A Constructive Proof of the Fundamental Theorem of Algebra without using the Rationals

Herman Geuvers, Freek Wiedijk, Jan Zwanenburg
{herman,freek,janz}@cs.kun.nl

Department of Computer Science, University of Nijmegen, the Netherlands

Abstract. In the FTA project in Nijmegen we have formalized a constructive proof of the Fundamental Theorem of Algebra. In the formalization, we have first defined the (constructive) algebraic hierarchy of groups, rings, fields, etcetera. For the reals we have then defined the notion of *real number structure*, which is basically a Cauchy complete Archimedean ordered field. This boils down to axiomatizing the constructive reals. The proof of FTA is then given from these axioms (so independent of a specific construction of the reals), where the complex numbers are defined as pairs of real numbers.
The proof of FTA that we have chosen to formalize is the one in the seminal book by Troelstra and van Dalen [17], originally due to Manfred Kneser [12]. The proof by Troelstra and van Dalen makes heavy use of the rational numbers (as suitable approximations of reals), which is quite common in constructive analysis, because equality on the rationals is decidable and equality on the reals isn't. In our case, this is not so convenient, because the axiomatization of the reals doesn't 'contain' the rationals. Moreover, we found it rather unnatural to let a proof about the reals be mainly dealing with rationals. Therefore, our version of the FTA proof doesn't refer to the rational numbers. The proof described here is a faithful presentation of a fully formalized proof in the Coq system.

1 Introduction

The Fundamental Theorem of Algebra states that the field of complex numbers is algebraically closed. More explicitly, it says that

For every non-constant polynomial

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

with coefficients in $\mathbb{C}$*, the equation* $f(z) = 0$ *has a solution.*

This theorem has a long and illustrious history (see [6] or [11] for an overview). It was proved for the first time in Gauss's Ph.D. thesis from 1799. Many proofs of the Fundamental Theorem of Algebra are known, most of which have a constructive version.

The proof that we're presenting here was invented by Manfred Kneser [12] (inspired by a proof of his father, Hellmuth Kneser, in [11]), and is a constructive

version of the simple proof that derives a contradiction from the assumption that the (non-constant) polynomial f is minimal at z_0 with $|f(z_0)| \neq 0$. We briefly repeat the classical proof here. Let $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ be a non-constant polynomial.

First note that $|f(z)|$ must have a minimum somewhere, because $|f(z)| \to \infty$ if $|z| \to \infty$. We may assume the minimum to be reached for $z = 0$. (If the minimum is reached for z_0, consider the polynomial $g(z) = f(z + z_0)$.) Now, assume the minimum of $|f(z)|$ is not 0 (i.e. $f(0) \neq 0$). The function $f(z)$ has the form

$$f(z) = a_0 + a_k z^k + O\left(z^{k+1}\right)$$

with $a_k \neq 0$. Because of this, $f(0) = a_0 \neq 0$ and we can take

$$z = \epsilon \sqrt[k]{-\frac{a_0}{a_k}}$$

with $\epsilon \in \mathbb{R}_{>0}$, and if ϵ is small enough, the part $O\left(z^{k+1}\right)$ will be negligible compared to the rest, and we get a $z \neq 0$ for which

$$\begin{aligned} |f(z)| &= a_0 + a_k (\epsilon \sqrt[k]{-\frac{a_0}{a_k}})^k \\ &= a_0(1 - \epsilon^k) \\ &< |f(0)| \end{aligned}$$

So $|f(0)|$ is not the minimum and we have derived a contradiction.

By iterating this idea, one can try to construct a Cauchy sequence to a zero of the polynomial. The main difficulty with this approach is that we have two conflicting requirements for the choice of ϵ:

- if ϵ is chosen too small each time, we may not reach the zero in countably many steps (we will go down, but might not go down all the way to zero).
- if ϵ is not small enough, we are not allowed to ignore the $O\left(z^{k+1}\right)$ part.

The solution to this is that, instead of using the above representation (in which the term $a_k z^k$ is the *smallest* power with a non-zero coefficient), in the constructive proof one just takes *some* appropriate k (not necessarily the smallest) and writes $f(z)$ as

$$f(z) = a_0 + a_k (z - z_0)^k + \textit{the other terms}$$

That way one can make sure that not only $|f(z)| < |f(0)|$, but in fact $|f(z)| < q\,|f(0)|$ for some fixed $q < 1$.

The FTA proof along these lines presented by Manfred Kneser in [12] is classical ('to improve readability'), but it is stated that it can be made constructive without any serious problems. In [17], a constructive version of this proof is given, using rational approximations to overcome the undecidability of equality on the reals. Another constructive version of the Kneser proof is presented by Schwichtenberg in [15], also using rational approximations, but along different lines. The constructive version of FTA reads as follows.

For every polynomial

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

with coefficients in $\mathbb{C}$*, such that* $a_k \# 0$ *for some* $k > 0$*, the equation* $f(z) = 0$ *has a solution.*

As the equality on $\mathbb{R}$ (and therefore on $\mathbb{C}$) is not decidable (we don't have $\forall x, y \in \mathbb{R}(x = y \vee x \neq y)$) we can't just write $f(z)$ as $a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ with $a_n \neq 0$. Therefore, in constructive analysis, one works with the notion of apartness, usually denoted by $\#$, which is a 'positive inequality': $a \# b$ if we positively know them to be distinct, i.e. we know a distance ϵ between them. Now, one can constructively find a root of f if we positively know some coefficient a_k $(k > 0)$ to be distinct from 0. The proof of constructive FTA proceeds by first proving it for *monic* polynomials (i.e. where $a_n = 1$).

The original Kneser proof of FTA for monic polynomials makes use of an approximation of the polynomial with coefficients in $\mathbb{Q}$, because it needs to compare the size of various expressions (which is not decidable in $\mathbb{R}$). We found this unsatisfactory: the rational numbers don't seem to have anything to do with the Fundamental Theorem of Algebra! Also, in our Coq formalization of Kneser's proof, we introduced the real numbers axiomatically (so *a priori* we didn't have $\mathbb{Q}$ in our formalization), and it seemed silly to reconstruct the rational numbers inside our real numbers just to be able to formalize this proof. Therefore, instead of constructing $\mathbb{Q}$, we modified the proof so that it no longer referred to the rationals. The result is presented here.

The main idea behind the modification of the proof is that we introduce 'fuzziness' in the comparisons. The proof will contains a 'fuzziness parameter' ϵ Instead of having to decide whether

$$x < y \vee x = y \vee x > y,$$

all we need to establish is whether

$$x < y + \epsilon \vee x > y - \epsilon$$

(which we might write as

$$x \leq_\epsilon y \vee x \geq_\epsilon y$$

using a relation $\leq_\epsilon$). Constructively we have *cotransitivity* of the order relation

$$x < y \Rightarrow x < z \vee z < y$$

from which it follows that the disjunction with the ϵ's is decidable.

Apart from not needing $\mathbb{Q}$, another difference between the proof presented here and the proof in [17] is that we have avoided using Vandermonde determinants. In the original proof, this is used to prove FTA from FTA for monic polynomials. We prove this implication directly, using some polynomial arithmetic. Therefore there's no use of linear algebra in the proof anymore.

We have formalized the proof presented here using the Coq system: this was known as the FTA project [7]. In the formalization, we treat the real numbers axiomatically. More precisely, the reals form a part of a *constructive algebraic hierarchy*, which consists (among other things) of the abstract notions of rings, fields and ordered fields. See [8] for details. The base level of this hierarchy consists of the notion of *constructive setoid*, which is basically a pair of a type and an *apartness* relation over the type. (For constructive reals, 'being apart' is more basic then 'being equal', so we start from apartness.) In this hierarchy, a *real number structure* is defined as a Cauchy complete Archimedean ordered field. In the FTA project, the Fundamental Theorem of Algebra was proven for any real number structure, so as a matter of fact the theorem was proven from the axioms for the constructive reals. Also it was shown that real number structures exist by actually constructing one. Details on this construction can be found in [9], where also other axiomatizations are discussed and it is shown that any two real number structures are isomorphic.

The whole formalization turned out to be 930K of Coq source code, which includes the construction of the real numbers by Milad Niqui, see [9]. The parts that directly correspond to the mathematics in this paper is about 65K of Coq source. The final lemma that was proved in the formalization was, in Coq syntax:

```
(f:(cpoly_cring CC))(nonConst ? f) -> (EX z | f!z [=] Zero)
```

The plan of the paper is as follows: for an overview we first present the root-finding algorithm that's implicit in Kneser's proof (for simplicity we give the classical version of that algorithm). After that we give the full constructive Kneser proof, which contains a correctness proof of the algorithm.

2 The Kneser Algorithm, Classically

Let

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

be a monic polynomial over the complex numbers of degree $n > 0$. Let be given an arbitrary complex number z_0. We are going to describe an algorithm that computes a Cauchy sequence

$$z_0, z_1, z_2, \ldots$$

that converges to a zero of this polynomial.

Suppose that z_i has already been established. From this we have to determine the next term in the sequence, z_{i+1}. There are two possibilities:

- In the case that $f(z_i) = 0$ we already are at a zero, and so we will take $z_{i+1} = z_i$.
- In the case that $f(z_i) \neq 0$ we consider the polynomial f_{z_i}, defined by[1] $f_{z_i}(z) \equiv f(z + z_i)$, find an appropriate offset δ_i and then take $z_{i+1} = z_i + \delta_i$.

[1] The shift from f to f_{z_i} corresponds to the step in the classical FTA proof (see Section 1) where the polynomial is shifted so that the alleged minimum is reached in 0

So in the second case we have the polynomial

$$f_{z_i}(z) = b_n z^n + b_{n-1} z^{n-1} + \ldots + b_1 z + b_0$$

(the coefficients b_k really depend on z_i, but we won't write this dependency to keep the formulas simple), with $b_n = 1$ and $b_0 = f_{z_i}(0) = f(z_i) \neq 0$, and we have to determine δ_i.

First, we will determine $|\delta_i|$. Define

$$r_0 = \min_{k \in \{1,\ldots,n\}, b_k \neq 0} \sqrt[k]{|b_0|/|b_k|}$$

and from this define a sequence of radii

$$r_0 > r_1 > r_2 > \ldots$$

by

$$r_j = 3^{-j} r_0$$

(so every radius is $\frac{1}{3}$ of the previous one).

Now for each j let k_j be the element of $\{1, \ldots, n\}$ such that

$$\left|b_{k_j}\right| {r_j}^{k_j}$$

is maximal (if there are more elements of $\{1, \ldots, n\}$ for which the maximum is attained, then take the least one). This will give a decreasing sequence[2]

$$k_0 \geq k_1 \geq k_2 \geq \ldots$$

Take the least $j > 0$ for which

$$k_{j-1} = k_j = k_{j+1}$$

and let $r = r_j$ and $k = k_j$. We will define δ_i such that $|\delta_i| = r$, and such that $b_k {\delta_i}^k$ points opposite to b_0 in the complex plane. This means that we take

$$\delta_i = r \sqrt[k]{-\frac{b_0/b_k}{|b_0/b_k|}}$$

and $z_{i+1} = z_i + \delta_i$. This concludes the description of the classical version of the Kneser algorithm.

Note that this last step introduces ambiguity, because there are k different complex roots. So the sequence

$$z_0, z_1, z_2, \ldots$$

[2] That this sequence is decreasing is seen by the following argument: if $\left|b_{k_j}\right| {r_j}^{k_j}$ is the maximum among $\{|b_1| {r_j}, \ldots, |b_n| {r_j}^n\}$, then $\left|b_{k_j}\right| {r_{j+1}}^{k_j} > |b_i| {r_{j+1}}^i$ for all $i > k_j$, because $|b_i| {r_{j+1}}^i = \frac{1}{3^i} |b_i| {r_j}^i \leq \frac{1}{3^i} \left|b_{k_j}\right| {r_j}^{k_j} < \frac{1}{3^{k_j}} \left|b_{k_j}\right| {r_j}^{k_j} = \left|b_{k_j}\right| {r_{j+1}}^{k_j}$.

really is a path in an infinite tree which this algorithm computes. Of course, following different paths in this tree one might find different zeroes.

The correctness of the algorithm is a consequence of the following properties of the choice for δ_i (and r). (These properties and the correctness will be proved in detail in the next Section.)

$$\begin{aligned} |f_{z_i}(\delta_i)| &< q\,|f_{z_i}(0)| \text{ for some fixed } q < 1, \\ r^n &< |f_{z_i}(0)|\,. \end{aligned}$$

The first inequality says that $|f(z_{i+1})| < q\,|f(z_i)|$, so the f-values of the sequence $z_0, z_1, z_2, \ldots$ converge to 0. The second inequality says that $|z_{i+1} - z_i|^n = |\delta_i|^n = r^n < |f(z_i)|$, so the sequence $z_0, z_1, z_2, \ldots$ converges.

3 The Kneser Proof, Constructively

We will now present our variation on Kneser's proof of the Fundamental Theorem of Algebra. This variant of the proof doesn't make use of $\mathbb{Q}$, unlike the proof from [17] that it was based on. In the proof we have isolated the parts that are about the reals and the parts that really need the complex numbers.

The only essential property of the complex numbers that is used is the existence of k-th roots, which can be proved independently of FTA. The most well-known proof of this fact proceeds by first moving to a polar coordinate representation of $\mathbb{C}$. As we have chosen $\mathbb{R}^2$ as a representation of $\mathbb{C}$, this is not an easy proof to formalize. (One would first have to define the arctan function and establish an isomorphism between the two representations.) Therefore we have chosen a different proof, which appears e.g. in [5], and [13] and is basically constructive. Here, the existence of k-th roots in $\mathbb{C}$ is derived directly from the existence of square roots in $\mathbb{C}$ and the fact that all polynomials over $\mathbb{R}$ of odd degree have a root. The proof of these properties have all been completely formalized in Coq. Note here that the intermediate value theorem (which implies directly that all polynomials over $\mathbb{R}$ of odd degree have a root) is not valid constructively. However, the intermediate value theorem can be proved for polynomials. (In our formalization we have followed the proof of [17], using Lemma 6 for a substantial shortcut.)

The proof of FTA goes through three lemmas, which in the Coq formalization have been called 'the Key Lemma', 'the Main Lemma' and 'the Kneser Lemma'. The presentation that we give here directly corresponds to the way it was formalized in Coq.

We first state an auxiliary lemma, that says that constructively it's possible to find the maximum of a sequence of numbers 'up to ϵ':

Lemma 1. *For $n > 0$, $\epsilon > 0$ and $c_1, \ldots, c_n \in \mathbb{R}$, there is a k such that for all $i \in \{1, \ldots, n\}$:*

$$c_k > c_i - \epsilon$$

The proof is a straightforward induction using the cotransitivity of the $<$ relation: to determine the 'maximum up to ϵ' of $c_1, \ldots, c_{n+1}$, first determine (induction hypothesis) the 'maximum up to $\epsilon/2$' of $c_1, \ldots, c_n$, say c_k and then choose c_k if $c_{n+1} < c_k + \epsilon$ and c_{n+1} if $c_{n+1} > c_k - \epsilon/2$. The latter choice can be made because of cotransitivity of $<$.

We now state the Key Lemma:

Lemma 2 (Key Lemma). *For every $n > 0$, $\epsilon > 0$ and $a_0 > \epsilon$, $a_1 \ldots, a_{n-1} \geq 0$, $a_n = 1$, there exist $r_0 > 0$ and $k_j \in \{1, \ldots, n\}$ with $k_0 \geq k_1 \geq k_2 \geq \ldots$ such that*

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

and for all $j \in \mathbb{N}$, if we define $r_j = 3^{-j} r_0$, for all $i \in \{1, \ldots, n\}$ it holds that

$$a_{k_j} {r_j}^{k_j} > a_i {r_j}^i - \epsilon$$

This lemma corresponds directly to the part of the algorithm from the previous section that establishes r_0 and the sequence $k_0 \geq k_1 \geq k_2 \geq \ldots$ (what is called $|b_i|$ there, is called a_i here, because that way the Key Lemma doesn't need to refer to complex numbers). The choice for r_0 in the classical situation as $r_0 = \min_{k \in \{1,\ldots,n\}, b_k \neq 0} \sqrt[k]{|b_0|/|b_k|}$ is is here represented by choosing r_0 such that $|b_0| = \max_{k \in \{1,\ldots,n\}} |b_k| r_0^k$.

The real difference with the classical situation is that 'taking the maximum' during the selection of the k_j is just 'up to ϵ': a term $a_i {r_j}^i$ different from $a_{k_j} {r_j}^{k_j}$ may actually be the biggest, but it may not exceed the selected one by more than ϵ.

We will now prove the Key Lemma:

Proof. We first select k_0 and r_0. This is done by taking initial values for k_0 and r_0 and then considering in turn for i the values $n-1$ down to 1, preserving the following invariant:

$$\begin{aligned} &a_{k_0} {r_0}^{k_0} = a_0 - \epsilon, \\ &a_{k_0} {r_0}^{k_0} > a_l {r_0}^l - \epsilon \text{ for all } l \in \{i, \ldots, n\}. \end{aligned}$$

Start with the initial values $k_0 = n$ and $r_0 = \sqrt[n]{a_0 - \epsilon}$. Then, at each i (from $n-1$ down to 1) we update the values of k_0 and r_0 as follows.

- If $a_i r_0^i < a_0$, do nothing. The invariant trivially remains to hold.
- If $a_i r_0^i > a_0 - \epsilon$, set k_0 to i and r_0 to $\sqrt[i]{(a_0 - \epsilon)/a_i}$ (in which case r_0 will decrease). The first part of the invariant trivially remains to hold. For the second part: $a_{k_0} {r_0}^{k_0} = a_0 - \epsilon$, which is larger than each of the $a_l {r_0}^l - \epsilon$ (by the invariant for the previous choice of i and the fact that r_0 has decreased).

After this, k_0 and r_0 have the appropriate values.

To get k_{j+1} from k_j, let $k = k_j$, $r = 3^{-j} r_0$ and apply Lemma 1 with $\epsilon/2$ to the sequence

$$a_1(r/3), a_2(r/3)^2, \ldots, a_k(r/3)^k$$

to get $k' = k_{j+1}$. (So $k_j \geq k_{j+1}$.) Then for $i \leq k$ the inequality $a_{k'}(r/3)^{k'} > a_i(r/3)^i - \epsilon$ follows directly, while for $i > k$ we have:

$$a_k(r/3)^k = 3^{-k}a_k r^k > 3^{-k}\left(a_i r^i - \epsilon\right) = 3^{-k}a_i r^i - 3^{-k}\epsilon > a_i(r/3)^i - \epsilon/2$$

and so:

$$a_{k'}(r/3)^{k'} > a_k(r/3)^k - \epsilon/2 > a_i(r/3)^i - \epsilon$$

□

We will now state and prove the Main Lemma, which isolates the part of the proof that's about the real numbers from the part that involves the complex numbers.

Lemma 3 (Main Lemma). *For every $n > 0$, $\epsilon > 0$, $a_0 > \epsilon$, $a_1 \ldots, a_{n-1} \geq 0$, $a_n = 1$, there exists an $r > 0$ and a $k \in \{1, \ldots, n\}$ that satisfy the inequalities*

$$\begin{aligned} r^n &< a_0 \\ 3^{-2n^2}a_0 - 2\epsilon < a_k r^k &< a_0 \end{aligned}$$

and have the property

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

The Main Lemma corresponds to the choice for r and k in the description of the classical algorithm. The first condition states that r cannot be too large in comparison to the previous value: this corresponds to the property $r^n < |f_{z_i}(0)|$, mentioned in the discussion of the classical algorithm. The second condition is to make sure that, if we let $b_k\delta_i^k$ point in the opposite direction of b_0, then $\left|b_0 + b_k\delta_i^k\right|$ gets sufficiently smaller. (The Main Lemma is about reals, but it will be applied by taking $a_i = |b_i|$, where the b_i are the coefficients of the polynomial.) Moreover, the second and the third condition together make sure that the sum of the remaining terms $a_i r^i$ is negligible.

We will now prove the Main Lemma.

Proof. Apply the Key Lemma to get sequences $k_0, k_1, k_2 \ldots$ and $r_0, r_1, r_2 \ldots$ Because the sequence k_j is non-increasing in the finite set $\{1, \ldots, n\}$ there exists a (smallest) $j < 2n$ with

$$k_{j-1} = k_j = k_{j+1}$$

Take $k = k_j$ and $r = r_j$.

Because $r = 3^{-j}r_0 \leq r_0$, for all i we have $a_i r^i \leq a_i {r_0}^i < a_{k_0}{r_0}^{k_0} + \epsilon = a_0$. Of this statement $r^n < a_0$ and $a_k r^k < a_0$ are special cases. From $a_{k_0}r^{k_0} = 3^{-jk_0}a_{k_0}{r_0}^{k_0} \geq 3^{-jn}a_{k_0}{r_0}^{k_0} = 3^{-jn}(a_0 - \epsilon) \geq 3^{-jn}a_0 - \epsilon$ it follows that $a_k r^k > a_{k_0}r^{k_0} - \epsilon \geq 3^{-jn}a_0 - 2\epsilon > 3^{-2n^2}a_0 - 2\epsilon$.

From $k = k_{j+1}$ we get that for all $i \in \{1, \ldots, n\}$

$$a_k(r/3)^k > a_i(r/3)^i - \epsilon$$

and from that it follows that

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

and therefore

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

In exactly the same way we get from $k = k_{j-1}$ that

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

and so

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

Together this gives

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

□

We now state and prove the 'Kneser Lemma'. This lemma states that we can find what was called δ_i in the previous Section: an appropriate vector that moves us sufficiently closer to a zero. In the classical version of the Kneser proof, one distinguishes cases according to $f(0) = 0$ or $f(0) \neq 0$. In the first case we are done, while in the second case one finds a $z \in \mathbb{C}$ such that

$$|z|^n < |f(0)|$$

and

$$|f(z)| < q\,|f(0)|$$

(where $q < 1$ is some fixed multiplication factor that only depends on the degree of the polynomial).

However, we don't know $f(0) = 0 \vee f(0) \neq 0$ constructively. Therefore, we here have a $c > 0$ that takes the role of $|f(0)|$. This c can get arbitrary close to $|f(0)|$ from above. Here is the constructive version of the Kneser Lemma:

Lemma 4 (Kneser Lemma). *For every $n > 0$ there is a q with $0 < q < 1$, such that for all monic polynomials $f(z)$ of degree n over the complex numbers, and for all $c > 0$ such that*

$$|f(0)| < c$$

there exists a $z \in \mathbb{C}$ *such that*

$$|z|^n < c$$

and

$$|f(z)| < qc$$

Proof. First of all, we give the factor q explicitly:

$$q = 1 - 3^{-2n^2-n}$$

We now show how to find z.

Write the polynomial $f(z)$ as

$$f(z) = b_n z^n + b_{n-1} z^{n-1} + \ldots + b_1 z + b_0$$

Because $f(z)$ is monic we have that $b_n = 1$, Also, we have that $b_0 = f(0)$, so the condition about c states that $|b_0| < c$. As $qc > 0$ we can make the following case distinction

$$|f(0)| < qc \quad \vee \quad |f(0)| > 0.$$

In the first case we are done by taking $z := 0$. In the second case we proceed as follows. Define $a_i = |b_i|$ for $i \in \{0, \ldots, n\}$ and choose an $\epsilon > 0$ such that

$$2\epsilon < 3^{-2n^2} a_0 \tag{1}$$

$$(3^n + 1)\epsilon < q(c - a_0) \tag{2}$$

Then $\epsilon < a_0$ and we apply the Main Lemma (Lemma 3) to $a_0, \ldots, a_n$ to obtain $r > 0$ and $k \in \{1, \ldots, n\}$ satisfying

$$r^n < a_0$$
$$3^{-2n^2} a_0 - 2\epsilon < a_k r^k < a_0$$
$$\textstyle\sum_{i=1}^{k-1} a_i r^i + \sum_{i=k+1}^{n} a_i r^i < (1 - 3^{-n}) a_k r^k + 3^n \epsilon$$

Finally take

$$z = r \sqrt[k]{-\frac{b_0/b_k}{a_0/a_k}}$$

(This makes use of inequality (1) $2\epsilon < 3^{-2n^2} a_0$, because we need to know that $a_k > 0$.) Then because $|b_0| = a_0$ and $|b_k| = a_k$ we have

$$|z| = r$$

From this, we get

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

For the second property of z we start by computing $|b_0 + b_k z^k|$:

$$\begin{aligned} |b_0 + b_k z^k| &= \Big| b_0 + b_k r^k \Big(-\frac{b_0/b_k}{a_0/a_k} \Big) \Big| \\ &= \Big| \frac{b_0}{a_0} (a_0 - a_k r^k) \Big| \\ &= |a_0 - a_k r^k| \\ &= a_0 - a_k r^k \end{aligned}$$

(Using the inequality $a_k r^k < a_0$.)

By the triangle inequality for the complex numbers, we then get

$$\begin{aligned}
\Big|\sum_{i=0}^{n} b_i z^i\Big| &\le \big|b_0 + b_k z^k\big| + \sum_{i=1}^{k-1} a_i r^i + \sum_{i=k+1}^{n} a_i r^i \\
&< a_0 - a_k r^k + (1 - 3^{-n}) a_k r^k + 3^n \epsilon \\
&= a_0 - 3^{-n} a_k r^k + 3^n \epsilon \\
&< a_0 - 3^{-n}(3^{-2n^2} a_0 - 2\epsilon) + 3^n \epsilon \\
&= (1 - 3^{-2n^2 - n}) a_0 + 3^n \epsilon + 3^{-n} 2\epsilon \\
&< q a_0 + 3^n \epsilon + \epsilon \\
&< qc,
\end{aligned}$$

where the final inequality follows from (2) $(3^n + 1)\epsilon < q(c - a_0)$. □

Next we prove the special case of the Fundamental Theorem of Algebra for monic polynomials:

Lemma 5 (Fundamental Theorem of Algebra for monic polynomials). *For every monic polynomial $f(z)$ of degree $n > 0$ over the complex numbers, there exists $z \in \mathbb{C}$ such that $f(z) = 0$.*

Proof. Take any $c > 0$ with $c > |f(0)|$. We construct a sequence $z_i \in \mathbb{C}$ such that for all i

$$|f(z_i)| < q^i c \tag{3}$$
$$|z_{i+1} - z_i| < (q^i c)^{1/n} \tag{4}$$

where $q < 1$ is given by the Kneser Lemma 4. This sequence is constructed by iteratively applying the Kneser Lemma to $f_{z_i}(z) \equiv f(z + z_i)$ to find $z_{i+1} - z_i$. The required properties of z_i then follow directly from the properties in the Kneser Lemma, by induction on i.

Because of 4, the z_i form a Cauchy sequence:

$$\begin{aligned}
|z_{m+i} - z_m| &\le |z_{m+i} - z_{m+i-1}| + \ldots + |z_{m+1} - z_m| \\
&< (q^{(m+i-1)/n} + q^{(m+i-2)/n} + \ldots + q^{m/n}) c^{1/n} \\
&= \frac{q^{m/n} - q^{(m+i)/n}}{1 - q^{1/n}} c^{1/n} \\
&= q^{m/n} \frac{1 - q^{i/n}}{1 - q^{1/n}} c^{1/n} \\
&< q^{m/n} \frac{c^{1/n}}{1 - q^{1/n}}.
\end{aligned}$$

By choosing m sufficiently large (n is fixed), this last expression can be made arbitrarily small.

Then, because z_i is a Cauchy sequence, the limit $z = \lim_{i\to\infty} z_i$ exists and by continuity of f one has

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

so $f(z) = 0$. □

Finally we prove the full Fundamental Theorem of Algebra. A polynomial is called *non-constant* if for some $k > 0$ one of its coefficients a_k is apart from zero. We denote this by $f \# 0$. This a_k doesn't necessarily need to be the head coefficient a_n of the polynomial. In fact the head coefficient a_n might be zero (we can't know this), so proving the full Fundamental Theorem of Algebra is not as easy as just dividing by a_n and then applying Lemma 5.

We need one more important property stating, in a sense, the opposite of the Fundamental Theorem of Algebra: instead of showing that there is an argument for which the polynomial is zero, it shows that there is an argument for which the polynomial is *apart* from zero. This fact comes as an immediate corollary of the following lemma.

Lemma 6. *Given a polynomial f of degree at most n and $n+1$ distinct points $z_0, z_1, \ldots, z_n \in \mathbb{C}$, $f(z_i) \# 0$ for at least one of the z_i.*

Proof. Write $f(z)$ in the form

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

which means that $f(z)$ has at most degree n. Then for any $n+1$ different $z_0, z_1, \ldots, z_n \in \mathbb{C}$ one can write

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

because both sides have at most degree n, and coincide on $n+1$ points (and hence they are equal). This means that we can write $f(z)$ in the form

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

for some $n+1$ polynomials f_i. Because this sum is $\# 0$, there is some $i \in \{0, \ldots, n\}$ for which the polynomial $f(z_i) f_i \# 0$ and therefore for this i we have that $f(z_i) \# 0$. □

Corollary 1. *For every polynomial $f \# 0$ over the complex numbers, there exists $z \in \mathbb{C}$ such that $f(z) \# 0$.*

Theorem 1 (Fundamental Theorem of Algebra). *For every non-constant polynomial $f(z)$ over the complex numbers, there exists $z \in \mathbb{C}$ such that $f(z) = 0$.*

Proof. We write

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

Because a_n might be zero, we call n the *length* of f instead of calling it the degree of f. We'll prove the theorem with induction on this length n.

With Corollary 1 find a $z_0 \in \mathbb{C}$ such that $f(z_0) \# 0$. Then if we define $f_{z_0}(z) \equiv f(z + z_0)$, it is sufficient to find a zero of f_{z_0}, because if z is a zero of f_{z_0} then $z + z_0$ will be a zero of f. So all we need to prove is that f_{z_0} has a zero.

We write

$$f_{z_0}(z) = b_n z^n + b_{n-1} z^{n-1} + \ldots + b_1 z + b_0$$

with $b_0 = f_{z_0}(0) = f(z_0) \# 0$. We define the *reverse* ${f_{z_0}}^{rev}(z)$ of this polynomial to be the polynomial

$$b_0 z^n + b_1 z^{n-1} + \ldots + b_{n-1} z + b_n$$

so with the coefficients in the opposite order. This reverse operation has the property that the reversal of a product is the product of the reversals: $(gh)^{rev} = g^{rev} h^{rev}$.

Now ${f_{z_0}}^{rev}(z)/b_0$ is monic, so by Lemma 5 it has a zero c, and so it can be written as $(z - c)g(z)$. Because, as we noted, reversals commute with products, this implies that the original f_{z_0} can be written as

$$f_{z_0}(z) = (c_1 z + c_0) h(z)$$

where $h(z)$ is a lower length polynomial of the form

$$h(z) = d_{n-1} z^{n-1} + \ldots + d_1 z + d_0$$

Because f_{z_0} is non-constant, we have $b_i \# 0$ for some $i > 0$. And because

$$b_i = c_0 d_i + c_1 d_{i-1}$$

we find that either $c_0 d_i \# 0$ or $c_1 d_{i-1} \# 0$.

- In the case that $c_0 d_i \# 0$, we get $d_i \# 0$ and therefore $h(z)$ is non-constant, has a zero by induction, and this zero will also be a zero of f_{z_0}.
- In the case that $c_1 d_{i-1} \# 0$, we get $c_1 \# 0$ and then $-c_0/c_1$ will be a zero of f_{z_0}.

□

4 Convergence Speed of the Kneser Algorithm

The Kneser proof (and the algorithm that is implicit in it) as presented in this paper differs from the Kneser proof from [17] in an important respect. In this paper we define the sequence

$$r_0 > r_1 > r_2 > \ldots$$

(and the matching sequence $k_0 \geq k_1 \geq k_2 \geq \ldots$) to start at zero. In [17] the r_j sequence starts at minus one

$$r_{-1} > r_0 > r_1 > r_2 > \ldots$$

Each r_j is three times as small as the previous one, so in the other variant of the proof the search for an appropriate r starts at a radius that is three times as big as the radius r_0. To distinguish the two proofs we'll call the proof that is in this paper the *slow* variant of the proof and the one where the sequences r_j and k_j start at -1 the *fast* variant of the proof.

In Coq we formalized the slow variant of the proof. It is a simpler proof and we wanted to finish the formalization as fast as possible. Also in Coq it's easier to formalize a sequence starting at 0 than a sequence starting at -1. (One could shift the sequence by one but that would complicate the formulas in various places.)

The fast variant of the proof has the advantage that the corresponding algorithm behaves like Newton-Raphson when the algorithm gets close to the zero of the polynomial. The algorithm from the slow variant of the proof converges slower, because close to a zero it only takes one third of a Newton-Raphson step. In the slow variant of the proof, close to a zero we get $k_0 = k_1 = k_2 = \ldots = 1$, which means that $j = 1$ and so $r = r_1 = \frac{1}{3}r_0$, where r_0 is the Newton-Raphson distance. Note that close to the zero, the value of the polynomial will then be multiplied with approximately a factor of $2/3$ at each step, which is much better than the 'worst case' factor of $q = 1 - 3^{-2n^2-n}$ which appears in the proof. As an example of the behavior of the algorithm from the slow variant of the proof we calculate $\sqrt{2} \approx 1.41421$ by finding a root of $z^2 - 2$, starting from $z_0 = 1$:

$$\begin{array}{lcl}
z_0 = & 1 & = 1 \\
z_1 = & 7/6 & \approx 1.16667 \\
z_2 = & 317/252 & \approx 1.25794 \\
z_3 = & 629453/479304 & \approx 1.31326 \\
z_4 = & 2440520044877/1810196044272 & \approx 1.34821 \\
z_5 = & \ldots & \approx 1.37075 \\
z_6 = & \ldots & \approx 1.38547
\end{array}$$

In this sequence the Kneser algorithm takes $\log(1/10)/\log(2/3) \approx 5.7$ steps to gain one decimal of precision.

In the fast variant of the proof we get, close to a zero $k_{-1} = k_0 = k_1 = k_2 = \ldots = 1$, which means that then $j = 0$ and so $r = r_0$. In the case of $\sqrt{2}$ this gives

$$\begin{array}{lcl}
z_0 = & 1 & = 1 \\
z_1 = & 3/2 & \approx 1.5 \\
z_2 = & 17/12 & \approx 1.41666666666666666666666667 \\
z_3 = & 577/408 & \approx 1.41421568627450980392156686 \\
z_4 = & 665857/470832 & \approx 1.41421356237468991062629560 \\
z_5 = & 886731088897/627013566048 & \approx 1.41421356237309504880168960 \\
z_6 = & \ldots & \approx 1.41421356237309504880168870
\end{array}$$

This is the same sequence that the Newton-Raphson algorithm calculates. This particular sequence consists of continued fraction approximations of $\sqrt{2}$ and

the correct number of decimals doubles with every step. Note that the Kneser algorithm of the fast variant of the proof only coincides with Newton-Raphson close to the zero. With Newton-Raphson not all start values lead to a convergent sequence, but with the Kneser algorithm it does.

To change the proof in this paper to the fast variant (where the sequences r_j and k_j start at -1), only the proof of the Key Lemma needs to be modified. Apart from going from k_j to k_{j+1} we will also need to go from k_0 to k_{-1}. To be able to do that, the k_0 and r_0 will need to satisfy a stricter restriction than before. It needs to satisfy

$$a_{k_0} r_0^{k_0} > a_i r_0^i - \epsilon'$$

where

$$\epsilon' = 3^{-n}\epsilon$$

To find such k_0 and r_0 one proceeds like before, but this time distinguishing between

$$a_i r_0^i < a_0 - \epsilon + \epsilon'$$

and

$$a_i r_0^i > a_0 - \epsilon$$

at every iteration. Then to get k_{-1} from k_0 one applies Lemma 1 to the sequence

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

with a reasoning similar to the k_{j+1} from k_j case.

5 Brief overview of other constructive proofs

The first constructive proof of FTA (for monic polynomials) is from Weyl [18], where the winding number is used to simultaneously find all zeros of a (monic) polynomial. A similar but more abstract proof, also using the winding number, occurs in [1], where FTA is proved for arbitrary non-constant polynomials. Based on Weyl's approach, [10] presents an implementation of an algorithm for the simultaneous determination of the zeros of a polynomial.

In [2], Brouwer and De Loor give a constructive proof of FTA for monic polynomials by first proving it for polynomials with rational complex coefficients (which have the advantage that equality is decidable) and then make the transition (viewing a complex number as the limit of a series of rational complex numbers) to general monic polynomials over $\mathbb{C}$. This proof – and also Weyl's and other FTA proofs – are discussed and compared in [14].

Brouwer [3] was the first to generalize the constructive FTA proof to arbitrary non-constant polynomials (where we just know *some* coefficient to be apart from 0). In [16] it is shown that, for general non-constant polynomials, there is a continuous map from the coefficients to the set of zeros.

Acknowledgements We thank the referees for their very valuable comments, which led us to improve part of the proof. We thank Henk Barendregt, Randy Pollack for inspiring discussions and their valuable comments. Thanks to Helmut Schwichtenberg for the enlightening and stimulating discussions on the FTA proof of Kneser and for providing us with a copy of [15]. We thank Bas Spitters and Wim Veldman for various discussions on the constructive aspects of analysis.

References

1. E. Bishop and D. Bridges, *Constructive Analysis*, Number 279 in Grundlehren der mathematischen Wissenschaften. Springer, 1985.
2. L.E.J. Brouwer and B. de Loor, Intuitionistischer Beweis des Fundamentalsatzes der Algebra, in *Proceedings of the KNAW*, 27, pp. 186–188, 1924.
3. L.E.J. Brouwer, Intuitionistische Ergänzung des Fundamentalsatzes der Algebra, in *Proceedings of the KNAW*, 27, pp. 631–634, 1924.
4. B. Dejon and P. Henrici, Editors, *Constructive Aspects of the Fundamental Theorem of Algebra*, Proceedings of a symposium at IBM Research Lab, Zürich-Rüschlikon, June 5-7, 1967, Wiley-Interscience, London.
5. H.-D. Ebbinghaus et al. (eds.), *Numbers*, Springer, 1991, 395 pp.
6. B. Fine and G. Rosenberger, *The Fundamental Theorem of Algebra*, Undergraduate Texts in Mathematics, Springer, 1997, xii+208 pp.
7. H. Geuvers, F. Wiedijk, J. Zwanenburg, R. Pollack, M. Niqui, H. Barendregt, FTA project, http://www.cs.kun.nl/gi/projects/fta/.
8. H. Geuvers, R. Pollack, F. Wiedijk, and J. Zwanenburg. The algebraic hierarchy of the FTA project, in *Calculemus 2001 workshop proceedings*, pp. 13–27, Siena, 2001.
9. H. Geuvers, M. Niqui, Constructive Reals in Coq: Axioms and Categoricity, *Types 2000 Workshop, Durham, UK*, this volume.
10. P. Henrici and I. Gargantini, Uniformly convergent algorithms for the simultaneous approximation of all zeros of a polynomial, in [4], pp. 77–113.
11. H. Kneser, Der Fundamentalsatz der Algebra und der Intuitionismus, *Math. Zeitschrift*, 46, 1940, pp. 287–302.
12. M. Kneser, Ergänzung zu einer Arbeit von Hellmuth Kneser über den Fundamentalsatz der Algebra, *Math. Zeitschrift*, 177, 1981, pp. 285–287.
13. J.E. Littlewood, Every polynomial has a root, *Journal of the London Math. Soc.* 16, 1941, pp. 95–98.
14. B. de Loor, *Die Hoofstelling van die Algebra van Intuïtionistiese standpunt*, Ph.D. Thesis, Univ. of Amsterdam, Netherlands, Feb. 1925, pp. 63 (South-African).
15. Helmut Schwichtenberg, Ein konstruktiver Beweis des Fundamentalsatzes, Appendix A (pp. 91–96) of Algebra, Lecture notes, Mathematisches Institut der Universität München 1998, http://www.mathematik.uni-muenchen.de/schwicht/lectures/algebra/ws98/skript.ps
16. E. Specker, The Fundamental Theorem of Algebra in Recursive Analysis, in [4], pp. 321–329.
17. A. Troelstra and D. van Dalen, *Constructivism in Mathematics*, vols. 121 and 123 in Studies in Logic and The Found. of Math., North-Holland, 1988.
18. H. Weyl, Randbemerkungen zu Hauptproblemen der Mathematik, *Math. Zeitschrift*, 20, 1924, pp. 131–150.