_k}{a_0/a_k}} \right| |i| = r \sqrt[k]{\frac{|b_0|/|b_k|}{a_0/a_k}} = r \sqrt[k]{\frac{a_0/a_k}{a_0/a_k}} = r$$

Combining this $|b_0| < c$ and Proposition 3.3, we get

$$|z'|^n = r^n < a_0 = |b_0| < c$$

This proves the first property of z'. For the second property z' has to satisfy, that is, $|f(z')| < qc$, we compute the following

$$\begin{aligned}
|b_0 + b_k (z')^k| &= \left| b_0 - b_k r^k \frac{b_0/b_k}{a_0/a_k} \right| \\
&= \left| b_0 - \frac{r^k b_0}{a_0/a_k} \right| \\
&= \left| \frac{b_0}{a_0} (a_0 - r^k a_k) \right| \\
&= \frac{|b_0|}{a_0} |a_0 - r^k a_k| \\
&= a_0 - a_k r^k \qquad (a_0 > a_k r^k \text{ from Proposition 3.3})
\end{aligned}$$

Having this, we finally conclude (using that the triangle inequality holds for complex numbers)

$$\begin{aligned}
|f(z')| = \left|\sum_{i=0}^{n} b_i z'^i\right| &\leq |b_0 + b_k(z')^k| + \left|\sum_{i=1}^{k-1} b_i (z')^i\right| + \left|\sum_{i=k+1}^{n} b_i (z')^i\right| \\
&\leq |b_0 + b_k(z')^k| + \sum_{i=1}^{k-1} |b_i (z')^i| + \sum_{i=k+1}^{n} |b_i (z')^i| \\
&= |b_0 + b_k(z')^k| + \sum_{i=1}^{k-1} a_i r^i + \sum_{i=k+1}^{n} a_i r^i \\
&< a_0 - a_k r^k + (1 - 3^{-n}) a_k r^k + 3^n \epsilon \\
&= a_0 - 3^{-n} a_k r^k + 3^n \epsilon \\
&< a_0 - 3^{-n}(3^{-2n^2} a_0 - 2\epsilon) + 3^n \epsilon && \text{Proposition 3.3} \\
&= (1 - 3^{-2n^2 - n}) a_0 + 3^n \epsilon + 3^{-n} 2\epsilon \\
&< q a_0 + 3^n \epsilon + \epsilon \\
&= q a_0 + (3^n + 1)\epsilon \\
&< q a_0 + q(c - a_0) = qc && \text{Consequence of (4)}
\end{aligned}$$

This concludes the proof for this proposition. □

As mentioned before, the Kneser Lemma gives way to the following proposition.

Proposition 3.5 (**Fundamental Theorem of Algebra for Monic Polynomials**). *For every monic complex polynomial $f(z)$, there exists a $z_\infty \in \mathbb{C}$ such that $f(z_\infty) = 0$.*

Proof. Take $c_0 > 0$ such that $c_0 > |f(0)|$. We will construct a Cauchy sequence $(z_i)_{i \in \mathbb{N}}$ that will converge to z_∞. The sequence will be contructed as follows:

- For $i = 1$, we apply the Kneser Lemma fo $f(z)$ and obtain z_1, which will satisfy the properties of $|f(z_1)| < qc_0$ and $|z_1|^n < c_0$.
- For z_{i+1}, consder z_i and the polynomial $f_{z_i}(z) \equiv f(z + z_i)$. Set $c := q^i c_0$. Since $c > |f_{z_i}(0)|$, we apply the Kneser Lemma to $f_{z_i}(z)$ and obtain a term we will call y_i which will satisfy $|f_{z_i}(y_i)| < qc = q^{i+1} c_0$ and $|y_i| < c$. Finally, we define $z_{i+1} := y_i + z_i$.

We claim that the sequence $(z_i)_{i \in \mathbb{N}}$ satisfies the following two properties:

$$|f(z_i)| < q^i c_0 \tag{5}$$

$$|z_{i+1} - z_i| < \sqrt[n]{q^i c_0} \tag{6}$$

Let us prove this by induction of i:

1. *(Base Step)* Let $i = 2$ and $c = qc_0$. We know that $z_2 = y_1 + z_1$, where y_1 is the result of applying the Kneser Lemma to $f_{z_1}(z)$. Thus, we have that (5) is satisfied since $|f(z_2)| = |f(y_1 + z_1)| = |f_{z_1}(y_1)| < qc = q^2 c_0$. Also, if we rearrange $z_2 = y_1 + z_1$ to $y_1 = z_2 - z_1$, we have that $|z_2 - z_1|^n = |y_1|^n < c = c_0$. So, $|z_2 - z_1| < \sqrt[n]{qc_0}$, which satisfies (6).
2. *(Inductive Hypothesis)* Assume for some i that z_i satisfies (5) and (6).
3. *(Inductive Step)* We will show that z_{i+1} satisfies (5) and (6). Set $c = q^i c_0$. Since z_i satisfies (5), we have that $|f_{z_i}(0)| < c$ we can apply the Kneser Lemma to $f_{z_i}(z)$ and obtain y_i. Also, we have that $z_{i+1} = y_i + z_i$, so we conclude that $|f(z_{i+1})| = |f(y_i + z_i)| = |f_{z_i}(y_i)| < qc = q^{i+1} c_0$. Also, if we rearrange $z_{i+1} = y_i + z_i$ to obtain $y_i = z_{i+1} - z_i$ we get $|z_{i+1} - z_i|^n = |y_i|^n < c = q^i c_0$. Finally, $|z_{i+1} - z_i| = |y_i| < \sqrt[n]{q^i c_0}$. Thus, z_{i+1} satisfies (5) and (6).

Having these properties of $(z_i)_{i\in\mathbb{N}}$, we can now prove that it is Cauchy. Consider, for $m, l > 0$

$$\begin{aligned}
|z_{m+l} - z_m| &= |z_{m+l} - z_{m+l-1} + z_{m+l-1} - \ldots - z_{m+1} + z_{m+1} - z_m| \\
&\leq |z_{m+l} - z_{m+l-1}| + \ldots + |z_{m+1} - z_m| \\
&< \sum_{k=0}^{l-1} (q^{m+k}c)^{\frac{1}{n}} \\
&= c^{\frac{1}{n}} \sum_{k=0}^{l-1} q^{\frac{m+k}{n}} \\
&= c^{\frac{1}{n}} \left(\frac{q^{\frac{m}{n}} - q^{\frac{m+l}{n}}}{1 - q^{\frac{1}{n}}} \right) \\
&= c^{\frac{1}{n}} q^{\frac{m}{n}} \left(\frac{1 - q^{\frac{l}{m}}}{1 - q^{\frac{1}{n}}} \right) \\
&< \frac{c^{\frac{1}{n}} q^{\frac{m}{n}}}{1 - q^{\frac{1}{n}}}
\end{aligned}$$

By taking m large enough, we can make the final expression as small as possible and that will guarantee the Cauchy property. Since $(z_i)_{i\in\mathbb{N}}$ is Cauchy, then we have that $z_\infty = \lim_{i\to\infty} z_i$ exists

and since $f(z)$ is a polynomial, and thus, it is continuous, we have that:

$$|f(z_\infty)| = \lim_{i\to\infty} |f(z_i)| \leq \lim_{i\to\infty} q^i c_0 = 0$$

Since $0 < q < 1$. So $f(z_\infty) = 0$. □

Before proving the Fundamental Theorem of Algebra for all polynomials, we must define the notion of a non-constant polynomial. Intuitively, a non-constant polynomial is a polynomial of positive degree. Since we are working within Constructivism, we need a more precise definition of a non-constant polynomial.

Definition 3.6. A polynomial $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ is non-constant if there is a $k \in \{1, \ldots, n\}$ such that $a_k \# 0$.

Having this notion defined, we now present a proposition that is the opposite of what we are striving to prove. We need a way of knowing that a given polynomials not the zero polynomial. Before, we were assuming that all of our polynomials were monic of positive degree, but we need to prove the Fundamental Theorem of Algebra for every for any given polynomial of positive degree. To ensure that our polynomial is non-constant, we introduce the following proposition.

Proposition 3.7. *Let $n \in \mathbb{N}_{>0}$. If f is a non-constant polynomial of degree at most n and there are $n+1$ distinct points $z_0, z_1, \ldots, z_n \in \mathbb{C}$, then $f(z_i) \# 0$ for at least one of the z_i's.*

Proof. We write $f(z)$ as:

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$$

By assumption, we have that there is a $k \in \{1, \ldots, n\}$ such that $a_k \# 0$. Now, we use $z_0, \ldots, z_n$ to interpolate the polynomial $f(z)$ in the following way:

$$f(z) = \sum_{i=0}^{n} f(z_i) \frac{(z - z_0) \cdot \ldots \cdot (z - z_{i-1})(z - z_{i+1}) \cdot \ldots \cdot (z - z_n)}{(z_i - z_0) \cdot \ldots \cdot (z_i - z_{i-1})(z_i - z_{i+1}) \cdot \ldots \cdot (z_i - z_n)}$$

Both sides of this equality are polynomials of degree at most n and they coincide on $n+1$ points, by the definition of interpolation, so they must be equal on $\mathbb{C}$. Thus, we can write $f(z)$ in the form

$$f(z) = \sum_{i=0}^{n} f(z_i) f_i(z)$$

where $f_i(z) = \frac{(z-z_0)\cdot\ldots\cdot(z-z_{i-1})(z-z_{i+1})\cdot\ldots\cdot(z-z_n)}{(z_i-z_0)\cdot\ldots\cdot(z_i-z_{i-1})(z_i-z_{i+1})\cdot\ldots\cdot(z_i-z_n)}$. Since $f \# 0$, then the right hand side is $\#0$ so we must have $f(z_i)f_i(z) \# 0$ for some $i \in \{1,\ldots,n\}$. This means that $f(z_i) \# 0$ for this specific i. □

Just before proving the Fundamental Theorem of Algebra for an arbitrary polynomial, we introduce the reverse of a polynomial which is a notion needed for the final part of this proof.

Definition 3.8. For a polynomial $f(z) = a_n z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$ we define its reverse $f^{rev}(z)$ as $f^{rev}(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_{n-1}z + a_n$. More specifically, $f^{rev}(z) = z^n \cdot f\left(\frac{1}{z}\right)$.

Remark. Observe that for two polynomials g, h we have that $(gh)^{rev} = g^{rev}h^{rev}$.

Finally, let us prove the Fundamental Theorem of Algebra through Kneser's Algorithm.

Theorem 3.9 (**Fundamental Theorem of Algebra**). *Let $f(z)$ be a non-constant polynomial. Then, there exist a $z' \in \mathbb{C}$ such that $f(z') = 0$.*

Proof. We write $f(z)$ as

$$f(z) = a_n z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$$

Since we do not know whether $a_n = 0 \vee a_n \# 0$, we will call n the length of f, instead of the degree. This proof goes by strong induction on n.

1. *(Base Step)* Let $n = 1$, so $f(z) = a_1 z + a_0$. Since $f \# 0$, then $a_1 \# 0$. Thus, $z' := \frac{-a_0}{a_1}$ satisfies the equation $f(z') = 0$.

2. *(Inductive Hypothesis)* For every $n = 1, 2, \ldots, k$ where $k \in \mathbb{N}$, it holds that for every non-constant polynomial $f(z)$ of length k, there exists a $z' \in \mathbb{C}$ such that $f(z') = 0$.

3. *(Inductive Step)* Let $f(z) = a_{k+1}z^{k+1} + a_k z^k + \ldots + a_1 z + a_0$ be a non-constant polynomial of length $k+1$. Since f is of degree at most $k+1$, we have that there is a $z_0 \in \mathbb{C}$ such that $f(z_0) \# 0$ by Proposition 3.7. Now, we consider the polynomial $f_{z_0}(z) \equiv f(z + z_0)$. The problem translates to finding a z' for $f_{z_0}(z)$ such that $f_{z_0}(z') = 0$ because this would mean that $z_0 + z'$ is a root of f. We write $f_{z_0}(z)$ as

   $$f_{z_0}(z) = b_{k+1}z^{k+1} + b_k z^k + \ldots + b_1 z + b_0$$

   where $b_0 = f(z_0) \# 0$.

   Let us consider now the polynomial $f_{z_0}^{rev}$. Also, let us remember that for two polynomials h, g, we have that $(gh)^{rev} = (g)^{rev}(h)^{rev}$. Since $\frac{f_{z_0}^{rev}(z)}{b_0}$ is monic, then there is a $c \in \mathbb{C}$ such that $\frac{f_{z_0}^{rev}(c)}{b_0} = 0$. Thus, we can write $\frac{f_{z_0}^{rev}(c)}{b_0}$ as

   $$\frac{f_{z_0}^{rev}(z)}{b_0} = (z-c)g(z)$$

   More precisely, we have that

   $$f_{z_0}^{rev}(z) = b_0(z-c)g(z)$$

   So,

   $$f_{z_0}(z) = b_0(cz-1)h(z)$$

   where $h(z) = g^{rev}(z)$ and it is of the form $h(z) = d_k z^k + d_{k-1}z^{k-1} + \ldots + d_1 z + d_0$. Since $f_{z_0}(z)$ is non-constant, we have that $b_i \# 0$ for some $i \in \{1,\ldots,k+1\}$, which allows us to conclude that $b_i = b_0 d_i + (-c)b_0 d_{i-1}$. Therefore, we have $b_0 d_i \# 0 \vee (-c)b_0 d_{i-1} \# 0$.

   - If $b_0 d_i \# 0$, then $d_i \# 0$ so $h(z)$ is non-constant which means that, by our inductive hypothesis, $h(z)$ has a zero which we call y. Thus, $z' = z_0 + y$ is a root of f.
   - If $(-c)b_0 d_{i-1} \# 0$, then $(-c)b_0 \# 0$ which means that $z' = \frac{1}{c} + z_0$ is a root of f.

□

As we have seen in this chapter, this algorithm does not rely on rational numbers to find a root of any polynomial. Also, the first three propositions involved the real numbers exclusively because we apply them to the modulus of the coefficients of our given polynomial. Moreover, the Kneser Lemma gives us way into the Fundamental Theorem of Algebra for Monic Polynomials, and with some additional notions and the proof of an extra property of non-constant polynomials, we conclude with the proof of the Fundamental Theorem of Algebra. In the next chapter, we will elaborate on a comparison of the proof presented in this chapter of the Kneser Algorithm and an alternative proof of the algorithm given in [1].

4 A Variation of the Kneser Algorithm

In this chapter, we will compare and contrast the proof of the Kneser Algorithm given in the previous chapter and the proof given by A. S. Troelstra in [1]. This comparison focuses mainly on Proposition 3.2 and it implements a different algorithm such that the generated sequences (r_n) and (k_n) start from $n = -1$ and not from $n = 0$ as we described in the previous chapter. For practical manners, we reproduced and analyzed the proof in [3] since axiomatizing a sequence that starts at $n = -1$ would lead to an adjustment of the formulas that are presented later in the proof. This is because we would have to shift the sequence by one and this requires additional adjustment. It is important to note that both ways of presenting and proving the algorithm are valid.

The purpose of implementing this brief chapter on the variation of the proof of the Kneser Algorithm is to show an alternative way of proving the algorithm through the use of a shifted sequence. This new sequence starting from $n = -1$ of k_n's and r_n's affects the convergence behavior of the algorithm when it is implemented for a given non-constant polynomial. Let us first reproduce the proof of the alternative version of Proposition 3.2 and then elaborate on the consequence this has on the implementation. We will only treat this superficially since this thesis focuses mainly on the theoretical part of the Kneser Algorithm. More on this topic can be read in [3]. The alternative version of Proposition 3.2 goes as follows.

Proposition 4.1 (**Proposition 3.2 as in [1]**). *Let $n > 0, \epsilon > 0, a_0 > \epsilon, a_1, \ldots, a_{n-1} \geq 0, a_n = 1$. We can construct an $r_0 > 0$ and $k_0 \in \{1, \ldots, n\}$ such that*

$$a_{k_0} r_0^{k_0} = a_0 - \epsilon$$

Moreover, for all $j \in \{-1, 0, 1, 2, \ldots\}$ there exists a $k_j \in \{1, \ldots, n\}$ with $k_{-1} \geq k_0 \geq k_1 \geq \ldots \geq k_j \geq \ldots$ such that for all $i \in \{1, \ldots, n\}$

$$a_{k_j} \left(\frac{r_0}{3^{-j}}\right)^{k_j} > a_i \left(\frac{r_0}{3^{-j}}\right)^{i} - 3^{-n}\epsilon$$

Formally, this statement translates to

$$\forall n \in \mathbb{N}\ \forall \epsilon > 0((a_0 > \epsilon \wedge a_1, \ldots, a_n \geq 0) \rightarrow (\exists r_0 > 0 \exists k_0 \in \{1, \ldots, n\}(a_{k_0} r_0^{k_0} = a_0 - \epsilon)\ \wedge \forall j \in \mathbb{N}_{>0}$$

$$\exists k_j \in \{1, \ldots, n\}(k_0 \geq k_1 \geq \ldots \geq k_j \geq \ldots\ \wedge\ \forall i \in \{1, \ldots, n\}(a_{k_j} \left(\frac{r_0}{3^{-j}}\right)^{k_j} > a_i \left(\frac{r_0}{3^{-j}}\right)^{i} - 3^{-n}\epsilon)))).$$

Proof. The proof is divided into two parts, as the one for Proposition 3.2. In the first part, we must determine the appropriate choice for k_0 and r_0 to be able to prove the equality of the proposition. This will be done by taking initial values for both k_0 and r_0 and updating them through an algorithm that will be described below, considering in turn for i the values $n - 1$ until 1, in this order. We will consider these two following invariants:

$$a_{k_0} r_0^{k_0} = a_0 - \epsilon \tag{1}$$

$$a_{k_0} r_0^{k_0} > a_l r_0^l - 3^{-n}\epsilon \quad \textit{for all } l \in \{i, \ldots, n\} \tag{2}$$

In the second part, we will focus on generating the sequence of k_j's as well as generating k_{-1} and proving the inequality of the proposition.

1. Let us start by taking $k_0 = n$ and $r_0 = \sqrt[n]{a_0 - \epsilon}$. For now, this choice satisfies (1). We will start updating k_0 and r_0 as follows (running i from $n - 1$ to 1):

   - If $a_i r_0^i < a_0 - \epsilon + 3^{-n}\epsilon$, do nothing since $a_i r_0^i - 3^{-n}\epsilon < a_0 - \epsilon = a_n(\sqrt[n]{a_0 - \epsilon})^n = a_{k_0} r_0^{k_0}$. So both invariants are respected.
   - If $a_0 - \epsilon < a_i r_0^i$, set k_0 to i and r_0 to $\sqrt[i]{\frac{a_0 - \epsilon}{a_i}}$. By assumption, r_0 decreases. This still respects (1). Now, we must show that our new choice for k_0 and r_0 respect (2). This is the case because for every l such that $i < l \leq n$ it holds that $a_i r_0^i = a_0 - \epsilon > a_l r_0^l - 3^{-n}\epsilon$.

   After applying this algorithm, we have the proper choice of k_0 and r_0.

2. In this step, we will first determine the sequence $k_0 \geq k_1 \geq \ldots$. This will be done through an inductive algorithm, which at the same time, will satisfy the inequality of the proposition. Assume we have k_j for some $j \in \mathbb{N}$ and define $r_j := 3^{-j} r_0$. Consider the sequence

$$a_1 \left(\frac{r_j}{3}\right), a_2 \left(\frac{r_j}{3}\right)^2, \ldots, a_{k_j} \left(\frac{r_j}{3}\right)^{k_j}$$

Applying Lemma 3.1 for $\frac{3^{-n}\epsilon}{2}$ to this sequence, we obtain k_{j+1}. We have to show that this satisfies the proposition. The fact that $k_j \geq k_{j+1}$ is trivial. We now must show the inequality. We have to consider two cases for i: $i \leq k_j \vee i > k_j$.

- For $i \leq k_j$, we have that $a_{k_{j+1}}(r_{j+1})^{k_{j+1}} = a_{k_{j+1}} \left(\frac{r_j}{3}\right)^{k_{j+1}} > a_i \left(\frac{r}{3}\right)^i - 3^{-n}\epsilon = a_i (r_{j+1})^i - 3^{-n}\epsilon$ by the way we chose k_{j+1}.
- For $i > k_j$ we have:

  $$a_{k_j} \left(\frac{r_j}{3}\right)^{k_j} = 3^{-k_j} a_{k_j} (r_j)^{k_j} > 3^{-k_j}(a_i (r_j)^i - 3^{-n}\epsilon) = 3^{-k_j} a_i (r_j)^i - 3^{-(k_j+n)}\epsilon > a_i (r_{j+1})^i - \frac{3^{-n}\epsilon}{2}$$

  So, it is the case that

$$a_{k_{j+1}}(r_{j+1})^{k_{j+1}} = a_{k_{j+1}} \left(\frac{r_j}{3}\right)^{k_{j+1}} > a_{k_j} \left(\frac{r_j}{3}\right)^{k_j} - \frac{3^{-n}\epsilon}{2} > a_i \left(\frac{r_j}{3}\right) - 3^{-n}\epsilon$$

Finally, in order to obtain k_{-1}, we consider the following sequence:

$$a_{k_0}(3r_0)^{k_0}, \ldots, a_n (3r_0)^n$$

Apply Lemma 3.1 with $\frac{\epsilon}{2}$ and this way we obtain k_{-1}. It is easy to see that it satisfies $k_{-1} \geq k_j$ for all $j \in \mathbb{N}$ and it also satisfies $a_{k_j} \left(\frac{r_0}{3^{-j}}\right)^{k_j} > a_i \left(\frac{r_0}{3^{-j}}\right)^i - 3^{-n}\epsilon$.
This concludes the proof of the inequality in the proposition.

□

As we can see in the proof, the sequence of k_j's starts at $j = -1$ and then continues on for $j \in \mathbb{N}$. This affects the convergence behavior when the algorithm is implemented, as we stated before. This is because when we apply Proposition 3.3 and get our k and r having used Proposition 4.1 before, we get an r that is three times larger than the one obtained by applying Proposition 3.2 before applying Proposition 3.3. When the Cauchy sequence is close to the zero of the polynomial, the new version of the algorithm (the one that uses Proposition 4.1) takes a step that is three times closer to the zero than that of the old version of the algorithm (the one that uses Proposition 3.2). This causes the convergence to be faster in the new version than in the old, and theoretically, it can be an improvement of the Kneser Algorithm when implemented.

5 Conclusion

Through Constructivism, we have reproduced and analyzed the construction of the real numbers through Cauchy sequences followed by a reproduction and analysis of the Kneser Algorithm. As we recall, we started from the natural numbers and then defined the rationals. After this, we constructed the field of Cauchy sequences which, when divided into equivalence classes, gives us a way to constructively define the reals. Moreover, we introduced the very important and characteristic notions of order and apartness that allow us to compare real numbers, since equality between real numbers is not decidable in Constructivism. We then continued with the axiomatization of the real numbers in the proof assistant Coq. First, we axiomatize the structures such as Constructive Set, Constructive Ring with Apartness and an Ordered Field with an Apartness relation and an order. Second, we move on to defining and axiomatizing the rationals with a variant on the usual way of defining the rationals just as pairs of integers to avoid the denominator being 0. Finally, we showed that the field of Cauchy sequences forms a real number structure.

For further research, it would be useful to analyze the implementation of the algorithm with the variant in th previous chapter. This has been done superficially in [3] but a thorough analysis of the convergence behavior of the algorithm would be something useful in order to improve its use. Another possible topic of research would be to compare the Kneser Algorithm with other root finding algorithms such as the Newton method, Secant Method and other algorithms used for the root finding of polynomials. This can be extended treating different examples and showing when each algorithm runs into trouble depending on which situations.

It is important to remind ourselves once again of the usefulness of having algorithms such as the Kneser Algorithm which serve as constructive proofs for the Fundamental Theorem of Algebra. These algorithms serve as a tool to construct solutions of theorems we have proven but have no proper way of constructing a solution. Through implementing and constantly improving these algorithms we can arrive to better solutions and constructions that can be used outside of the context of Constructivism.

References

[1] A. S. Troelstra and D. van Dalen, *Constructivism in Mathematics: An Introduction.* Elsevier, 1988.

[2] A. S. Troelstra and D. van Dalen, *Choice sequences : a chapter of intuitionistic mathematics.* Clarendon Press Oxford [Eng.], 1977.

[3] H. Geuvers, F. Wiedijk, and J. Zwanenburg, "A constructive proof of the fundamental theorem of algebra without using the rationals," in *Selected Papers from the International Workshop on Types for Proofs and Programs*, TYPES '00, (Berlin, Heidelberg), pp. 96–111, Springer-Verlag, 2002.

[4] E. Bishop, *Foundations of Constructive Analysis.* Mcgraw-Hill, 1967.

[5] H. Geuvers and M. Niqui, "Constructive reals in coq: Axioms and categoricity," in *Selected Papers from the International Workshop on Types for Proofs and Programs*, TYPES '00, (Berlin, Heidelberg), pp. 79–95, Springer-Verlag, 2002.

[6] M. Kneser, "Ergänzung zu einer arbeit von hellmuth kneser über den fundamentalsatz der algebra," *Mathematische Zeitschrift*, vol. 177, pp. 285–288, 1981.

[7] H. Kneser, "Der fundamentalsatz der algebra und der intuitionismus," *Mathematische Zeitschrift*, vol. 46, pp. 287–302, 1940.

Appendix A Coq Codes

To axiomatize a constructive set C with apartness $\#$ and equality $=$ we have the following Coq code:

```
Record Csetoid      : Type :=
{ C                 :> Set;
  [=]               : C->C->Prop;
  [#]               : C->C->Prop;
  ap_irr            : (x:C)~(x [#] x);
  ap_sym            : (x,y:C) (x [#] y) -> (y [#] x);
  ap_cot            : (x,y:C) (x [#] y) -> (z:C)(x [#] z)\/(z [#] y);
  ap_tight          : (x,y:C)~(x [#] y)  <-> (x [#] y)                    }.
```

To axiomatize a constructive commutative ring R with operations $+$ and $*$ and relations of apartness $\#$ and equality $=$ we have the following Coq code:

```
Record CRing        : Type :=
{ R                 :> CSetoid;
  zero              : R;
  [+]               : R->R->R;
  add_strext        : (x1,x2,y1,y2)((x1 [+] y1) [#] (x2 [+] y2)) ->
                                                  (x1 [#] x2)\/(y1 [#] y2);
  add_assoc         : (x,y,z:R)((x [+] (y [+] z)) [=] ((x [+] y) [+] z));
  add_unit          : (x:R)((x [+] zero) [=] x);
  add_commut        : (x,y:R)((x [+] y) [=] (y [+] x));

  [--]              : R->R;
  minus_strext      : (x,y:R)([--]x [#] [--]y) -> (x [#] y);
  minus_proof       : (x:R)([--]x [+] x) [=] zero);
  one               : R;
  [*]               : R->R->R;
  mult_strext       : (x1,x2,y1,y2)((x1 [*] y1) [*] (x2 [*] y2)) ->
                                                  (x1 [*] x2)\/(y1 [*] y2);
  mult_assoc        : (x,y,z:R)((x [*] (y [*] z)) [=] ((x [*] y) [*] z));
  mult_unit         : (x:R)((x [*] one) [=] x);
  mult_commut       : (x,y:R)((x [*] y) [=] (y [*] x));
  dist              : (x,y,z:R) ((x [*] (y [+] z)) [=]
                                          ((x [*] y) [+] (x [*] z)));
  non_triv          : (one [#] zero)
```

The subset S that contains all of the elements for which a function `Prop` is applicable in C is axiomatized in Coq through the following code:

```
Record subsetoid [S : CSetoid; P : S -> Prop] : Set :=
  { elem            :> S;
    prf             : (P elem)                                          }.
```

To axiomatize the inverses in F we have the following Coq code:

```
Record CField       : Type :=
{ F                 :> CRing;
  rcpcl             : (NonZeros F) -> (NonZeros F)
  rcpcl_strext      : (x,y:(NonZeros F))((rcpcl x) [#] (rcpcl y)) ->
                                                        (x [#] y);
  rcpcl_proof       : (x:(NonZeros F))
                          ((nzinj x) [*] (nzinj (rcpcl x )) [=] one)}.
```

Remark. The function `nzinj : (NonZeros F) -> F` maps a non-zero element of R to the same element in F. It is just a projection of `NonZeros F` onto F.

To define the linear order $<$ we have the following code in Coq:

```
Record COrdField  : Type :=
{ OF              :> CField
  [<]             : OF->OF->Prop
  less_strext     : (x1,x2,y1,y2:OF) (x1 [<] y1) ->
                                (x2 [<] y2)\/(x1 [#] x2)\/(y1 [#] y2);
  less_trans      : (x,y,z:OF)(x [<] y) -> (y [<] z) -> (x [<] z);
  less_irr        : (x:OF)~(x [<] x);
  less_asym       : (x,y:OF)(x [<] y) -> ~(y [<] y);
  add_resp_less   : (x,y:OF)(x [<] y) ->
                                        (z:OF)((x [+] z) [<] (y [+] z));
  times_resp_pos  : (x,y:OF)(zero [<] x) -> (zero [<] y)->
                                                (zero [<] (x [*] y));
  less_conf_ap    : (x,y:F)(x [#] y) <-> ((x [<] y)\/(y [<] x)        }.
```

Introduce the function $|\cdot|$ on F through the following code:

```
AbsSmall [e,x:F]  : Prop := ([--]e [<] x) /\ (x [<] e).
```

Introduce the Cauchy condition on F through the following code:

```
Definition cauchy [g:nat->F]: Prop :=
  (e:F)(zero [<] e) ->
    (EX N:nat | (m:nat)(le N m) -> (AbsSmall e ((g m)[-](g N)))       ).
```

Introduce the function `lim` through the following code:

```
Record CReals     : Type :=
{IR               :> CField;
lim               : (s:nat->IR)(cauchy s)->IR;
lim_proof         : (s:nat->F)(c:(cauchy s))
                      (e:F)(zero [<] e) ->
                        (EX N:nat | (m:nat)(le n m) ->
                                      (AbsSmall e (s m)[-](lim s c)));
arch_proof        : (x:F)(EX n:nat | (x [<] (nreal n)))              }.
```