Sturm's Theorem: determining the number of zeroes of polynomials in an open interval.

Bachelor's thesis

Eric Spreen
University of Groningen
e.spreen@student.rug.nl

July 12, 2014

Supervisors:

Prof. Dr. J. Top
University of Groningen

Dr. R. Dyer
University of Groningen

rijksuniversiteit groningen
2014 | 400 jaar

Abstract

A review of the theory of polynomial rings and extension fields is presented, followed by an introduction on ordered, formally real, and real closed fields. This theory is then used to prove Sturm's Theorem, a classical result that enables one to find the number of roots of a polynomial that are contained within an open interval, simply by counting the number of sign changes in two sequences. This result can be extended to decide the existence of a root of a family of polynomials, by evaluating a set of polynomial equations, inequations and inequalities with integer coefficients.

Contents

Chapter 1

Introduction

In many of the natural sciences, polynomials and polynomial systems occur as useful approximations to real-world phenomena. As an example of this we give the harmonic oscillator, which is used in physics to approximate dynamical systems that are very close to an equilibrium point. The potential energy of such a (one-dimensional) system takes the form

$$V(x) = \frac{1}{2}kx^2,$$

which is a second-degree polynomial in one variable. A similar case occurs in higher-dimensional systems (in 3D, and with multiple bodies). Another example is the hydrogen atom in quantum mechanics, where the radial wave-functions takes on the form: [3]

$$R_{nl}(r) = \frac{1}{r}e^{-\rho}\rho^{l+1}v(\rho), \quad \rho = \frac{r}{an},$$

where $v(\rho)$ is a polynomial, and $n \in \mathbb{N}, n > 0$ and $l \in \mathbb{N}$.[1] It is a crucial problem to find the zeroes of these functions in order to determine the electronic structure of the atom, which can be done by finding the zeroes of the polynomial $\rho^{l+1}v(\rho)$.

It is clear from these examples that finding solutions of polynomial equations is a fundamental problem in applied mathematics. A classical result that enables us to do this numerically is Sturm's Theorem, named after Jacques Charles François Sturm. This theorem gives the number of zeroes of a polynomial that are contained within a certain open interval, enabling us to determine the zeroes (by partitioning the number line appropriately, up to machine precision) of a polynomial numerically.

We will discuss Sturm's Theorem in the context of real closed fields, an abstraction of the real number system that has significantly different realizations. The key to the success of Sturm's Theorem in real closed fields

[1] We use the convention that $0 \in \mathbb{N}$.

is the analog of the intermediate value theorem for polynomials. It can be shown that this result, and various other key theorems from real analysis hold for polynomials in real closed fields.

After the discussion of Sturm's Theorem, we will discuss an extension of Sturm's Theorem that allows us to simplify the problem of the existence of a zero in a certain interval for a whole family of polynomials. The result will be a finite set of systems of polynomial equations, inequations and inequalities with integer coefficients, any one of which may be satisfied by the parameters of the family for the resulting polynomial to have zero in the interval. From this we can quickly establish criteria for the existence of a zero of a whole family of polynomials. A secondary result is that if a polynomial with rational coefficients has a zero in one real closed field, it will have a zero in every other real closed field.

As a high school student I have often wondered whether it would be possible to form an equation of which the solvability is undecidable, in particular when I was unable to solve a particular problem. At the very end we will touch on this question.

A significant portion of this report follows [4] and [5]. If no citations have been provided, these are the sources. We will assume that the reader has a basic understanding of algebraic structures, such as monoids, groups and rings.

Chapter 2

Polynomials and Extensions

Before we can begin our study of real closed fields, we will develop the theory of polynomial rings over a field to some extent. This chapter will give basic results on arbitrary polynomial rings, and applications on extension rings and fields. Most of this chapter will follow [4].

We will say that a subring R of a ring S is generated by a set $A \subset S$, if R is the smallest subring that contains A. Also, if $u_1, \ldots, u_n \in S$ (and $\forall r \in R : u_i r = r u_i, 1 \leqslant i \leqslant n$), then we denote the ring that is generated by $R \cup \{ u_1, \ldots, u_n \}$ by $R[u_1, \ldots, u_n]$. We can readily note that $R[u_1, u_2] = (R[u_1])[u_2]$ by definition. The existance of such a subring follows from the observation that any arbitrary intersection of subrings of S is again a subring of S.

2.1 Polynomial rings

Definition 2.1.1. Given a ring R, its *polynomial ring* $R[x]$ is the ring of functions $f : \mathbb{N} \to R$ such that there exists a $k \in \mathbb{N}$ with $\forall n \in \mathbb{N} : n \geqslant k \implies f(n) = 0$. Addition and multiplication in $R[x]$ are defined as follows; for $f(x), g(x) \in R[x]$ and any $n \in \mathbb{N}$:

$$(f + g)(n) = f(n) + g(n), \qquad (fg)(n) = \sum_{i=0}^{n} f(i)g(n - i).$$

and 0 and 1 as obvious. The elements of $R[x]$ are called *polynomials* with coefficients in R, and the function values of a polynomial are called the *coefficients* of a polynomial.

We will establish the basic properties of polynomial rings. The proofs will be ommitted and can be found in [4, Sec.2.10].

Proposition 2.1.1 (Properties of polynomial rings)**.** *Let R be a ring and $R[x]$ its polynomial ring. Then:*

1. *There exists an injective homomorphism $R \to R[x]$, so that R may be regarded as a subring of $R[x]$.*

2. *Let $x \in R[x]$ be the polynomial with $x(1) = 1$ and $x(n) = 0$ if $n \in \mathbb{N} \setminus \{1\}$. Then $R[x]$ is generated by $R \cup \{x\}$. Furthermore, all elements of R commute with x.*

3. *For any $f(x) \in \mathbb{N}$, there exists an $n \in \mathbb{N}$ and unique $a_0, \ldots, a_n \in R$ such that $f(x) = \sum_{i=0}^{n} a_i x^i$.*

4. *If R is commutative, then so is $R[x]$.*

Proposition 2.1.2 (Evaluation homomorphism)**.** *If R and S are rings, $\phi : R \to S$ is a homomorphism, $u \in S$ and $\forall r \in R : \phi(r)u = u\phi(r)$, then there exists a unique homomorphism $\psi : R[x] \to S$ such that $\psi|_R = \phi$ and $\psi(x) = u$. Also, the kernel of ψ is an ideal $I \subseteq R[x]$ such that $I \cap R = \ker(\phi)$.*

This homomorphism is called the evaluation homomorphism *in u.*

Note: Evaluation in an overring

From the proposition above, it follows immediately that if we let R be a subring of S and ϕ the inclusion homomorphism, the kernel of every evaluation homomorphism in an element of S will be an ideal I of $R[x]$ with $I \cap R = \{0\}$.

We can note that if R is a ring, then the following property is "universal" for the polynomial ring $R[x]$ (in the sense that any rings that have this property are isomorphic): if S is any other ring, and $\phi : R \to S$ is a homomorphism, $u \in S$ and $\forall r \in R : \phi(r)u = u\phi(r)$, then there exists an $x \in R[x]$ and a unique homomorphism $\psi : R[x] \to S$ so that $\psi|_R = \phi$, $\phi(x) = u$ and $R[x]$ is generated by $R \cup \{x\}$. [4, p.124]

Note: Notation of polynomials

From now on, we will denote a polynomial with coefficients in a ring R as $f(x)$ and its value under a evaluation homomorphism in some u as $f(u)$. Also, if $f(u) = 0$, then u is called a *zero* of $f(x)$ in S.

Corollary 2.1.3. *If R and S are rings, and $\phi : R \to S$ is a homomorphism, then there exists a unique homomorphism $\psi : R[x] \to S[x']$ such that $\psi|_R = \phi$ and $\psi(x) = x'$.*

We will also use the notion of a polynomial in multiple indeterminates. We can formalize this notion by (for any $n \in \mathbb{N}$, $n > 1$) defining the ring $R[x_1, \ldots, x_n] := R[x_1] \ldots [x_n]$. By induction we can then get an evaluation homomorphism in multiple variables.

2.2 Degree arithmetic

We have seen that for any polynomial $0 \neq f(x) = \sum_{i=0}^{n} a_i x^i$ there is some $k \in \mathbb{N}$ such that $a_k \neq 0$, but $a_i = 0$ if $i > k$. This observation is a strong tool that we will use often in further arguments. We therefore define

Definition 2.2.1. If R is a ring and $0 \neq f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$, then the *degree* of $f(x)$ is the largest $k \in \mathbb{N}$ such that $a_k \neq 0$. If $f(x) = 0$, then the degree is $-\infty$. We will denote the degree of $f(x)$ by $\deg(f)$ or $\deg(f(x))$.

Furthermore, the *leading coefficient* of $f(x)$ is $a_{\deg(f)}$ if $f(x) \neq 0$ and 0 if $f(x) = 0$. This will be denoted by $\mathrm{lc}(f)$ or $\mathrm{lc}(f(x))$. A polynomial $f(x)$ will be called *monic* if $\mathrm{lc}(f) = 1$.

The following two lemmas can be proven quickly by the definition of the degree and considering the leading coefficients of $f(x) + g(x)$ and $f(x)g(x)$ respectively.

Lemma 2.2.1. *If R is a ring, then for any $f(x), g(x) \in R[x]$: $\deg(f(x) + g(x)) \leqslant \max(\deg(f), \deg(g))$.*

Lemma 2.2.2. *If D is a domain, then $D[x]$ is also a domain, and for all $f(x), g(x) \in D[x]$ we have $\deg(fg) = \deg(f) + \deg(g)$.*[1] *Also, the units of $D[x]$ will be the units of D.*

2.3 Euclidean division algorithm

The proof of the following proposition will be given when we prove algorithm 1.

Proposition 2.3.1. *Let R be a commutative ring, and $f(x), g(x) \in R[x]$ with $g(x) \neq 0$, $m = \deg(g)$ and b_m the leading coefficient of $g(x)$. Then there exist $k \in \mathbb{N}, q(x), r(x) \in R[x]$ such that:*

$$b^k f(x) = q(x)g(x) + r(x) \wedge \deg(r) < \deg(g). \tag{2.1}$$

Corollary 2.3.2. *Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist* unique *$q(x), r(x) \in F[x]$ such that:*

$$f(x) = q(x)g(x) + r(x) \wedge \deg(r) < \deg(g). \tag{2.2}$$

Proof. We can find some $k \in \mathbb{N}$ and $q(x), r(x) \in F[x]$ such that $b_m^k f(x) = q(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$, where $b_m = \mathrm{lc}(g)$. Now since $g(x) \neq 0$, we have $b_m \neq 0$ and thus $f(x) = (b_m^{-k} q(x))g(x) + (b_m^{-k} r(x))$. Also, since F is a domain: $\deg(b_m^{-k} r(x)) = \deg(b_m^{-k}) + \deg(r(x)) = \deg(r(x)) < \deg(g(x))$.

[1] It is to be understood here that $-\infty + a = -\infty$ for any $a \in \mathbb{N} \cup \{-\infty\}$.

Now let $q_1(x), r_1(x) \in F[x]$ also satisfy (2.2). Then $(q(x) - q_1(x))g(x) = r_1(x) - r(x)$. Without loss of generality we may assume that $\deg(r) \geqslant \deg(r_1)$. It then follows that $\deg(g) > \deg(r) \geqslant \deg(r_1 - r) = \deg(q - q_1) + \deg(g)$ and this is only possible if $\deg(q - q_1) = -\infty$. Then $q(x) = q_1(x)$ and thus $r_1(x) = r(x)$. □

ALGORITHM 1: EUCLIDEAN DIVISION ALGORITHM

Let R be a commutative ring and $f(x), g(x) \in R[x]$ with $f(x), g(x) \neq 0$. Also let $m = \deg(g) \in \mathbb{N}$ and $0 \neq b \in R$ the leading coefficient of $g(x)$. Define the following three coupled sequences:

$$f_0(x) = f(x) \qquad \begin{aligned} n_0 &= \deg(f_0) \\ a_0 &= \mathrm{lc}(f_0) \end{aligned}$$

$$f_{i+1}(x) = \begin{cases} bf_i(x) - a_i x^{n_i - m} g(x) & n_i \geqslant m \\ 0 & n_i < m \end{cases} \qquad \begin{aligned} n_{i+1} &= \deg(f_{i+1}) \\ a_{i+1} &= \mathrm{lc}(f_{i+1}) \end{aligned}$$

Then there exists a $k \in \mathbb{N}$ such that $f_k(x) \neq 0$, $f_{k+1}(x) = 0$ and $n_k < m$. Also[2]:

$$b_m^k f(x) = \left(\sum_{l=0}^{k-1} a_l b^{k-l-1} x^{n_l - m} \right) g(x) + f_k(x). \tag{2.3}$$

Proof. Let $i \in \mathbb{N}$. We then see that $\deg(f_{i+1}) = \deg(bf_i(x) - a_i x^{n_i - m} g(x) < \deg(f_i(x))$, since the leading coefficients of $bf_i(x)$ and $a_i x^{n_i - m} g(x)$ are both $a_i b$. This shows that the degree strictly decreases each step, and since $f_0(x) \neq 0$, there exists some $k \in \mathbb{N}$ such that $f_k(x) \neq 0$, $\deg(f_k) = n_k < m$ and thus $f_{k+1}(x) = 0$. We may see this k as the terminal step of the algorithm, since from this point on only zero polynomials will be produced.

We will now prove the following: for any $i \in \mathbb{N}$ such that $i \leqslant k$ we have $b^i f(x) = f_i(x) + \left(\sum_{l=0}^{i-1} a_l b^{i-l-1} x^{n_l - m} \right) g(x)$. For $i = 0$ this is clear, so pick $i \in \mathbb{N}$ with $0 < i \leqslant k$ and assume this holds for $i - 1$. Then:

$$\begin{aligned} b^i f(x) = bb^{i-1} f(x) &= bf_{i-1}(x) + b \left(\sum_{l=0}^{i-2} a_l b^{i-l-2} x^{n_l - m} \right) g(x) \\ &= f_i(x) + a_{i-1} x^{n_{i-1} - m} g(x) + \left(\sum_{l=0}^{i-2} a_l b^{i-l-1} x^{n_l - m} \right) g(x) \\ &= f_i(x) + \left(\sum_{l=0}^{i-1} a_l b^{i-l-1} x^{n_l - m} \right) g(x). \end{aligned}$$

This proves our claim. We can then set $i = k$ to obtain our final formula for $f(x)$, which concludes the proof and also proves proposition 2.3.1, since $\deg(f_k) = n_k < m = \deg(g)$. □

[2] We understand here, that if $k = 0$, the sum evaluates to 0.

2.3.1 Polynomial factors

The Euclidean division algorithm can be used to prove an array of useful facts. The first of these will concern factors of polynomials. Since we will almost exclusively be concerned with commutative rings from this point on, R will denote a commutative ring in the rest of this chapter.

Definition 2.3.1. If $f(x), g(x) \in R[x]$, then $g(x)$ is a *factor* of $f(x)$ – denoted as $g(x) \mid f(x)$ – if and only if there exists an $h(x) \in R[x]$ such that $f(x) = g(x)h(x)$.

Also, a polynomial $f(x) \in R[x]$ of positive degree will be called *reducible* if there exist $g(x), h(x) \in R[x]$ of positive degree such that $f(x) = g(x)h(x)$. Otherwise, $f(x)$ will be called *irreducible*.[3]

The following two results characterize the zeroes of a polynomial. They will be used a couple of times in the next chapters.

Lemma 2.3.3. *If $f(x) \in R[x]$ and $a \in R$, then there exists a unique $q(x) \in R[x]$ such that $f(x) = (x - a)q(x) + f(a)$.*

Proof. By the Euclidean division algorithm we may pick $q(x), r(x) \in R[x]$ with $\deg(r) < \deg(x - a) = 1$ and $f(x) = (x - a)q(x) + r(x)$. We then immediately see that $f(a) = (a - a)q(a) + r(a) = r(a)$, and since $\deg(r) < 1$ we must have $r(x) = f(a)$. Also, since $r(x)$ is fixed in this way, if $q_1(x)$ also satisfies $f(x) = (x - a)q_1(x) + r(x)$, then $(x - a)(q(x) - q_1(x)) = 0$. Now, since the leading coefficient of x is 1, which is not a zero divisor, we get $q(x) = q_1(x)$. □

Corollary 2.3.4. *If $f(x) \in R[x]$ and $a \in R$. Then a is a zero of $f(x)$ if and only if $(x - a) \mid f(x)$.*

Proof. By the previous lemma there is a $q(x) \in R[x]$ such that $f(x) = (x - a)q(x) + f(a)$. So, if $f(a) = 0$, then $(x - a)|f(x)$. Conversely, if $(x - a)|f(x)$, there exists some $h(x) \in R[x]$ such that $f(x) = (x - a)h(x)$. But then $f(a) = (a - a)h(a) = 0$. □

We can also apply the Euclidean division algorithm to determine a greatest common factor of two polynomials with coefficients in a field F. By a greatest common factor (or divisor) of a pair of polynomials $(f(x), g(x))$ we mean a polynomial $h(x)$ such that $h(x) \mid f(x)$, $h(x) \mid g(x)$ and if $d(x) \in F[x]$ such that $d(x) \mid f(x)$ and $d(x) \mid g(x)$, then $d(x) \mid h(x)$. Degree considerations quickly show that two greatest common factors differ by a unit factor in F. Now, for any two polynomials $f(x), g(x) \in F[x]$ we then define $\gcd(f, g) \in F[x]$ to be the unique monic greatest common divisor.

[3]Several other definitions are possible. For example, a polynomial may be called irreducible if it is not a unit, and if it can be written as a product of two polynomials, one of them must be a unit. However, in polynomial rings over a field, this leads to the same concept. Hence we adopt this definition.

Lemma 2.3.5. *Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, and $q(x), r(x) \in F[x]$ such that $\deg(r) < \deg(g)$ and $f(x) = q(x)g(x) + r(x)$. Then for every $h(x) \in F[x]$, $h(x) \mid f(x)$ and $h(x) \mid g(x)$ if and only if $h(x) \mid g(x)$ and $h(x) \mid r(x)$.*

Proof. Let $h(x) \in F[x]$. If $h(x) \mid f(x)$ and $h(x) \mid g(x)$, then there exists some $\alpha(x), \beta(x) \in F[x]$ such that $f(x) = \alpha(x)h(x)$ and $g(x) = \beta(x)h(x)$. Then $r(x) = f(x) - q(x)g(x) = \alpha(x)h(x) - q(x)\beta(x)h(x) = (\alpha(x) - q(x)\beta(x))h(x)$, so that $h(x) \mid r(x)$ and $h(x) \mid g(x)$.

Conversely, let $h(x) \mid g(x)$ and $h(x) \mid r(x)$. Then there exist $\gamma(x), \rho(x) \in F[x]$ so that $g(x) = \gamma(x)h(x)$ and $r(x) = \rho(x)h(x)$, so that $f(x) = (q(x)\gamma(x) + \rho(x))h(x)$ and thus $h(x) \mid f(x)$ and $h(x) \mid g(x)$. □

ALGORITHM 2: THE GCD AND EUCLIDEAN SEQUENCE OF TWO POLYNOMIALS OVER A FIELD

Let $f(x), g(x) \in F[x]$ where F is a field and $g(x) \neq 0$, and define the following sequence:

$$h_0(x) = f(x) \qquad h_1(x) = g(x)$$

$$h_{i+2}(x) = \begin{cases} q_{i+1}(x)h_{i+1}(x) - h_i(x), & \text{if } h_{i+1}(x) \neq 0 \\ 0, & \text{if } h_{i+1}(x) = 0 \end{cases}$$

$$\deg(h_{i+2}) < \deg(h_{i+1}), \qquad i \in \mathbb{N}.$$

(It is understood here that $-\infty < -\infty$). Then there exists a $1 \leqslant s \in \mathbb{N}$ such that $h_s(x) \neq 0$, but $h_{s+1}(x) = 0$. Furthermore, $h_s(x)$ is a greatest common factor of $f(x)$ and $g(x)$. The finite sequence (terminating at $h_s(x)$) thusly defined is called the Euclidean sequence of $f(x)$ and $g(x)$.

Proof. Let $d(x) \in F[x]$ be a common divisor of $f(x)$ and $g(x)$. Then by repeated use of lemma 2.3.5 see that this is the case if and only if $d(x)$ is a common divisor of $h_{s-1}(x)$ and $h_s(x)$. Therefore, every common divisor of $f(x)$ and $g(x)$ will be a factor of $h_s(x)$. Also, since $h_s(x) \mid q_s(x)h_s(x) = h_{s-1}(x)$ and $h_s(x)$ is a factor of itself, $h_s(x)$ is a common factor of $f(x)$ and $g(x)$, and thus a greatest common factor. □

2.4 Field extensions

In the theory of fields, the main subject of study is a field extension. Informally, this is a field that contains some other field. This notion is particularly important for the study of polynomial equations. We will discuss field extension that are generated by finitely many elements, which can be seen as fields that are obtained by adjoining some elements.

Definition 2.4.1. Let F be a field. An *field extension* over F is then a field E such that F is a subfield of E.

If $S \subseteq F$, then a subfield K of F is said to be generated by S if it is the smallest subfield containing S.

If E is a field extension over F, and $S \subseteq E$, we denote the subfield generated by $S \cup F$ by $F(S)$. If $S = \{ u_1, \ldots, u_n \}$ is finite, we denote it by $F(u_1, \ldots, u_n)$.

2.4.1 Simple Field Extensions

We will first consider the structure of simple field extensions. That is, field extensions over F of the form $F(u)$. The following proposition will be crucial in our discussion. In this discussion we take a slightly different route than in [4].

Proposition 2.4.1. *Let F be a field. Then $F[x]$ is a principal ideal domain.*

Proof. It is clear that the trivial ideal $\{ 0 \}$ is a principal ideal. Therefore, let $\{ 0 \} \neq I \subseteq F[x]$ be an ideal of $F[x]$ and $f(x) \in I$. We may also clearly pick a non-zero $g(x) \in R[x]$ of minimal degree. Then there exist $q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$ with $\deg(r) < \deg(g)$. But then $r(x) = f(x) - q(x)g(x) \in I$. Since $g(x)$ was of minimal degree, we must have that $r(x) = 0$. Therefore $f(x) = q(x)g(x)$ for some $q(x) \in F[x]$ and we conclude that $I = (g(x))$ is principal. We have also already seen that, since F is a domain, $F[x]$ is a domain. This concludes the proof. □

Definition 2.4.2. If R is a subring of a commutative ring S, and $u \in S$, we will call u *algebraic* over R if there exists a $0 \neq f(x) \in R[x]$ such that $f(u) = 0$. Otherwise, we will call u *transcendental* over R.

A field extension E over F will be called *algebraic* if and only if every element of E is algebraic over F.

Lemma 2.4.2. *If R is a subring of the commutative ring S and $u \in S$ is transcendental over R, then $F[x] \cong F[u]$.*

Proof. If u is transcendental over R, then the kernel of the evaluation homomorphism $\rho : F[x] \to S$ in u is $\{ 0 \}$. This shows that $F[x] \cong A = \rho(F[x])$. Since A contains R and u, we obtain $R[u] \subseteq A$. Also, if $x \in A$, then there exists some $f(x) = \sum_{i=1}^{n} a_i x^i \in F[x]$ such that $x = f(u) = \sum_{i=1}^{n} a_i u^i \in R[u]$. Therefore, $A \subseteq R[u]$ and we conclude that $F[x] \cong A = R[u]$. □

Lemma 2.4.3. *Let F be a field and $f(x) \in F[x]$ of positive degree and irreducible. Then $F[x]/(f(x))$ is a field. Furthermore, $F[x]/(f(x)) = F(u)$, where $u = x \mod (f(x))$ is a zero of $f(x)$, when regarded as a polynomial with coefficients in $F[x]/(f(x))$.*

Proof. Let $J' \subseteq F[x]/I$ be an ideal, where $I = (f(x))$. Then there exists an ideal $J \subseteq F[x]$ such that $I \subseteq J$ and $J' \cong J/I$. Since $F[x]$ is a principal ideal domain, we can find a $g(x) \in F[x]$ such that $J = (g(x))$. Therefore,

there exists a $h(x) \in F[x]$ such that $f(x) = h(x)g(x)$. Now, since $f(x)$ is irreducible, we have either $h(x) \in F$ or $g(x) \in F$. In the first case, we get $J = I$, so that $J' = \{\, 0 \mod I \,\}$. In the second case we get $J = F[x]$, so that $J' = F[x]/I$. This shows that $F[x]/I$ has only the trivial ideals and thus it is a field.

Now set $K = F[x]/(f(x))$ and let $u = x \mod (f(x)) \in K$. Then clearly $f(u) = f(x) \mod (f(x)) = 0 \mod (f(x))$. We also have $F(u) \subseteq K$. Now let $a \in K$. Then there exists some $b(x) \in F[x]$ so that $a = b(x) \mod (f(x))$. But, there also exist $q(x), r(x) \in F[x]$ with $\deg(r) < \deg(f)$ and $b(x) = q(x)f(x) + r(x)$. Therefore $a = r(x) \mod (f(x)) = r(u)$. Now write $r(x) = \sum_{i=0}^{m} r_i x^i$. Then $a = r(u) = \sum_{i=0}^{m} r_i u^i \in F(u)$. We therefore conclude that $K = F(u)$. □

Proposition 2.4.4. *Let E be a field extension over F and $u \in F$. If u is transcendental over F, then $F(u) \cong F(x)$, the field of fractions of $F[x]$. If u is algebraic over F, there exists some irreducible $g(x) \in F[x]$ such that $F(u) \cong F[x]/(g(x))$. Moreover, this $g(x)$ is unique up to a unit multiplier.*

Proof. If u is transcendental, then $F[x] \cong F[u]$. Now, since $F[u] \subseteq F(u)$, and the field of fractions of $F[u]$ is the smallest field containing $F[u]$ (and the fields of fractions of two isomorphic integral domains are isomorphic), we get $F(u) \cong F(u)$.

Now suppose that u is algebraic over F. Then, since $F[x]$ is a principal ideal domain, there exists some $g(x) \in F[x]$ such that the kernel of the evaluation homomorphism $\rho : F[x] \to E$ in u is $I = (g(x))$ and thus $\rho(F[x]) \cong F[x]/I$, by the first isomorphism theorem of rings. We claim that $F[x]/I$ is a field.

Suppose that there exist $f(x), h(x) \in F[x]$ such that $g(x) = f(x)h(x)$. Now, if $f(x) \in I$, then there exists a $k(x) \in F[x]$ such that $f(x) = k(x)g(x)$ and hence $g(x) = h(x)k(x)g(x)$. This would imply that $\deg(h) = 0$, and hence $h(x) \in F$. Similarly, if $h(x) \in I$, then $f(x) \in F$. Now let both $f(x), h(x) \notin I$. Then $f(u) \neq 0 \neq h(u)$, but $f(u)h(u) = g(u) = 0$, so then E would contain non-zero zero-divisors. From this we conclude that $g(x)$ is irreducible, and by lemma 2.4.3 we conclude that $F[x]/I$ is a field.

We now observe that $F \subseteq \rho(F[x])$ (since $I \cap F = \{\, 0 \,\}$) and $u \in \rho(F[x])$, so that $F(u) \subseteq \rho(F[x])$. But if $x \in \rho(F[x])$, then there exists a $f(x) = \sum_{i=1}^{n} a_i x^i \in F[x]$ with $x = f(u) = \sum_{i=1}^{n} a_i u^i \in F(u)$. Therefore, $F(u) = \rho(F[x]) \cong F[x]/(g(x))$.

Now let $\{\, 0 \,\} \neq I \subseteq F[x]$ be an ideal and $f(x), g(x) \in F[x]$ such that $I = (f(x)) = (g(x))$. Then, there exist $h(x), k(x) \in F[x]$ such that $f(x) = h(x)g(x)$ and $g(x) = k(x)f(x)$, so that $f(x) = h(x)k(x)f(x)$. Degree considerations then show that $0 \neq h(x), k(x) \in F$. Therefore, $f(x) = ag(x)$ for some unit $a \in F$. □

Definition 2.4.3. If E is a field extension over F, and $u \in E$ is algebraic

over F, we call the unique monic polynomial $g(x) \in F[x]$ such that $F(u) \cong F[x]/(g(x))$ the *minimum polynomial* of u over F.

Also, if $E = F(u)$, we call E a *simple field extension* over F with generator u, and u is called a *primitive element* of E.

2.4.2 Dimensionality of an Extension

If we have a field extension E over F, we may regard E as a vector space over F. In this vector space, the addition is the normal addition of the field, and the scalar multiplication is the normal multiplication in F, where the scalars lie in F. In particular, in vector spaces we have the notion of a dimension. This dimension turns out to be of critical importance.

Definition 2.4.4. If E is a field extension over F, the *dimensionality* (or degree) of E over F is the dimensionality of E regarded as a vector space over F, which shall be denoted as $[E : F]$.

Proposition 2.4.5. *Let E be a field extension over F and $u \in F$. Then u is algebraic over F if and only if $[F(u) : F] < \infty$. Moreover, if u is algebraic, then $[F(u) : F]$ is the degree of the minimum polynomial of u.*

Proof. Let u be algebraic over F and $f(x) \in F[x]$ its minimum polynomial. Now let $a \in F(u)$ be arbitrary. Then there exists a $g(x) = \sum_{i=0}^{n-1} a_i x^i \in F[x]$ such that $a = g(u) = \sum_{i=0}^{n-1} a_i u^i$ where $n = \deg(f)$ and $a_i \in F$ for $0 \leqslant i \leqslant n-1$. Therefore, $(1, u, \ldots, u^{n-1})$ spans the vector space $F(u)$ over F. Now let $b_0, \ldots, b_{n-1} \in F$ such that $\sum_{i=0} b_i u^i = 0$. Then $h(x) = \sum_{i=0}^{n-1} b_i x^i \in (f(x))$. But since $\deg(h) < \deg(f)$ we get $h(x) = 0$, so that $b_0 = \cdots = b_{n-1} = 0$. This shows that $(1, u, \ldots, u^{n-1})$ is a base for the vector space $F(u)$ over F, and hence $[F(u) : F] = n < \infty$.

Now let u be transcendental over F. Then let $n \in \mathbb{N}$ and $a_0, \ldots, a_n \in F$. We recall that $F[x] \subseteq F(x) \cong F(u)$. Therefore, $0 = \sum_{i=0}^{n} a_i u^i \cong \sum_{i=0}^{n} a_i x^i$ implies that $a_0 = \cdots = a_n = 0$, which shows that there exists no finite base for $F[x]$ as a vector space over F. Now, since $F[x]$ is a subspace of $F(u)$, we then certainly have that $[F(u) : F] = \infty$. By negation of this argument, we get that if $[F(u) : F] < \infty$, then u must be algebraic over F. □

Proposition 2.4.6 (Dimensionality formula)**.** *Let K be a field extension over E, which is in turn a field extension over F. Then K is a field extension over F and $[K : F] < \infty$ if and only if $[K : E], [E : F] < \infty$. If $[K : F] < \infty$, then:*

$$[K : F] = [K : E][E : F] \tag{2.4}$$

Proof. It is trivial that K is a field extension over F.

If $[K : F] < \infty$, then $[E : F] < \infty$, since E is a subspace of K. Now let $\{ u_1, \ldots, u_n \} \subset K$ be a base for K. Then for every $a \in K$ there exist

$a_1, \ldots, a_n \in F \subseteq E$ such that $\sum_{i=1}^{n} a_i u_i = a$. Therefore, $\{ u_1, \ldots, u_n \}$ spans K as a vector space over E. We conclude that $[K : E] \leqslant n < \infty$.

Now let $[K : E], [E : F] < \infty$ and pick bases $(u_1, \ldots, u_m) \subseteq E$ and $(v_1, \ldots, v_n) \subseteq K$ for E over F and K over E respectively. Pick any $a \in K$. Then there exist $a_1, \ldots, a_n \in E$ such that $a = \sum_{i=1}^{n} a_i v_i$. Also, for $1 \leqslant i \leqslant n$ there exist $b_{i1}, \ldots, b_{im} \in F$ such that $a_i = \sum_{j=1}^{m} b_{ij} u_j$. This gives us $a = \sum_{i=1}^{n} \sum_{j=1}^{m} b_{ij} u_j v_i$, so that the set $\{ u_j v_i \mid 1 \leqslant i \leqslant n \wedge 1 \leqslant j \leqslant m \}$ spans K as a vector space over F. Now let $c_{11}, \ldots, c_{nm} \in F$ such that $\sum_{i=0}^{n} \sum_{j=0}^{m} c_{ij} u_j v_i = 0$. Then clearly for $1 \leqslant i \leqslant n$: $d_i = \sum_{j=0}^{m} c_{ij} u_j = 0$. This implies that for $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$ we have $c_{ij} = 0$. Therefore we have obtained a base for K over F and $[K : F] = nm = [K : E][E : F] < \infty$. □

The following corollary is immediate and will be used later on.

Corollary 2.4.7. *Let K be a field extension of F with $[K : F] < \infty$. Then for any field extension $E \subseteq K$ of F, $[E : F] \mid [K : F]$. Also, if $[K : F]$ is prime, then the only subfields of K that contain F are K and F themselves.*

2.4.3 Splitting Fields

We have seen before that if we have a field extension E over F and some monic polynomial $f(x) \in F[x]$, the $u \in E$ is a zero of $f(x)$ if and only if $(x - u) \mid f(x)$, where we regard $f(x)$ as a polynomial in $E[x]$ (by the induced inclusion homomorphism). It would of course be great if we could find a field extension E over F where we could write $f(x) = \prod_{i=1}^{n} (x - r_i)$ for $r_1, \ldots, r_n \in E$. Also, taking into account the results we obtained for the dimensionalities of field extensions, we would like that $E = F(r_1, \ldots, r_n)$, since then $[E : F] = \prod_{i=1}^{n} [F(u_1, \ldots, u_i) : F(u_1, \ldots, u_{i-1})]$ (where the first term in the product is understood to be $[F(u_1) : F]$. Also, if $r \in E$ is then a zero of $f(x)$, then $0 = f(r) = \prod_{i=1}^{n} (r - r_i)$ such that $r = r_i$ for some $1 \leqslant i \leqslant n$. We will call such a field extension a splitting field of $f(x)$ over F.

Definition 2.4.5. Let F be a field and $f(x) \in F[x]$ monic. Then a splitting field of $f(x)$ over F is a field extension E over F, such that in $E[x]$ we can write $f(x) = \prod_{i=1}^{n} (x - r_i)$ for $r_1, \ldots, r_n \in E$ and $E = F(r_1, \ldots, r_n)$.

Proposition 2.4.8. *If F is a field and $f(x) \in F[x]$ is monic, then there exists a splitting field E of $f(x)$ over F.*

Proof. Let $f(x) = \prod_{i=1}^{k} f_i(x)$ where for $1 \leqslant i \leqslant k$, $f_k(x) \in F[x]$ is monic and irreducible. Then $k \leqslant n = \deg(f)$. If $n = k$, F itself is a splitting field of $f(x)$. Now let $n - k > 0$. Then for some $j \in \{ 1, \ldots, k \}$ we have $\deg(f_j) > 1$. Set $K = F[x]/(f_1(x))$, which is a field that contains F, and $r = x \mod (f_i(x))$, so that $K = F(r)$ and $f_1(r) = 0$. Then in $K[x]$

we have $f(x) = \prod_{i=1}^{l} g_i(x)$, where for $1 \leqslant i \leqslant l$, $g_i(x) \in K[x]$ are the irreducible factors of $f(x)$ in $K[x]$. Since these factors can be obtained by taking the irreducible factors of the $f_i(x)$ and $(x - r) \in K[x]$ is an irreducible factor of $f_1(x)$, we obtain $n \geqslant l > k$, so that $n - l < n - k$. By induction we then obtain an extension field $E = K(r_1, \ldots, r_n)$ such that $f(x) = \prod_{i=i}^{n}(x - r_i)$, where $r = r_i$ for some $1 \leqslant i \leqslant n$. This shows that $E = F(r)(r_1, \ldots, r_n) = F(r_1, \ldots, r_n)$ is a splitting field of $f(x)$ over F. $\square$

We state the following proposition without proof, which can be found in [4].

Proposition 2.4.9. *Let F be a field, $f(x) \in F[x]$ monic and of positive degree, and E and E' splitting fields of $f(x)$ over F. Then $E \cong E'$.*

We may now quickly see that the splitting of a monic polynomial in factors of degree one is unique. Therefore, the zeroes are unique and the following definition is consistent over every possible splitting field.

Definition 2.4.6. Let F be a field, $f(x) \in F[x]$ monic and of positive degree, and E a splitting field of $f(x)$ over F. Write $f(x) = \prod_{i=1}^{m}(x - r_i)^{k_i}$, where $r_i \neq r_j$ if $i \neq j$. We then call k_i the *multiplicity* of r_i. Also, a zero r_i is called a *simple zero* if and only if it has multiplicity 1. Otherwise, it is called a *multiple zero.*

We lastly make the connection between the derivative of a polynomial and the character of its zeroes. Informally, we will see that a zero (in a splitting field) has multiplicity greater than 1 if and only if the polynomial and its derivative have a common factor of positive degree. For this we define the following map on a polynomial ring of a field.

Definition 2.4.7. Let F be a field. We then define the *standard derivation* in $F[x]$ as the unique function $F[x] \to F[x] : f(x) \mapsto f'(x)$ so that for any $f(x), g(x) \in F[x]$:

1. $(f + g)'(x) = f'(x) + g'(x)$
2. $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$
3. $x' = 1$.

As in real analysis we may quickly derive all the familiar algebraic properties of polynomial derivatives. We can now state the following proposition, the proof of which can be found in [4, Sec. 4.4].

Proposition 2.4.10. *Let F be a field, $f(x) \in F[x]$ monic and of positive degree, and E any splitting field of $f(x)$ over F. Then all zeroes of $f(x)$ in E are simple if and only if* $\gcd(f, f') = 1$.

2.4.4 Galois Theory

Galois theory is one of the pearls of modern mathematics. It allows one to study solutions of algebraic equations in a purely algebraic way. At the heart of the theory is the connection between the solutions of such equations and group theory. We will state the fundamental results without proof for later use. An extensive treatment of this subject may (again) be found in [4, Ch. 4]. Throughout this subsection, F denotes a field.

Definition 2.4.8. $f(x) \in F[x]$ is called *seperable* if and only if its irreducible factors have distinct zeroes in any splitting field.

An algebraic field extension E over F is called *seperable* over F if and only if the minimum polynomial over F of every element of E is seperable. Also, E is called *normal* over F if and only if every irreducible polynomial in $F[x]$ that has a zero in E splits into factors of degree 1.

Lemma 2.4.11. *Any field extension E over F of characteristic 0 is seperable.*

Definition 2.4.9 (The Galois group)**.** Let E be a field extension over F. The *Galois group* of E over F is then the group $\mathrm{Gal}(E/F)$ of automorphisms of E that reduce to the identity when restricted to F.

Also, if G is any subgroup of the group of automorphisms of E, then $\mathrm{Inv}\, G \subseteq E$ is the subfield of elements that are invariant under all automorphisms in G.[4]

Definition 2.4.10. A field extension E over F is called a *Galois field extension* if and only if E is a splitting field of $f(x)$ over F for some seperable $f(x) \in F[x]$.

Lemma 2.4.12. *If E is a splitting field of $f(x)$ over F for some monic seperable $f(x) \in F[x]$, then $|\,\mathrm{Gal}(E/F)| = [E : F]$.*

Proposition 2.4.13. *Let E be a field extension over F. Then the following statements are equivalent:*

- *E is a Galois field extension over F.*
- *$F = \mathrm{Inv}\, G$ for some finite subgroup of $\mathrm{Aut}\, E$.*
- *$[E : F] < \infty$, and E is normal and seperable over F.*

Theorem 2.4.14 (Fundamental Theorem of Galois Theory)**.** *Let E be a Galois field extension over F and define:*

- *Γ is the set of subgroups of $\mathrm{Gal}(E/F)$.*

[4] It follows that $G = \mathrm{Gal}(E/F)$ is the subgroup of $\mathrm{Aut}\, E$ such that $\mathrm{Inv}\, G = F$.

- Σ *is the set of subfields* $K \subseteq E$ *such that* $F \subseteq K$.
- $\gamma : \Gamma \to \Sigma : H \mapsto \mathrm{Inv}(H)$.
- $\sigma : \Sigma \to \Gamma : K \mapsto \mathrm{Gal}(E/K)$.

Then γ *and* σ *are inverse bijections, and we have the following properties:*

1. $\forall H_1, H_2 \in \Gamma : H_1 \subseteq H_2 \iff \mathrm{Inv}\, H_1 \supseteq H_2$,
2. $\forall H \in \Gamma : |H| = [E : \mathrm{Inv}\, H] \wedge [G : H] = [\mathrm{Inv}\, H : F]$,
3. $\forall H \in \Gamma$*:* H *is a normal subgroup of* $\mathrm{Gal}(E/F)$ *if and only if* $\mathrm{Inv}\, H$ *is a normal field extension over* F*. In this case* $\mathrm{Gal}((\mathrm{Inv}\, H)/F) \cong (G/H)$.

Chapter 3

Real Closed Fields

In this chapter we will develop the framework in which we prove Sturm's Theorem. We will begin with a discussion of ordered fields, showing that a field can be (compatibly) ordered if and only if the field is formally real (meaning that no non-zero element is a sum of squares). We will then discuss real closed fields and some of their key properties, going on to investigate several equivalent characterizations of real closed fields. This serves to illustrate the importance of real closed fields in applications. Again we will follow [4] in our discourse.

3.1 Ordered and Formally Real Fields

Definition 3.1.1. An *ordered field* is a pair (F, P) where F is a field, and $P \subset F$ such that

1. $0 \notin P$,
2. $\forall a \in F : a = 0 \vee a \in P \vee -a \in P$,
3. $\forall a, b \in P : a + b \in P \wedge ab \in P$.

We call the elements of P the positive elements of F.

We also say that a field F can be ordered if and only if a $P \subset F$ exists so that (F, P) is an ordered field.

Lemma 3.1.1. *If (F, P) is an ordered field, define the set of negative elements $N = \{ x \in F \mid \exists p \in P : x = -p \}$. Then P, N and $\{ 0 \}$ are disjoint and $F = P \cup \{ 0 \} \cup N$.*

Proof. We first note that $0 \notin P$ by property 1. This implies that $0 = -0 \notin N$. Therefore $P \cap \{ 0 \} = \varnothing = N \cap \{ 0 \}$. Now suppose that $P \cap N \neq \varnothing$ and let $a \in P \cap N$. Then $-a \in P$, so by property 3: $0 = a - a \in P$. This contradiction with property 1 shows that $P \cap N = \varnothing$.

Now let $a \in F \backslash \{ 0 \}$. Then by property 2, $a \in P$ or $a \in N$, so $a \in P \cup N$ and $F = P \cup \{ 0 \} \cup N$. □

Definition 3.1.1 of an ordered field is not so intuitive at first glance, but it becomes more transparent when we recall that P were the positive elements and we consider the following:

Proposition 3.1.2. *Any ordered field (F, P) induces a strict total order $>$ by:*

$$\forall a, b \in F : a > b \iff a - b \in P, \tag{3.1}$$

with the following properties:

1. $\forall a \in F : \big[a > 0 \iff \forall b \in F : a + b > b\big]$,
2. $\forall a, b \in F : a > 0 \wedge b > 0 \implies ab > 0$.

Conversely, if $>$ is a strict total order with the properties above, then $P = \{\, x \in F \mid x > 0 \,\}$ defines an ordered field (F, P).

Proof. Let (F, P) be an ordered field and define $>$ as above. We shall first show that $>$ is a strict total order. Let $a, b, c \in F$ such that $a > b$ and $b > c$. Then $a - b \in P$ and $b - c \in P$. We then have $a - c = a - b + b - c \in P$, so $a > c$, which shows that $>$ is transitive. Then, if we take $a, b \in F$, we see by lemma 3.1.1 that either $a = b$, $a - b \in P$, or $b - a \in P$. Therefore, either $a = b$, $a > b$ or $b > a$, so $>$ is trichotomous and a strict total order.

To prove property 1, let $a \in F$. If $a > 0$, then $\forall b \in F : (a+b)-b = a \in P$, so $\forall b \in F : a + b > b$. Conversely, if $\forall b \in F : a + b > b$, then this is in particular the case for $b = 0$: $a > 0$.

To prove property 2, let $a, b \in F$ with $a > 0$ and $b > 0$. Then $a, b \in P$ and thus $ab \in P$, which shows that $ab > 0$.

Let us now suppose that we are given a strict total order $>$ on F satisfying properties 1 and 2. Define $P = \{\, x \in F \mid x > 0 \,\}$. Then clearly $0 \notin F$, since otherwise $0 > 0$, which is the first property of an ordered field. Also, by the trichotomy of $>$, we have for any $a \in F$: $a > 0$, $a = 0$, or $0 > a$. This means: $a = a - 0 \in P$, $a = 0$, or $-a = 0 - a \in P$, so P also satisfies the second property. Now let $a, b \in P$. Then by property 1 and the transitivity of $>$: $a > 0 \implies a + b > b > 0 \implies a + b \in P$. Also, by property 2: $a > 0 \wedge b > 0 \implies ab > 0 \implies ab \in P$, which finally shows that (F, P) is an ordered field. □

Note: Notation of ordered fields

From now on, if we speak of an ordered field (F, P), and we use the symbol $>$, this will denote the induced strict total order. Also, the symbol $\geqslant$ will denote the total order induced by $>$ (defined by $a \geqslant b \iff a > 0 \vee a = b$). Similarly, for $a \in F$ we write $|a| = a$ if $a = 0$ or $a > 0$ and $|a| = -a$ if $a < 0$. If the set P is not used, we may also just write: "the ordered field F".

Lemma 3.1.3. *If (F, P) is an ordered field, then for any $a \in F^* : a^2 \in P$. In particular we see that $1 = 1^2 \in P$.*

Proof. Let $a \in F^*$. Then either $a \in P$ or $-a \in P$, so that $a^2 = (-a)^2 \in P$, since P is closed under multiplication. □

We state the following lemma without proof, as it is simply proven by considering the various possibilities of the signs of a and b.

Lemma 3.1.4 (Triangle inequality)**.** *If (F, P) is an ordered field, then for any $a, b \in F$:*

$$|a + b| \leqslant |a| + |b|. \tag{3.2}$$

We will now go on to prove a nice characterization of an ordered field in terms of sums of squares. The following definition is due to Artin and Schreier [1][1].

Definition 3.1.2. A *formally real field* is a field F that satisfies the following property:

$$\forall n \in \mathbb{N} \forall a_1, \ldots, a_n \in F \left[\sum_{i=0}^{n} a_i^2 = 0 \implies \forall i \in \{ 1, \ldots, n \} : a_i = 0 \right],$$

i.e. the zero of the field is not the sum of non-zero squares, or the vanishing of a sum of squares implies the vanishing of all the individual squares.

The following lemma illustrates a different characterization[2].

Lemma 3.1.5. *A field F is formally real if and only if $\nexists a_1, \ldots, a_n \in F$ such that $\sum_{i=1}^{n} a_i^2 = -1$.*

Proof. Let F be formally real. Now suppose that there exist $a_1, \ldots, a_n \in F$ such that $\sum_{i=1}^{n} a_i^2 = -1$. Then $\sum_{i=1}^{n} a_i^2 + 1^2 = -1 + 1^2 = 0$, which is forbidden, so no such $\{ a_i \}$ exist.

Conversely, let there exist no $a_1, \ldots, a_n \in F$ such that $\sum_{i=1}^{n} a_i^2 = -1$ and take $b_0, \ldots, b_m \in F$ such that $\sum_{i=0}^{m} b_i^2 = 0$, and suppose that $b_0 \neq 0$ (i.e. one of the b_i is non-zero). Then $-b_0^2 \neq 0$ and $\sum_{i=1}^{m} b_i^2 = -b_0^2 \implies \sum_{i=1}^{m} \left(\frac{b_i}{b_0} \right)^2 = -1$, which gives us a contradiction. Therefore, F is formally real. □

Lemma 3.1.6. *Any ordered field (F, P) is formally real.*

Proof. Let $a \in F \setminus \{ 0 \}$. Then either $a > 0$ or $-a > 0$ and thus $a^2 = (-a)^2 > 0$. We will now show that any sum of non-zero squares is strictly greater than zero by induction.

The induction basis was the first step of the proof. Therefore, let $k \in \mathbb{N}$, $k > 0$, $a_1, \ldots, a_{k+1} \in F \setminus \{ 0 \}$ and $\sum_{i=1}^{k} a_i^2 > 0$. Then $a_{k+1}^2 > 0$ and thus $\sum_{i=1}^{k+1} a_i^2 > \sum_{i=1}^{k} a_i^2 > 0$.

Therefore, if $a_1, \ldots, a_n \in F$ and $\sum_{i=1}^{n} a_i^2 = 0$, we must have that $a_1 = \cdots = a_n = 0$ and thus F is formally real. □

[1] Artin and Schreier chose this as one of the key properties of the real number system, in an effort to characterize the real numbers in a purely algebraic way.

[2] This was actually the original definition of Artin and Schreier.

The converse of the foregoing lemma is a theorem that was proved by Artin and Schreier [1, Satz 1.], and gives the definite answer on the connection between the sums of squares in a field and orderings. We follow a proof of Jean-Pierre Serre [6][3]. We first prove the following

Lemma 3.1.7. *If P_0 is a subgroup of the multiplicative group F^* of a field, such that P_0 is closed under addition and contains all non-zero squares, and if $a \in F^*$ such that $-a \notin P_0$, then*

$$P_1 = P_0 + P_0a = \{\, p \in F \mid \exists x, y \in P_0 : p = x + ya \,\}$$

is a subgroup of F^* that is closed under addition.

Proof. Let $p_1 = x_1 + y_1a, p_2 = x_2 + y_2a \in P_1$, where $x_1, y_1, x_2, y_2 \in P_0$. Then $p_1 + p_2 = (x_1 + x_2) + (y_1 + y_2)a \in P_1$, since P_0 is closed under addition. Also, $p_1p_2 = (x_1 + y_1a)(x_2 + y_2a) = (x_1x_2 + y_1y_2a^2) + (x_1y_2 + x_2y_1)a \in P_1$, since $a^2 \in P_0$ and P_0 is closed under addition and multiplication.

If $0 \in P_1$, then $\exists x, y \in P_0 : x + ya = 0$, so $-a = xy^{-1} \in P_0$, which leads to a contradiction. This shows that $0 \notin P_1$ and thus $P_1 \subseteq F^*$.

Lastly, let $p = x + ya \in P_1, x, y \in P_0$. Then $p^{-1} = (x + ya)^{-1} = (x + ya)(x + ya)^{-2} = [x((x + ya)^{-1})^2] + [y((x + ya)^{-1})^2]a \in P_1$, since $x + ya \neq 0$ and P_0 contains all non-zero squares. Therefore, $P_1 \subseteq F^*$ is a subgroup of the multiplicative group of F that is closed under addition. □

Proposition 3.1.8 (Serre)**.** *If L is an extension field of an ordered field (K, P), then L can be ordered as (L, P_L) with $P \subseteq P_L$ (i.e. the ordering on L extends that on K) if and only if for all $p_1, \ldots, p_n \in P \subseteq K$ and $x_1, \ldots, x_n \in L$: $\sum_{i=1}^n p_i x_i^2 = 0 \implies x_1 = \cdots = x_n = 0$.*

Proof. Let (L, P_L) be an ordered extension field of an ordered field (K, P) with $P \subseteq P_L$. Now take $p_1, \ldots, p_n \in P$ and $x_1, \ldots, x_n \in L$. We first see that for every x_i either $x_i = 0$, in which case $x_i^2 = 0$, or $x_i > 0$ or $-x_i > 0$ so that $x_i^2 = (-x_i)^2 > 0$. Therefore, since each $p_i > 0$ and the positive elements are closed under addition and multiplication, if one of the $x_i \neq 0$: $\sum_{i=1}^n p_i x_i^2 > 0$. So, $\sum_{i=1}^n p_i x_i^2 = 0$ implies that all $x_i = 0$.

Now suppose that the converse is true. Define T as the set of subgroups of L^* that are closed under addition and contain all elements of the form px^2 where $p \in P$ and $x \in L^*$.

Clearly the set $P_0 = \{\, \sum_{i=1}^n p_i x_i^2 \mid p \in P \wedge x_i \in L^* \,\}$ is closed under addition. Now let $x = \sum_{i=1}^n p_i x_i^2, y = \sum_{j=1}^m q_j y_j^2 \in P_0$, where all $p_i, q_j \in P$ and $x_i, y_j \in L^*$. Then $xy = \sum_{i=1}^n \sum_{j=1}^m p_i q_j (x_i y_j)^2 \in P_0$, so P_0 is closed under multiplication. Also, if $x \in P_0$, then $x^{-1} = xx^{-2} \in P_0$, because $x \neq 0$ (by the hypothesis) and thus $x^{-2} = (x^{-1})^2 \in P_0$. This shows that $P_0 \in T$, and thus T is non-empty.

[3] It is entertaining to note that although this argument was thought up by Serre, it was presented on a seminar by Élie Cartan.

By Zorn's Lemma we may now pick a maximal element $P_L \in T$. We claim that this P_L makes L an ordered field that extends K. To see this, let $a \in L^*$. If both a and $-a \in P_L$, then $0 \in P_L$, which is a contradiction, so a and $-a$ cannot be simultaneously in P_L. Now, if $-a \notin P_L$, define $P' = \{ x + ya \mid x, y \in P_L \}$. Since P_L certainly contains all non-zero squares ($1 \in P$), we can conclude by lemma 3.1.7 P' also is a subgroup of L^* that is closed under addition. Furthermore, take $p \in P$ and $x \in L^*$. Then $px^2 = px^2(1+a)(1+a)^{-1} = (px^2 + px^2a)(1+a)^{-1} \in P'$, so $P' \in T$. Also, if $x \in P_L$, then $x = x(1+a)(1+a)^{-1} = (x + xa)(1+a)^{-1} \in P'$, so $P_L \subseteq P'$. Because we took P_L to be maximal in T we can now conclude that $P_L = P'$. Lastly, $a = a(1+a)(1+a)^{-1} = (a^2 + a)(1+a)^{-1} \in P' = P_L$, since P_L contains all non-zero squares. We can now conclude that either $-a \in P_L$ or $a \in P_L$ exclusively.

The above showed that (L, P_L) is an ordered field. Now, if $p \in P \subseteq K$, then $p = p1^2 \in P_L$, so $P \subseteq P_L$ and the order extends the order on K. □

Now we are ready to prove

Theorem 3.1.9. *A field F can be ordered if and only if it is formally real.*

Proof. We already saw that if a field F can be ordered, then it is formally real. Conversely, let F be a formally real field. Then its characteristic is 0 (for if it has characteristic $n \geqslant 1$, then $\sum_{i=1}^{n} 1^2 = 0$, which is not the case), and thus it contains $\mathbb{Q}$ as a subfield.

Let $0 < \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} \in \mathbb{Q}$ where all $p_i \in \mathbb{Z}$ and $q_i \in \mathbb{Z} \setminus \{ 0 \}$, and $x_1, \ldots, x_n \in F$ with $\sum_{i=1}^{n} \frac{p_i}{q_i} x_i^2 = 0$. Let us multiply with $q_1 \ldots q_n$:

$$0 = q_1 \ldots q_n \sum_{i=1}^{n} \frac{p_i}{q_i} x^2 = \sum_{i=1}^{n} \left(\prod_{\substack{j=1 \\ j \neq i}}^{n} q_j \right) p_i x_i^2.$$

This is now a sum of integer multiples of squares, and thus simply a sum of squares. Since F is formally real, we can conclude that all $x_i = 0$. By proposition 3.1.8 we can therefore conclude that there exists an order on F that extends the standard order on $\mathbb{Q}$. □

As our last result on formally real/ordered fields we will give the following lemma, which provides us with bounds on the zeroes of a monic polynomial.

Lemma 3.1.10. *Let F be an ordered field, $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in F[x]$ monic and of positive degree, and $c \in F$. Define $M = \max(1, \sum_{i=0}^{n-1} |a_i|)$. Then $|c| > M$ implies that $|f(c)| > 0$. Conversely, if $f(c) = 0$, then $-M \leqslant c \leqslant M$.*

Proof. Let $c \in F$ with $|c| > M$. We first note $c \neq 0$, so that: $1 = u^{-n} f(u) - \sum_{i=1}^{n-1} a_i u^{i-n}$. Also, $|u^{-n}| < 1$, and for $i \in 0, \ldots, n-1$ we have $|u^{i-n}| <$

$|u^{-1}|$. From this, and the triangle inequality, it follows that:

$$\begin{aligned} 1 &= |u^{-n}f(u) - \sum_{i=1}^{n-1} a_i u^{i-n}| \\ &\leqslant |u^{-n}||f(u)| + \sum_{i=1}^{n-1} |a_i||u^{i-n}| \\ &< |f(u)| + |u^{-1}| \sum_{i=1}^{n-1} |a_i| \\ &\leqslant |f(u)| + M^{-1}M = |f(u)| + 1, \end{aligned}$$

from which we can conclude that $|f(u)| > 0$.

If we now negate this statement, then $f(c) = 0$ implies that $-M \leqslant c \leqslant M$. □

3.2 Real Closed Fields

Artin and Schreier defined a refinement of formally real fields in an attempt to capture the characteristic algebraic properties of the real numbers. There are several useful examples of formally real fields, which include the real numbers, the real numbers that are algebraic over $\mathbb{Q}$, the hyperreal numbers and the computable numbers. Let us state the definition.

Definition 3.2.1. A field F is called *real closed* if and only if F is formally real and no proper algebraic extension field of F is formally real.

This definition and the foregoing discussion of formally real fields shows that a real closed field F is *closed* in the sense that it can be ordered, but no extension of it can be ordered. We will go on to find some more useful characterizations. We first observe the following very useful facts, where we follow the proof in [1].

Lemma 3.2.1. *If F is a real closed field, then:*

- *Every sum of squares in F can also be written as a single square.*
- $\forall x \in F\ \exists y \in F : x = y^2 \vee -x = y^2$.
- *Every polynomial $f(x) \in F[x]$ of odd degree has a zero in F.*

Proof. Let $\gamma \in F$ not be a square. Then the polynomial $x^2 - \gamma \in F[x]$ is irreducible, so $F(\sqrt{\gamma}) = F[x]/(x^2 - \gamma)$ is a proper field extension of F, hence it is not formally real. This shows that there exist $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in F$ such that

$$\gamma \sum_{\nu=1}^{n} \alpha_\nu^2 + \sum_{\nu=1}^{n} \beta_\nu^2 + 2\sqrt{\gamma} \sum_{\nu=1}^{n} \alpha_\nu \beta_\nu = \sum_{\nu=1}^{n} (\alpha_\nu \sqrt{\gamma} + \beta_\nu)^2 = -1.$$

If $\sum_{\nu=1}^{n} \alpha_\nu \beta_\nu \neq 0$, then $\sqrt{\gamma} \in F$, which leads to a contradiction, so that this sum vanishes. Also, if $\sum_{\nu=1}^{n} \alpha_\nu^2 = 0$, then -1 would be a sum of squares in F, which is also a contradiction, so that sum does not vanish. We can then conclude that γ is not a sum of squares in F, since otherwise -1 would be a sum of squares in F. Negating this statement leads to the first property.

By the first property we may now pick $\alpha, \beta \in F$ such that:

$$\alpha^2 = \sum_{\nu=1}^{n} \alpha_\nu^2, \qquad \beta^2 = 1 + \sum_{\nu=1}^{n} \beta_\nu^2$$

(observe that $1 = 1^2$) and thus:

$$-\gamma = \frac{1 + \sum_{\nu=1}^{n} \beta_\nu^2}{\sum_{\nu=1}^{n} \alpha_\nu^2} = \frac{\beta^2}{\alpha^2} = \left(\frac{\beta}{\alpha}\right)^2.$$

From this we can conclude that either γ is a square, or $-\gamma$ is a square, which shows the second property.

Now let us pick any polynomial $f(x) \in F[x]$ with $\deg(f) = 2n+1$, where $n \in \mathbb{N}$. Without loss of generality we may assume f to be monic, since F is a field. The third statement can then be proven by induction with respect to n.

If $n = 0$, then the polynomial is of first degree and thus of the form $f(x) = x - a$, where $a \in F$ is a zero of $f(x)$.

Now let $n \geqslant 1$ and the statement be true for all $g(x) \in F[x]$, $\deg(g) = 2k + 1$, $k \in \mathbb{N}$ and $k < n$. If $f(x)$ is reducible, then it can be written as $f(x) = g(x)h(x)$, where $g(x), h(x) \in F[x]$ are monic and of positive degree strictly smaller than $2n + 1$, and one of them (say $g(x)$)must be of odd degree, since $\deg(f) = \deg(g) + \deg(h)$. By the induction hypothesis, $g(x)$ then has a zero in F, and hence so does $f(x)$.

If $f(x)$ is irreducible, we can form the proper field extension $F(\alpha) = F[x]/(f(x))$, where $\alpha \in F(\alpha)$ is a zero of $f(x)$. We then know that $F(\alpha)$ is not formally real, and thus there exist $q_1(x), \ldots, q_r(x) \in F[x]$ with degree smaller than $2n + 1$ such that:

$$\sum_{\nu=1}^{r} (q_\nu(\alpha))^2 = -1 \in F.$$

This then shows that there exists some $g(x) \in F[x]$ such that:

$$\sum_{\nu=1}^{r} (q_\nu(x))^2 + f(x)g(x) = -1.$$

Now, the degree of the $q_\nu(x)^2$ must be even, and therefore the degree of the sum must be even and positive and strictly less than $4n + 2$. We therefore

conclude that $g(x)$ has odd degree less than or equal to $2n-1$. Therefore $g(x)$ has a zero $\rho \in F$. However, then:

$$-1 = \sum_{\nu=1}^{r} (q_\nu(\rho))^2 + f(\rho)g(\rho) = \sum_{\nu=1}^{r} (q_\nu(\rho))^2.$$

I.e. -1 is a sum of squares in F, leading to a contradiction. Therefore $f(x)$ must be reducible and the third statement has been proven. □

Lemma 3.2.2. *If a field F is real closed, there exists one and only one $P \subseteq F^*$ such that (F, P) is an ordered field. I.e. a real closed field can be uniquely ordered.*

Proof. If F is formally real, then we know that it can be ordered. Let $P \subset F$ be the positive numbers of such an ordering. Then we know that any non-zero square $x^2, x \in F^*$ must be positive.

Now, if F is real closed, it is formally real and can thus be ordered. Also, $\forall x \in F^*\ \exists y \in F^*$ such that $x = y^2$, in which case x must be positive, or $-x = y^2$, in which case $-x$ must be positive, in any ordering. Since this covers all non-zero elements of F, there exists only one ordering, namely the one where exactly all the non-zero squares are positive. □

NOTE

From now on, when we speak of a real closed field, we will implicitly assume that it is equipped with this unique order.

The following result is the analog of the classical Fundamental Theorem of Algebra, and shows that real closed fields capture the important property that we may obtain an algebraically closed field by adjoining a single square root. In particular, this shows that the real numbers $\mathbb{R}$ form a real closed field, since $\mathbb{C}$ is obtained by adjoining $\sqrt{-1}$ and is algebraically closed.

Theorem 3.2.3. *A field F is real closed if and only if it is not algebraically closed, and $C = F(\sqrt{-1}) = F[x]/(x^2+1)$ is algebraically closed.*

Proof. Let F be a real closed field. Then we see that x^2+1 is irreducible, and hence has no zeroes in F, since otherwise -1 would be a sum of squares in F. We can then define the field $C = F[x]/(x^2+1)$. We first define the automorphism $z = a + bi \mapsto \bar{z} = a - bi$ of C, where $i \in C$ denotes a zero (any one of the two) of x^2+1. This induces an automorphism $f(x) \mapsto \bar{f}(x)$ of $C[x]$. We then see that if $f(x) \in C[x]$, then $f(x)\bar{f}(x) \in F[x]$. Also, if $f(x)\bar{f}(x)$ has a zero r in C, then $f(r)\bar{f}(r) = 0$, and hence $f(x)$ has a zero in C.

We now show that every element of C can be written as a square. To this end, let $z = a + bi \in C$. Then $z\bar{z} = a^2 + b^2 \in F$ and non-negative,

so that $\exists \alpha \in F : a^2 + b^2 = \alpha^2$. Also, $\alpha^2 \geqslant a^2$ so that $|\alpha| \geqslant |a|$ and hence $\exists c_1, c_2 \in F$, where we can pick $c_1 c_2$ with the same sign as b, such that

$$c_1^2 = \frac{a + |\alpha|}{2}, \qquad c_2^2 = \frac{-a + |\alpha|}{2}.$$

Also:

$$(2c_1c_2)^2 = 4\frac{a + |\alpha|}{2}\frac{-a + |\alpha|}{2} = -a^2 + (a^2 + b^2) = b^2.$$

We can therefore conclude that $(c_1 + c_2 i)^2 = c_1^2 - c_2^2 + 2c_1c_2 i = a + bi$. This shows that there exists no algebraic extension field E of C with $[E : C] = 2$ (since any quadratic equation is reducible).

With the foregoing in mind, we now let $f(x) \in F[x]$ be a monic polynomial of even degree. We define E to be a splitting field over F of $f(x)(x^2+1)$, such that $C \subseteq E$. Then E is Galois over F (since F is of characteristic 0 and thus any polynomial in $F[x]$ is seperable; hence E is the splitting field of a separable polynomial). We write $|\operatorname{Gal} E/F| = 2^e m$, where m is odd. By Sylow's theorem, $\operatorname{Gal} E/F$ contains a subgroup $\mathcal{H}$ with $|\mathcal{H}| = 2^e$. Let H be the subfield of E containing F corresponding to $\mathcal{H}$ under the Galois pairing. Therefore, $2^e m = [E : F] = [E : H][H : F] = 2^e[H : F]$ so that $[H : F] = m$. But since every polynomial of odd degree in F has a zero in F, F has no proper odd-dimensional algebraic extension fields. Therefore, $m = 1$, $\mathcal{H} = \operatorname{Gal} E/F$, and $H = E$. We can now conclude that because $|\operatorname{Gal} E/F|$ is even, we can obtain E by repeatedly adjoining square roots. However, since we obtained C by adjoining a square root and C contains all possible square roots, we must have that $C = E$. Therefore, C is a splitting field of $f(x)(x^2 + 1)$ and hence contains all zeroes of $f(x)$[4]. This shows that every polynomial in $F[x]$ has a zero in C. By the reasoning above we can then conclude that C is algebraically closed.

We will now go on to show the converse. Let F be a field that is not algebraically closed, but let $C = F(i) = F[x]/(x^2+1)$ be algebraically closed. We then clearly see that $\sqrt{-1} \notin F$, since otherwise $x^2 + 1$ would be reducible and C would not be a field. Now let $a, b \in F$. We can show in the same way as before that every element of C can be written as a square, and so we pick $z \in C$ such that $z^2 = a + bi$. Then $a^2 + b^2 = (a + bi)(a - bi) = z^2\bar{z}^2 = (z\bar{z})^2$ and $z\bar{z} \in F$. This shows that every sum of squares in F can be written as a square. In particular, -1 is not a square, and hence not a sum of squares, so that F is formally real. We can also see that C is an algebraic closure of F (since C is generated by $i = \sqrt{-1}$ with minimum polynomial $x^2 + 1$, so that $[C : F] = 2 < \infty$ and C is algebraically closed), so that every algebraic extension of F is contained within C. But then, C is the only proper algebraic extension field, and C is not formally real (as $i^2 = -1$), so that F is real closed. □

[4]We note that $x^2 + 1$ splits in $C[x]$ as $(x - i)(x + i)$.

3.3 The Intermediate Value Theorem

In this section we will discuss a very important theorem for real continous and differentiable functions that holds in the context of polynomials with coefficients in a real closed field. This is the familiar intermediate value theorem, and it will be the key to our success in the next chapter.

Theorem 3.3.1 (Intermediate Value Theorem)**.** *Let F be a real closed field, $f(x) \in F[x]$, $a, b \in F$ and $a < b$. Then if $f(a)f(b) < 0$, there exists a $c \in F$ such that $a < c < b$ and $f(c) = 0$.*

Proof. From theorem 3.2.3 we already know that the only irreducible polynomials in $F[x]$ are going to be those of degree 1 or 2. Furthermore, a polynomial $x^2 + \alpha x + \beta \in R[x]$ is going to be irreducible if and only if $\alpha^2 - 4\beta < 0$. This follows in the same way as for second degree polynomials with real coefficients.

Now let us pick $f(x) \in F[x]$ to be monic and of positive degree. The general case then follows quickly by dividing out the leading coefficient and by noting that the premise cannot hold for polynomials of degree zero. We can write $f(x)$ in terms of its irreducible factors as:

$$f(x) = \prod_{i=1}^{m}(x - r_i) \prod_{j=1}^{s} g_j(x),$$

where $r_1, \ldots, r_m \in R$ and $g_1(x), \ldots, g_s(x) \in R[x]$ with:

$$g_j(x) = x^2 + a_j x + b_j, \quad a_j^2 - 4b_j < 0, \quad 1 \leqslant j \leqslant s.$$

For $j \in \{1, \ldots, s\}$ we can, by lemma 3.2.1, find $0 < c_j \in R$ such that $c_j^2 = \frac{1}{4}(4b_j - a_j^2)$. We can then write:

$$g_j(x) = \left(x + \frac{a_j}{2}\right)^2 + c_j^2,$$

so that for all $u \in R$, $g_j(u) > 0$.

We first rule out the case that $f(x)$ has no irreducible factors of first degree. If this would be the case, then $f(a)f(b) = \prod_{j=1}^{s} g_j(a)g_j(b) > 0$, contradicting our hypothesis.

Now, if $\forall i \in \{1, \ldots, m\} : a < r_i \wedge b < r_i$, then $f(a)f(b) = \prod_{i=1}^{m}(a - r_i)(b - r_i) \prod_{j=1}^{2} g_j(a)g_j(b) > 0$. Similarly, if $\forall i \in \{1, \ldots, m\} : a > r_i \wedge b > r_i$, then also $f(a)f(b) > 0$. We conclude that there exists a $i \in \{1, \ldots, m\}$ such that $a < r_i < b$ and $f(r_i) = 0$, which concludes the proof. □

The key property in the proof above was that every positive element of R can be written as a square, which is a characteristic property of real closed fields. It turns out that analogues of several other important theorems in real analysis, such as Rolle's Theorem and the Mean Value Theorem, hold for polynomials in a real closed field as well.

Chapter 4

Sturm's Theorem

In this chapter we will study the classical method for determining the number of zeroes of a polynomial with real coefficients that are contained within an open interval, which is based on a theorem by J.C.F. Sturm, published in 1829 [7]. In particular, this method allows us to symbolically locate the zeroes of a polynomial up to an arbitrary precision. We will study this method in the context of real closed fields, which we have shown to encompass the real number system.

We will give two versions of the theorem. The first gives a decision method in terms of variations in sign of a sequence of numbers. The second answers when a parametrized family of polynomials has zero in a certain interval, by reducing it to a set of polynomial equations and inequations for the parameters of the family, where the equations and inequations have integer coefficients. From the last theorem we can then quickly show that if a polynomial with rational coefficients has a zero in one real closed field, it will have a zero in any real closed field.

Throughout this chapter, R will denote a real closed field, equipped with the strict total order $>$. Also, if $a, b \in R$ and $a < b$ we will use the notations $[a, b] = \{ x \in R \mid a \leqslant x \leqslant b \}$ and $]a, b[= \{ x \in R \mid a < x < b \}$ for closed and open intervals respectively.

Most of this chapter draws from [4], but several definitions and theorems have been modified to streamline the discussion and to get some more general results.

4.1 Variations in sign

Definition 4.1.1. Let $(c_0, \ldots, c_n) \in R^{n+1}$ be a sequence of numbers in R. Then the number of variations in sign of this sequence is defined to be

$$| \{ i \in \{ 1, \ldots, n' \} \mid c'_{i-1} c'_i < 0 \} |,$$

where $(c'_0, \ldots, c'_{n'})$ is the subsequence obtained by dropping the zero elements of the original sequence.

Definition 4.1.2. Let $f(x) \in R[x]$ and $a, b \in R$ with $a < b$. Then a *Sturm sequence* for $f(x)$ on $[a, b]$ is a sequence of polynomials $(f_0(x), \ldots, f_s(x)) \in R[x]^{s+1}$ such that $f_0(x) = f(x)$ and:

1. $f_0(a)f_0(b) \neq 0$,
2. $\forall c \in [a, b] : f_s(c) \neq 0$ (i.e. $f_s(x)$ has no zeroes in $[a, b]$),
3. If $c \in [a, b]$ and $f_j(c) = 0$ for some $j \in \{1, \ldots, s-1\}$, then $f_{j-1}(c)f_{j+1}(c) < 0$,
4. If $c \in [a, b]$ and $f(c) = 0$, there exist open intervals $]c_1, c[,]c, c_2[\subset R$ such that $\forall u \in]c_1, c[: f_0(u)f_1(u) < 0$ and $\forall u \in]c, c_2[: f_0(u)f_1(u) > 0$.

In the proposition below we will show that a Sturm sequence can be used to calculate the number of distinct (i.e. not counting multiplicity) zeroes of the polynomial that lie in some open interval.

Proposition 4.1.1. *Let $f(x) \in R[x]$ be of positive degree, $a, b \in R$ with $a < b$, and $(f_0(x), \ldots, f_s(x))$ a Sturm sequence for $f(x)$ on $[a, b]$. For any $c \in [a, b]$, denote the number of variations in sign of $(f_0(c), \ldots, f_s(c))$ as V_c. Then the number of distinct zeroes of $f(x)$ within $]a, b[$ is $V_a - V_b$.*

Proof. Since the number of zeroes of all the $f_i(x)$ within $[a, b]$ is finite, we can write them down as $a = a_0 < a_1 < \cdots < a_m = b$ so that no $f_j(x)$ has a zero in any of the open intervals $]a_{i-1}, a_i[$, $1 \leqslant i \leqslant s$. Now pick for $1 \leqslant i \leqslant m$: $c_i \in]a_{i-1}, a_i[$.

First we see that no $f_j(x)$ has a zero in $]a_0, c_1[$. Then by the negation of theorem 3.3.1 we have $f_j(a_0)f_j(c_1) > 0$ for $j \in \{0, \ldots, s\}$. Now let $k \in \{0, \ldots, s\}$ with $f_k(a_0) = 0$. Then clearly $0 < k < s$, since $f_0(a_0) \neq 0 \neq f_s(a_0)$, and so $f_{k-1}(a_0)f_{k+1}(a_0) < 0$. Then $f_{k-1}(a_0)f_{k+1}(a_0)f_{k-1}(c)f_{k+1}(c) > 0$ implies that $f_{k-1}(c)f_{k+1}(c) < 0$. Taking into account all such k, we get $V_{a_0} = V_{c_1}$. In exactly the same way we may prove that $V_{c_m} = V_{a_m}$.

We now let $i \in 1, \ldots, m-1$. Then if $f(a_i) \neq 0$, we can carry through the same argument to get $V_{c_i} - V_{c_{i+1}} = 0$. If $f(a_i) = 0$, we note that (possibly by repicking our c_i and c_{i+1} to comply with property 4 of a Sturm sequence) $f_0(c_i)f_1(c_i) < 0$ and $f_0(c_{i+1})f_1(c_{i+1}) > 0$. Furthermore, the argument above again shows that if $1 < j < s$, then $f_{j-1}(c_i), f_j(c_i), f_{j+1}(c_i)$ and $f_{j-1}(c_{i+1}), f_j(c_{i+1}), f_{j+1}(c_{i+1})$ have the same number of variations in sign. Therefore in this case $V_{c_i} - V_{c_{i+1}} = 1$.

We can now write:

$$V_a - V_b = (V_a - V_{c_1}) + \sum_{i=1}^{m-1} (V_{c_i} - V_{c_{i+1}}) + (V_{c_m} - V_{a_m}) = \sum_{i=1}^{m-1} \delta_i,$$

where $\delta_i = 1$ if $f(a_i) = 0$ and $\delta_i = 0$ if $f(a_i) \neq 0$. Now since all of the zeroes of $f(x)$ that lie within $]a, b[$ per definition are one of the a_i, we have counted all the zeroes. Therefore, $V_a - V_b$ is the total number of distinct zeroes of $f(x)$ that lie within $]a, b[$. □

Now that we have a method of determining how many distinct zeroes a polynomial has in some open interval, given a Sturm sequence, we will need a method to actually produce a Sturm sequence. If we do this, we have a full-blown algorithm to determine the zeroes of a polynomial in some interval. Even better, if we can find a bound on the absolute values of the zeroes of a polynomial and strategically disect the resulting interval, we can locate the zeroes numerically up to an arbitrary precision! It turns out that we can construct a Sturm sequence in a formalized way, using the Euclidean division algorithm.

Definition 4.1.3. Let $f(x) \in R[x]$ be of positive degree and $f'(x) \in R[x]$ its formal derivative. Then define the following sequence, terminating when $f_{s+1}(x) = 0$:

$$\begin{aligned} f_0(x) &= f(x) \\ f_1(x) &= f'(x) \\ f_{i+1}(x) &= q_i(x) f_i(x) - f_{i-1}(x) \qquad \deg(f_{i+1}) < \deg(f_i),\ 1 \leqslant i \leqslant s \end{aligned} \tag{4.1}$$

where $q_i(x) \in R[x]$. Then $(f_0(x), \ldots, f_s(x))$ is called the *standard sequence* of $f(x)$.

Note: Existence and uniqueness

The polynomials $f_{i+1}(x)$ and $q_i(x)$ exist and are unique by corollary 2.3.2. Note however that we have picked $f_{i+1}(x) = -r(x)$. This is the key in producing a Sturm sequence.

We notice that if $(f_0(x), \ldots, f_s(x))$ is the standard sequence for some $f(x) \in R[x]$, then $f_s(x)$ is a common factor of $f(x)$ and $f'(x)$ and all $f_i(x)$, and any such common factor will be a factor of $f_s(x)$. Temporarily passing to the field of fractions of $R[x]$, we can then define a derived sequence $(g_0(x), \ldots, g_s(x))$ by setting $g_i(x) = f_i(x) f_s(x)^{-1}$ for $0 \leqslant i \leqslant s$ and observing that each $g_i(x) \in R[x]$.

Lemma 4.1.2. *Let $f(x) \in R[x]$ be of positive degree and $(f_0(x), \ldots, f_s(x))$ be its standard sequence. Define the* derived sequence *of $f(x)$ as $(g_0(x), \ldots, g_s(x))$, where $g_i(x) = f_i(x) f_s(x)^{-1} \in R(x)$[1] for $0 \leqslant i \leqslant s$. Then each $g_i(x) \in R[x]$, and the derived sequence is a Sturm sequence for $g_0(x)$ on every interval $[a, b]$ such that $g_0(a) g_0(b) \neq 0$.*

Furthermore, $\forall c \in R : f(c) = 0 \iff g_0(c) = 0$.

[1] $R(x)$ denotes the field of fractions of $R[x]$.

Proof. We showed above that $f_s(x)$ is a common factor of all the $f_i(x)$. Therefore, for every $0 \leqslant i \leqslant s$ we have some $h_i(x) \in R[x]$ such that $f_i(x) = h_i(x)f_s(x)$ and thus $g_i(x) = h_i(x)f_s(x)f_s(x)^{-1} = h_i(x) \in R[x]$.

We will now show that the derived sequence is a Sturm sequence. Let $a, b \in R$ with $a < b$ and $g_0(a)g_0(b) \neq 0$. Then clearly property 1 holds. Furthermore, $g_s(x) = 1$, so that $g_s(x)$ has no zeroes in R and hence not in $[a, b]$. We now use the definition of the standard sequence to see that for $1 \leqslant i \leqslant s$ (where it is understood that $g_{s+1}(x) = 0$:

$$\begin{aligned} g_{i-1}(x) &= f_{i-1}(x)f_s(x)^{-1} \\ &= (q_i(x)f_i(x) - f_{i+1}(x))f_s(x)^{-1} \\ &= q_i(x)g_i(x) - g_{i+1}(x). \end{aligned}$$

Suppose that $c \in [a, b]$ and $g_j(c) = 0$ for $0 < j < s$. Then $g_{j-1}(c)g_{j+1}(c) = q_j(c)g_j(c)g_{j+1}(c) - (g_{j+1}(c))^2 = -(g_{i+1}(c))^2 \leqslant 0$. Also, $g_{j-1}(c) = -g_{j+1}(c)$, so if $g_{j-1}(c) = 0$, then $g_j(c) = 0 = g_{j+1}(c)$ and by induction we can then show that $g_s(c) = 0$, which is not the case. Therefore property 3 holds.

Lastly, suppose that $c \in [a, b]$ and $g_0(c) = 0$. Then $f(c) = g_0(c)f_s(c) = 0$, so there exist $h(x) \in R[x]$ and $e \in \mathbb{N}$ such that $f(x) = (x-c)^e h(x)$, $e > 0$ and $h(c) \neq 0$. Also, $f'(x) = e(x-c)^{e-1}h(x) + (x-c)^e h'(x)$. Therefore, $(x-c)^{e-1}$ is a common factor of $f(x)$ and $f'(x)$ and hence a factor of $f_s(x)$. It follows that there exists a $k(x) \in R[x]$ such that $f_s(x) = (x-c)^{e-1}k(x)$ and $k(c) \neq 0$. Then $h(x) = k(x)l(x)$ and $h'(x) = k(x)m(x)$ for some $l(x), m(x) \in R[x]$ with $l(c) \neq 0 \neq m(c)$. Then $g_0(x) = (x - c)l(x)$ and $g_1(x) = (x - c)m(x) + el(x)$ and thus $g_1(c) = el(c) \neq 0$. We may then choose[2] an interval $[c_1, c_2]$ such that $c \in [c_1, c_2]$ and the interval contains no zeroes of $g_1(x)$ nor $l(x)$. Then by theorem 3.3.1, $g_1(x)l(x) > 0$, so that for $\gamma \in [c_1, c_2]$: $g_0(\gamma)g_1(\gamma) = (\gamma - c)g_1(\gamma)l(\gamma)$ which has the same sign as $\gamma - c$ and thus is negative when $\gamma \in]c_2, c[$ and positive when $\gamma \in]c, c_1[$. Hence property 4 holds and the derived sequence is a Sturm sequence for $g_0(x)$ in $[a, b]$. □

By combining the foregoing lemma and proposition, we may now prove the main result of this section.

Theorem 4.1.3 (Sturm's Theorem)**.** *Let $f(x) \in R[x]$ be of positive degree and $(f_0(x), \ldots, f_s(x))$ its standard sequence. For all $c \in R$, let V_c be the number of variations in sign of $(f_0(c), \ldots, f_s(c))$. Then, if $a, b \in R$, $a < b$ and $f(a)f(b) \neq 0$, the number of distinct zeroes of $f(x)$ in the interval $]a, b[$ is $V_a - V_b$.*

Proof. Let $(g_0(x), \ldots, g_s(x))$ be the derived sequence of $f(x)$. We have seen that $f(x)$ and $g_0(x)$ have the same distinct zeroes, so the derived sequence is a Sturm sequence for $g_0(x)$ on $[a, b]$. Also, since $f(a) \neq 0 \neq f(b)$, neither

[2] E.g. by choosing a random such interval and then filtering out the zeroes of $g_1(x)$ and $l(x)$ by taking the ones closest to c and averaging with c

$(x-a)$ nor $(x-b)$ are common factors of $f(x)$ and $f(x)$. It then follows that $f_s(a) \neq 0 \neq f_s(b)$ and thus the sequences

$$f_i(a) = g_i(a)f_s(a) \quad \text{and} \quad f_i(b) = g_i(b)f_s(b)$$

have the same variations in sign as the $g_i(a)$ and $g_i(b)$ respectively. Now, by the foregoing proposition and the observation above, the number of distinct zeroes of $f(x)$ in $]a,b[$ is equal to the number of distinct zeroes of $g(x)$ in the interval, which is $V_a - V_b$. □

We can use the foregoing result to form a useful algorithm, that runs in polynomial time with respect to the degree of the polynomial in question.

ALGORITHM 3: CALCULATING THE TOTAL NUMBER OF ZEROES OF A POLYNOMIAL

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ be monic and of positive degree. Define $\mu = 1 + \max(1, \sum_{i=0}^{n-1} |a_i|)$. Calculate the standard sequence $(f_0(x), \ldots, f_s(x))$ of $f(x)$ by repetitive use of algorithm 1. For $c \in R$, let V_c denote the number of variations in sign of the sequence $(f_0(c), \ldots, f_s(c))$. Then the total number of distinct zeroes of $f(x)$ in R is $V_{-\mu} - V_{\mu}$.

Proof. We have found in lemma 3.1.10 that all zeroes of $f(x)$ are contained in the interval $[-M, M]$, where $M = \max(1, \sum_{i=0}^{n-1} |a_i|)$. Therefore, all zeroes of $f(x)$ are certainly contained in the open interval $]-\mu, \mu[$, where $\mu = 1 + M$. If we combine this with Sturm's theorem, we get $V_{-\mu} - V_{\mu}$ as the total number of distinct zeroes of $f(x)$. □

Example. We let $f(x) = x^3 + 3x + 1 \in \mathbb{R}[x]$. Then $f'(x) = 3x^2 + 3$ and the Euclidean sequence of $f(x)$ and $f'(x)$ (and thus the standard sequence of $f(x)$ is:

$$\begin{aligned} f_0(x) &= x^3 + 3x + 1 \\ f_1(x) &= 3x^2 + 3 \\ f_2(x) &= -(2x + 1) \\ f_3(x) &= -\frac{15}{4}. \end{aligned}$$

We observe that all zeroes of $f(x)$ will lie in the interval $]-M-1, M+1[$, where $M = \max(1, 4) = 4$. We therefore evaluate the standard sequence at -5 and 5.

$$\begin{aligned} f_0(-5) &= -139 < 0 & \qquad f_0(5) &= 141 > 0 \\ f_1(-5) &= 78 > 0 & \qquad f_1(5) &= 78 > 0 \\ f_2(-5) &= 9 > 0 & \qquad f_2(5) &= -11 < 0 \\ f_3(-5) &= -\frac{15}{4} < 0 & \qquad f_3(5) &= -\frac{15}{4} < 0 \end{aligned}$$

From this we see that $V_{-5} - V_5 = 2 - 1 = 1$, so $f(x)$ has 1 distinct zero in any real closed field.

4.2 Systems of equations, inequations and inequalities

This section serves as a preamble to the next section. We will now develop the notion of a system of equations, inequations and inequalities, which are expressions $v(t_1, \ldots, t_r) = 0$, $v(t_1, \ldots, t_r) \neq 0$, and $v(t_1, \ldots, t_r) > 0$ respectively, where $v \in \mathbb{Z}[t_1, \ldots, t_r]$ for indeterminates $t_i, 1 \leqslant i \leqslant r$. Note that will write $v(t_i)$ for $v(t_1, \ldots, t_r)$ if it is more convenient. We can consider any ordered field F, which will contain $\mathbb{Z}$ as a subring. We then have an evaluation homomorphism $\mathbb{Z}[t_1, \ldots, t_r] \to F$ induced by the inclusion homomorphism, that sends $\mathbb{Z}$ to $\mathbb{Z}$ and t_i to some $c_i \in F$. In this way we can look for solutions of such an expression in the extension field F.

We further note, that if $v(c_1, \ldots, c_r) \neq 0$ and $w(c_1, \ldots, c_r) \neq 0$, then since the solutions of these two inequations are in a field F, we can rewrite this equivalently as $v(c_1, \ldots, c_r)w(c_1, \ldots, c_r) \neq 0$. So, any finite set of inequations can be replaced by a single inequation. We can now state the following definition.

Definition 4.2.1. An *r-system* (of equations, inequations and inequalities) is a triple

$$\begin{aligned}\Gamma &= ((v_1, \ldots, v_s), v_{\neq}, (v_{>1}, \ldots, v_{>u})) \\ &\in \left(\cup_{i=1}^{\infty}\mathbb{Z}[t_1, \ldots, t_r]^{(i)}\right) \times \mathbb{Z}[t_1, \ldots, t_r] \times \left(\cup_{i=1}^{\infty}\mathbb{Z}[t_1, \ldots, t_r]^{(i)}\right).\end{aligned}$$

Moreover, if (F, P) is an ordered field, then the solution set of Γ is the set $\Gamma(F)$ of $(c_1, \ldots, c_r) \in F^{(r)}$ such that:

$$\begin{gathered} v_1(c_i) = \cdots = v_s(c_i) = 0, \\ v_{\neq}(c_i) \neq 0, \\ v_{>1}(c_i), \ldots, v_{>u}(c_i) > 0. \end{gathered}$$

If we wish to specify a system without equalities, we can specify the trivial equality $0 = 0$. Similarly, we can adjoin the trivial inequation $1 \neq 0$ and inequality $1 > 0$. In this chapter, we shall not use inequalities much, and when we do not need them, we shall drop the last term in the triple, assuming the trivial inequality is to be adjoined. Also, when no inequation (the second element in the triple) has been specified, we assume that the trivial inequation must be adjoined.

We can now ask when a set of systems covers all possible cases. The following definition will make this formal.

Definition 4.2.2. An *r-cover* is a finite set of r-systems $\delta = \{\Delta_1, \ldots, \Delta_s\}$ such that for any ordered field F:

$$\bigcup_{\Delta \in \delta} \Delta(F) = F^{(r)}.$$

Also, a *refinement* of an r-cover γ is an r-cover δ, such that for any ordered field F of K: $\forall \Delta \in \delta\ \exists \Gamma \in \gamma : \Delta(F) \subseteq \Gamma(F)$.

Definition 4.2.3. If Γ and Δ are r-systems, their join is defined to be the r-system $\Gamma \sqcap \Delta$[3] that has as its equalities and inequalities both those of Γ and Δ, and as inequality the product of the inequalities of Γ and Δ.

We will give the following lemmas without proof, as they are quite straightforward if you just write out the definitions.

Lemma 4.2.1. *Let Γ and Δ be r-systems. Then:*

$$(\Gamma \sqcap \Delta)(F) = \Gamma(F) \cap \Delta(F),$$

for any ordered field F.

Lemma 4.2.2. *If Γ is an r-system and $\delta = \{ \Delta_1, \ldots, \Delta_s \}$ is a finite r-cover, and we define $\Gamma_j = \Gamma \sqcap \Delta_j$ for $1 \leqslant j \leqslant s$, then $\bigcup_{j=1}^{s} \Gamma_j(F) = \Gamma(F)$ for every ordered field F.*

Lemma 4.2.3. *Let $\gamma = \{ \Gamma_1, \ldots, \Gamma_u \}$ and $\delta = \{ \Delta_1, \ldots, \Delta_s \}$ be r-covers and define $\Gamma'_j = \Gamma_1 \sqcap \Delta_j$. Then $\gamma' = \{ \Gamma'_1, \ldots, \Gamma'_s, \Gamma_2, \ldots, \Gamma_u \}$ is again an r-cover, and a refinement of γ.*

4.3 Sturm's Theorem Parametrized

We will now consider a family of polynomials in a formally real field R whose coefficients are parametrized as multivariate polynomials over its prime ring $\mathbb{Z}$. That is, the family of polynomials is represented by a polynomial in $\mathbb{Z}[t_1, \ldots, t_r][x]$. The t_i represent parameters, and the x represents a variable we wish to solve for. Using Sturm's Theorem we will show that we can, algorithmically, obtain a cover of systems in $\mathbb{Z}$ such that a member of this family has a zero in a certain interval if and only if the parameters and boundaries satisfy one of those systems. This method could be extended to parametrize the systems that the coefficients have to satisfy with respect to the boundaries of the system, but that extension will not be considered here.

In order to get to our main result, we first let $K = \mathbb{Z}$ and R be a real closed field. We also let $r \in \mathbb{N}$, $r \geqslant 1$ and define $A = K[t_1, \ldots, t_r]$, where the $t_i, 1 \leqslant i \leqslant r$ are indeterminates. Now, if we pick $(c_1, \ldots, c_r) \in R^{(r)}$, we have a homomorphism $A \to R$ that extends the inclusion homomorphism $K \to R$ and sends $t_i \mapsto c_i$. Therefore, we have an extension of this homomorphism $A[x] \to R[x]$ that maps each parametrized polynomial to a polynomial with coefficients in F: $F(t_i; x) \mapsto F(c_i; x)$.

[3] This is not standard notation, but it proves intuitive given lemma 4.2.1.

Since A is a commutative ring, we can perfectly well perform Euclidean polynomial division in $A[x]$. If we now make the connection with the evaluation in $(c_1, \ldots, c_r)$ we can make the following important observation.

Lemma 4.3.1. *Let $F(t_i; x), G(t_i; x) \in A[x]$ with $G(t_i; x) \neq 0$ and $v_m(t_i)$ the leading coefficient of G. Then there exists an even $e \in \mathbb{N}$ and $Q(t_i; x), R(t_i; x) \in A[x]$ with $\deg(R) < \deg(G)$ and:*

$$v_m(t_i)^e F(t_i; x) = Q(t_i; x)G(t_i; x) - R(t_i; x).$$

Also, if $(c_1, \ldots, c_r) \in R^{(r)}$ and $v_m(c_i) \neq 0$, then the $q(x), r(x) \in R[x]$ with $F(c_i; x) = q(x)G(c_i; x) - r(x)$ and $\deg(r) < \deg(G(c_i))$ differ from $Q(c_i; x)$ and $R(c_i; x)$ by a common positive multiplier.

We also note that the choice of the $Q(t_i; x), R(t_i; x)$ and e are independent of which real closed field we use.

Proof. The existence of an arbitrary $e \in \mathbb{N}$ and the $Q(t_i; x), R(t_i; x) \in A[x]$ follows from the Euclidean division algorithm. However, if e is odd, we may multiply the entire equation by $v_m(t_i)$ and so obtain a new $\tilde{Q}(t_i; x)$ and $\tilde{R}(t_i; x)$ and an even $\tilde{e}$ so that the equation still holds.

Now, if $(c_1, \ldots, c_r) \in R^{(r)}$ such that $v_m(c_i) \neq 0$, then since e is even we have $v_m(c_i)^e > 0$. Then evaluating the equation in the c_i and dividing by $v_m(c_i)^e$, we obtain:

$$\begin{aligned} F(c_i; x) &= v_m(c_i)^{-e} Q(c_i; x)G(c_i; x) - v_m(c_i)^{-e} R(c_i; x) \\ &= q(x)G(c_i; x) - r(x), \end{aligned}$$

where the $q(x), r(x) \in R[x]$ are as above. And since such $q(x)$ and $r(x)$ are unique in the polynomial ring of a field, we have $Q(c_i; x) = v_m(c_i)^e q(x)$ and $R(c_i; x) = v_m(c_i)^e r(x)$. □

We are now ready to state the following proposition, that allows us to use Sturm's theorem on the parametrized polynomials.

Proposition 4.3.2. *Let $F(t_i; x), G(t_i; x) \in A[x]$ with $G(t_i; x) = \sum_{j=0}^{m} v_j(t_i)x^j \neq 0$. Define $G_k(t_i; x) = \sum_{j=0}^{k} v_j(t_i)x^j$ and the r-systems $\Gamma_k = ((v_j, j > k), v_k)$ for $0 \leqslant k \leqslant m$ and $\Gamma_{-\infty} = ((v_0, \ldots, v_m), 1)$[4]. Then we can obtain, in a finite number of steps, an r-cover $\delta = \{\Delta_1, \ldots, \Delta_h\}$ that is a refinement of the cover $\gamma = \{\Gamma_{-\infty}, \Gamma_0, \ldots, \Gamma_m\}$ and h sequences of polynomials $(F_{j0}(t_i; x), \ldots, F_{js_j}(t_i; x))$ in $A[x]$ such that, if $(c_1, \ldots, c_r) \in \Delta_j(R)$, then the terms of $(F_{j0}(c_i; x), \ldots, F_{js_j}(c_i; x))$ differ from the terms of the Euclidean sequence of $F(c_i; x)$ and $G(c_i; x)$ by a positive multiplier.*

Also, if this property holds in one real closed field, then it holds for any real closed field.

[4]The k and $-\infty$ correspond to the degree of $G(c_i; x)$ if $(c_i) \in \Gamma_k(R)$.

Proof. We consider any $k \in \{0, \ldots, m\}$ with $v_k(t_i) \neq 0$ (or equivalently $\Gamma_k(R) \neq \varnothing$), for else $G_k(t_i; x) = G_j(t_i; x)$ for some $j < k$ and Γ_k would not be contributing to the cover γ. We can then just as well omit Γ_k in our refinement. Now find $Q_k(t_i; x), R_k(t_i; x) \in A[x]$ as in the foregoing lemma. We have to consider two cases.

If $R_k(t_i; x) = 0$, we can take the sequence $(F, G, 0)$ and Γ_k as the corresponding system. This suffices because if $(c_1, \ldots, c_r) \in \Gamma_k(R)$, then $G(c_i; x) = G_k(c_i; x)$ and thus the Euclidean sequence would be $(F(c_i), G_k(c_i))$. Note that we will use this case as an induction basis in the next case.

Now let $R_k(t_i; x) \neq 0$. If $k = m > \deg(F)$, then we see that $R_k(t_i; x) = F(t_i; x)$. We may then obtain the result for $G(t_i; x)$ and $R_k(t_i; x)$, by going through the argument again and seeing that this case is then excluded. Otherwise $\deg(R_k) + \deg(G_k) < \deg(F) + \deg(G)$, so by induction on the sum of the degrees, we may obtain a cover $\delta_k = \{\Delta_{k0}, \ldots, \Delta_{kh_k}\}$ and h_k sequences $(F_{kl0}(t_i; x), \ldots, F_{kls_{kl}}(t_i; x))$ so that the required property holds for $G_k(t_i; x)$ and $R_k(t_i; x)$. We now define $\Gamma_{kl} = \Gamma_k \sqcap \Delta_{kl}$ for $l \in \{0, \ldots, h_k\}$. Then, if $(c_i) \in \Gamma_{kl}(R) \subseteq \Gamma_k(R)$, we have $G_k(c_i; x) = G(c_i; x)$. Also, since $F_{kl0}(c_i; x) = G_k(c_i; x) = G(c_i; x)$ and $F_{kl1}(c_i; x) = -R_k(c_i; x)$, we can take the sequences $(F(c_i; x), F_{kl0}(c_i; x), \ldots, F_{kls_{kl}}(c_i; x))$, whose terms differ from the Euclidean sequence of $F(c_i; x)$ and $G(c_i; x)$ by a positive multiplier, and pair these with the respective Γ_{kl}.

If we now let δ consist of the systems obtained above, and pair these with their respective sequences, including $\Gamma_{-\infty}$ with $(F, 0, 0)$, we have obtained a refinement of γ that satisfies our requirements. We also note now that the choice of the systems and sequences did not depend on the real closed field in question, so that the property holds for any real closed field. □

Example. Let $F(p, q; x) = x^2 + px + q$ and $G(p, q; x) = 2x + p$. We then have $\Gamma_{-\infty}(R) = \Gamma_0(R) = \varnothing$ and $\Gamma_1(R) = R^{(2)}$. We therefore consider only $k = 2$, $G_2(p, q; x) = G(p, q; x)$. We first observe that:

$$2^2 F(p, q; x) = (2x + p)G(p, q; x) - (p^2 - 4q).$$

We therefore set $R_2(p, q; x) = p^2 - 4q$. Now, since $R_2(p, q; x) \in A$, another step (only possible if $p^2 - 4q \neq 0$) will give us the 0 polynomial. We therefore have the 2-cover and corresponding sequences:

$$\begin{aligned} \Gamma_1 : a^2 - 4b = 0 \quad &\leftrightarrow \quad (F, G) \\ \Gamma_2 : a^2 - 4b \neq 0 \quad &\leftrightarrow \quad (F, G, R_2) \end{aligned}$$

If we now recall that the standard sequence of a polynomial $f(x)$ is simply the Euclidean sequence of $f(x)$ and its formal derivative, we can quickly prove the following theorem, which is our second main result. Note that this version is more general than the one in [4], as the systems we have to obtain include requirements on the bounds of our interval.

Theorem 4.3.3 (Parametrized version of Sturm's Theorem)**.** *Let $F(t_i; x) \in A[x]$. Then there exists a finite set of $r+2$-systems*[5] *ω in K – which we can obtain in a finite number of steps – such that for every $(c_1, \ldots, c_r, a, b) \in R^{(r+2)}$ with $a < b$, $F(c_i; x)$ has a zero in $[a, b]$ if and only if $F(c_i; a)F(c_i; b) = 0$ or $F(c_i; a)F(c_i; b) \neq 0$ and there is some $\Omega \in \omega$ such that $(c_1, \ldots, c_r, a, b) \in \Omega(R)$.*

We can restate this theorem as follows: *Let $F(t_i; x)$ be a family of polynomials whose coefficients are parametrized by polynomials with integer coefficients. Then for any interval $]a, b[$ we can obtain a finite set of systems of equations, inequations and inequalities, so that $F(c_i; x)$ has a zero in that interval if and only if the coefficient parameters (c_i) and the boundaries a and b satisfy one of those systems (provided that $F(c_i; a)F(c_i; b) \neq 0$).*

Proof of the parametrized version of Sturm's Theorem, 4.3.3. Let $F(t_i; x) = \sum_{\nu=1}^{n} u_\nu(t_i)x^\nu$, where $u_\nu(t_i) \in A$, and $u_n(t_i)$ is the leading coefficient. Now, if $F'(t_i; x) = 0$, then $F(t_i; x) = u_0(t_i)$ is constant and we can take the sole system $((u_0))$.

We can therefore now assume that $0 \neq F'(t_i; x) = \sum_{\nu=1}^{n} \nu u_\nu(t_i)x^{\nu-1}$. Then by proposition 4.3.2 we can obtain a cover $\delta = \{\Delta_0, \ldots, \Delta_h\}$ and corresponding sequences $(F_{j0}(t_i; x), \ldots, F_{js_j}(t_i; x))$ $(0 \leqslant j \leqslant h)$ such that if $(c_1, \ldots, c_r) \in \Delta_j$, then the terms of $(F_{j0}(c_i; x), \ldots, F_{js_j}(c_i; x))$ differ from the terms of the standard sequence of $F(c_i; x)$ by positive multipliers. In particular, we see that at any point, the number of sign changes is the same.

Now pick any $j \in \{0, \ldots, h\}$. Now, if we let γ be the same cover as in proposition 4.3.2, then δ is a refinement of γ. Therefore, if $(c_i) \in \Delta_j(R)$, we have either $u_n(c_i) = \cdots = u_1(c_i) = 0$ – in which case $F(c_i; x)$ has a zero if and only if $u_0(c_i) = 0$ – or there is some $k \in \{1, \ldots, n\}$ such that $u_k(c_i) \neq 0$ but $u_l(c_i) = 0$ for $l > k$. In the first case we set $\omega_j = \{((u_0))\}$: the sole equation $u_0 = 0$. In the latter case we may construct the following two sequences:

$$\alpha_{jl}(t_i; x_a, x_b) = u_m(t_i)^{2n_l} F_{jl}(t_i; x_a) \in A[x_a, x_b]$$
$$\beta_{jl}(t_i; x_a, x_b) = u_m(t_i)^{2n_l} F_{jl}(t_i; x_b) \in A[x_a, x_b],$$

for $0 \leqslant l \leqslant s_j$, and where $n_l = \deg(F_{jl})$ and x_a and x_b are new indeterminates. Then all the $\alpha_{jl}(c_i; a, b)$ and $\beta_{jl}(c_i; a, b)$ differ from $F_{jl}(c_i; a)$ and $F(c_i; b)$ respectively – and hence from the standard sequence of $F(c_i; x)$ at those points – by a positive multiplier. If $F(c_i; a)F(c_i; b) \neq 0$, we now conclude by Sturm's Theorem that $F(c_i; x)$ has a zero in $]a, b[$ if and only if the number of variations in sign of the sequences $(\alpha_{j0}(c_i; a, 0), \ldots, \alpha_{js_j}(c_i; a, 0))$ and $(\beta_{j0}(c_i; 0, b), \ldots, \beta_{js_j}(c_i; 0, b))$ are not equal. We therefore now take all

[5] The 2 extra parameters in the systems of ω correspond to the bounds of our interval. They serve to keep the set of systems independent of the real closed field that we choose to use.

possible $r+2$-systems on K that can be formed by the elements of those sequences (which is finite), and filter out the ones that lead to a difference in the number of variations in sign between the sequences and for each take the join with Δ_j[6], to form the set of systems ω_j. Then, if a $(c_i; a, b) \in \Omega(R)$ for some $\Omega \in \omega_j$, then $(c_i) \in \Delta_j(R)$, so that the above applies, and there is a difference between the variation in sign in the sequences $(\alpha_{jl}(c_i, a, 0))$ and $(\beta_{jl}(c_i, 0, b))$, so that $F(c_i; x)$ has a zero in $]a, b[$, provided that $F(c_i; a)F(c_i; b) \neq 0$. We also observe that if $F(c_i; a)F(c_i; b) = 0$, then $F(c_i; x)$ has a zero in $[a, b]$.

If we now let $\omega = \cup_{j=0}^{h} \omega_j$, we obtain the set of $r+2$-systems we require, since δ is a cover of K. □

Example. In our last example we obtained a 2-cover and the corresponding sequences $F(p, q; x) = x^2 + px + q$ and $F'(p, q; x) = 2x + p$. We write:

$$\begin{aligned} \Delta_1 : p^2 - 4q = 0 \quad &\leftrightarrow \quad (F, F') \\ \Delta_2 : p^2 - 4q \neq 0 \quad &\leftrightarrow \quad (F, F', p^2 - 4q). \end{aligned}$$

We can then define the corresponding α_{jl} and β_{jl} as follows:

$$\begin{aligned} \alpha_{10}(p, q; x_a, x_b) &= x_a^2 + px_a + q & \beta_{10}(p, q; x_a, x_b) &= x_b^2 + px_b + q \\ \alpha_{11}(p, q; x_a, x_b) &= 2x_a + p & \beta_{11}(p, q; x_a, x_b) &= 2x_b + p \end{aligned}$$

$$\begin{aligned} \alpha_{20}(p, q; x_a, x_b) &= x_a^2 + px_a + q & \beta_{20}(p, q; x_a, x_b) &= x_b^2 + px_b + q \\ \alpha_{21}(p, q; x_a, x_b) &= 2x_a + p & \beta_{21}(p, q; x_a, x_b) &= 2x_b + p \\ \alpha_{22}(p, q; x_a, x_b) &= p^2 - 4q & \beta_{22}(p, q; x_a, x_b) &= p^2 - 4q \end{aligned}$$

For Δ_1 we get the sole system $\Omega_{11} = ((p^2 - 4q), 1, (-(x_a^2 + px_a + q)(2x_a + p), (x_b^2 + px_b + q)(2x_b + p)))$, that is, α_{1l} will change sign, but β_{1l} will not.

For Δ_2, we have to consider three cases: the α_{2l} change sign once, and the β_{2l} don't (one zero), the α_{2l} change sign twice, and the β_{2l} don't (two zeroes), or the α_{2l} change sign twice and the β_{2l} change sign once (one zero). These cases can all occur in several ways, and so we end up with a whole pile of systems.

NOTE: EXISTENCE OF A ZERO

We have introduced two extra indeterminates in our systems in order to account for the zeroes of our polynomial. However, if we choose to investigate the problem of the existence of a zero in the entire field, we can drop those two parameters. This can be done by noting that we do not have to consider a and b up to the point that we define the sequences $(\alpha_{jl}(c_i))$ and $(\beta_{jl}(c_i))$. In particular, at that point we can see that for any $(c_i) \in R^{(r)}$, if $\rho \in R$ is to be a zero of $F(c_i; x)$, then necessarily $-\mu < \rho < \mu$,

[6]Technically, we now have to transform the r-system Δ_j to an $r+2$-system by using the inclusion homomorphism $A \to A[x_a, x_b]$ on all the elements of the system.

where $\mu = (k+1) + \sum_{\nu=0}^{m-1} u_\nu(c_i)^2 u_k(c_i)^{-2}$. We may from that point on let $a(t_i), b(t_i) \in A$ depend on the parameters and modify the $\alpha(t_i)$ and $\beta(t_i)$ accordingly, and finish the argument in the same way. We can therefore state the following corollary.

Corollary 4.3.4. *Let $F(t_i; x) \in A[x]$. Then we can construct a finite set of r-systems ω in K such that for any real closed field R, and $(c_1, \ldots, c_r) \in R^{(r)}$: $F(c_i; x)$ has a zero in R if and only if $(c_1, \ldots, c_r) \in \Omega(R)$ for some $\Omega \in \omega$.*

Restated: *Let $F(t_i; x) \in A[x]$ be a family of polynomials whose coefficients are parametrized by polynomials with integer coefficients. Then we can construct a finite set of systems of polynomial equations, inequations and inequalities with integer coefficients – independent of the real closed field in question – so that for some choice (c_i) of the parameters, $F(c_i; x) \in R[x]$ has a zero in R if and only if the (c_i) satisfy one of the constructed systems.*

Now let $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ and let $F(t_i; x) = \sum_{i=0}^{n} t_i x^i$. We then see that $F(a_i; x) = f(x)$. Suppose that all the $a_i \in \mathbb{Q} \subset R$ and that $f(x)$ has a zero in R. Then by corollary 4.3.4 we can construct a set of n-systems in $\mathbb{Z}$ such that the (a_i) satisfy one of those systems. Now let R' be another real closed field. Then clearly all $a_i \in R'$ (by an isomorphism of the prime fields) and they still satisfy one of those systems. Therefore, the corresponding polynomial in $R'[x]$ will also have a zero in R'.

Corollary 4.3.5. *If a polynomial $f(x)$ with rational coefficients has a zero in one real closed field, it will have a zero in any real closed field.*

This last corollary is i.a. of the utmost importance for computer calculations. E.g. the computable numbers, described by Turing as "the numbers whose expressions as a decimal are calculable by a machine"[9], can be shown to be real closed[2]. This then gives the result, that a polynomial with rational coefficients has a zero in the real numbers, if and only if it has a zero in the computable numbers. Therefore, for any polynomial with rational coefficients, we are in principle able to compute all its real zeroes with a computer (or any realization of a Turing machine).

4.3.1 Tarski's Principle

The question now naturally arises whether we can generalize this procedure to families of polynomials in multiple indeterminates. The answer turns out to be positive. The idea we can pursue is to replace an equation in multiple indeterminates to a set of equations in one less indeterminates. We may go on with this procedure to eventually obtain a set of equations that have to be satisfied for the original equation to be solvable. If we then invoke the parametrized version of Sturm's Theorem for each of these, we obtain a set of systems that will have to be satisfied by the parameters for our equation to be solvable. [4, Sec. 5.6]

This method has an important application in the so-called field of metamathematics, where the properties of mathematics itself are studied. In particular, it implies that every "elementary" sentence in the logic of a real closed field is decidable. This was shown by Tarski in 1948 for the real numbers. [8] Note that in the logic of a real closed field, we mean the first-order logic that remains when only the axioms of the field itself are assumed. Set-theoretic sentences are not allowed. This does however, to quote Tarski, "gives the mathematician the assurance that he will be able to solve every such problem (an elementary problem in a real closed field) by working at it long enough." And with that assurance we can continue to make algebraic exercises for high school students.

Epilogue

Sturm's Theorem has provided us with a very simple way to determine the zeroes of a polynomial that lie within a certain interval. It is interesting to note that despite the simplicity of this method, it is not widely taught in undergraduate calculus courses. Perhaps this can be attributed to the inefficiency of the algorithm compared to more modern root-finding methods, the amount of algebra involved, or simply its age (almost 200 years!). In either case I would like to express my hopes that the tides could change in this respect.

Nevertheless, the theorem not only provides us with this calculation method, it also leads to several important theoretical implications. As examples we have seen the decidability of the theory of real closed fields (in metamathematics), and the fact that if a polynomial with rational coefficients is going to have a zero in one real closed field, then it is going to have one in every real closed field. The last result finds an application in computer science, where we can conclude that we can compute every zero of a polynomial with rational (even computable!) coefficients with a computer program.

I have personally enjoyed this project very much due to the large amount of new algebra I have come to learn, and the discovery of an obscure, but fun and useful result. I know that I will definitely have use for Sturm's Theorem in the future.

Lastly, I would like to acknowledge Prof. Dr. Jaap Top and Dr. Ramsay Dyer for their support during the course of this project. Prof. Top has recommended this project, and they have both provided me with very useful feedback on the report, for which I am very grateful.

Bibliography

[1] E. Artin and O. Schreier. Algebraische konstruktion reele körper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):85–99, December 1927. Conference proceedings from June 1926.

[2] M. Braverman. On the complexity of real functions. In *Proceedings of the 2005 46th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, 2005.

[3] D.J. Griffiths. *Introduction to Quantum Mechanics*. Pearson Education, 2nd edition, 2005.

[4] N. Jacobson. *Basic Algebra*, volume 1. Dover, dover edition, 2009.

[5] N. Jacobson. *Basic Algebra*, volume 2. Dover, dover edition, 2009.

[6] J.P. Serre. Extensions de corps ordonnés. In *Comptes rendus des séances de l'Académie des Sciences*, pages 576–577, September 1949.

[7] J.C.F. Sturm. Mémoire sur la résolution des équations numériques. *Bulletin des Sciences de Férussac*, 11:419–425, 1829.

[8] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. RAND Corporation, 1948.

[9] A.M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42:230–265, 1937.