CONSTRUCTING ROOTS OF POLYNOMIALS OVER THE COMPLEX NUMBERS

Wim Ruitenburg

Department of Mathematics, Statistics and Computer Science
Marquette University
Milwaukee, WI 53233

§0. Introduction

Constructive proofs of the Fundamental Theorem of Algebra are known since 1924, when L. E. J. Brouwer, B. de Loor, and H. Weyl showed that nonconstant monic polynomials over the complex numbers have a complex root. Later that year Brouwer generalized this result by showing that each polynomial $f(X)$ having an invertible coefficient for some positive power of X has a root. These proofs are constructive equivalents of classical analytical proofs of the Fundamental Theorem. Modern versions of their results are in [1, pp. 156ff] and [12, pp. 434ff]. The time has come to give a constructive algebraic proof.

In [7] the authors use algebraic methods to show that the algebraic closure $\mathbf{C}^a$ of the field of rationals $\mathbf{Q}$ in the field of complex numbers $\mathbf{C}$ is algebraically closed and dense in $\mathbf{C}$. In the exercises it is indicated how one can construct roots of monic polynomials over the complexes more generally [7, p. 191]. There is, however, no indication how to accomplish this without resorting to some choice principles, or how to generalize this to polynomials of which it is only known that the coefficient of some positive power of X is invertible. We show that the more general version is indeed provable, and without resorting to choice principles.

We have two target audiences in mind: Constructivists and computer algebraists. To accommodate the former we present the algebraic results in more detail than would otherwise be necessary. For the latter, we will presently discuss some aspects of constructive mathematics, how it relates to algorithms, and why avoiding choice principles matters to us.

There exist several schools of constructive mathematics, the most well-known being Brouwer's intuitionism, Markov constructivism, and Bishop constructivism [2]. Modern followers, however, do not always closely adhere to the philosophies of the originators, so many 'dialects' developed, some of these motivated by the existence of models for constructive logic. The mathematics we use is based on the constructive logic that holds for all topos models [5], and is also called intuitionism. This intuitionism is essentially stricter than the constructivisms mentioned above, so our results hold in all topos models, and are acceptable to most constructivists at the same time. The most important restriction is the lack of choice principles. Fortunately, only a small amount of knowledge of intuitionism is required for understanding the constructive proofs of the Fundamental Theorem.

A clear illustration of where constructivism differs from classical mathematics is in proving statements of the form "there exists x such that $A(x)$." Classically it suffices to show that it is impossible that there is no x for which $A(x)$ holds. A constructive proof must construct x as well as a proof of $A(x)$. In particular, a constructive proof of "A or B" must consist of a proof of A or a proof of B. If B is the statement "not A", then a constructive proof of "A or not A" means either proving A, or proving that assuming A leads to an absurdity. Such proofs cannot always be found. So the Principle of the Excluded Middle fails.

There is a difference between proving "not A" and showing that A cannot be proven. We illustrate this through examples. It is well-known that constructive proofs have computational content. So if there is a constructive proof of the existence of a function $f\colon \mathbf{N} \to \mathbf{N}$ such that $A(n, f(n))$ holds for all natural numbers $n \in \mathbf{N}$, then, by classical techniques outside the realm of constructivism, one can show that f is a computable function. On one hand, if by classical means we know that there is no computable function f such that $A(n, f(n))$ holds for all n, then we know that "there exists f such that $A(n, f(n))$ for all n" cannot be proven. On the other hand, a *constructive* proof of the negation of this statement implies that the negation also holds in classical mathematics: There is no solution f whatsoever. Let us identify Turing machines with natural numbers by some primitive recursive bijective encoding. By the Halting Theorem there is no computable function f such that $f(n) = 0$ exactly when Turing machine n halts, but there are noncomputable ones. So it cannot be shown constructively that such a function exists, and it cannot be shown constructively that such a function does not exist. Another example, also based on the Halting Theorem, says that there is no constructive proof to decide for all binary sequences $\alpha\colon \mathbf{N} \to \{0, 1\}$ whether $\alpha(n) = 1$ for some n.

The three constructive schools mentioned above accept certain choice principles that are at least as strong as the simple axiom of Countable Choice. The simple axiom of *Countable Choice* says that if $A(m, n)$ is a statement about natural numbers m, n such that for all m there exists n with the property that $A(m, n)$ holds, then there exists a function f such that $A(m, f(m))$ holds for all m. [1] and [12], in their proofs of the Fundamental Theorem of Algebra, make essential use of choice principles extending Countable Choice. Although not explicitly stated, the construction of the algebraic closure $\mathbf{C}^a$ in [7] does not make essential use of any choice principles. By avoiding choice principles, results will hold in all topos models. This implies that if we are able to construct a solution x of an equation $f(x) = 0$ over the (Dedekind) reals using topos intuitionism, then x is locally continuous in the parameters of the equation. So, for example, we cannot show the existence of a solution of $X^3 + pX + q = 0$ over the (Dedekind) reals when (p, q) is close to $(0, 0)$, because it would imply the existence of a continuous solution $X(p, q)$ in a neighborhood of $(0, 0)$ [6]. For the same reason we cannot find a solution to the equation $X^2+c=0$ over the (Dedekind) complex numbers when c is near 0. With Countable Choice, however, one can find solutions. So if we allow the use of Countable Choice, then continuity of solutions in the parameters is no longer guaranteed.

The lack of choice principles does not prevent us from constructing functions. Suppose that $A(m,n)$ is a statement for which we can prove that for all $m \in \mathbf{N}$ there exists a least n for which $A(m,n)$ holds. Define f by $f(m) =$ the least n for which $A(m,n)$ holds. Then $A(m,f(m))$ holds for all m. The key distinction is that we are able to give a finite description that uniquely defines f.

Constructive mathematics without choice principles is stricter than 'computable' mathematics. Its constructive nature more than allows us to construct algorithms from the constructive proofs: It also proves the correctness of the algorithms. These implicit algorithms, however, are usually grossly inefficient since in practice constructivists concentrate on abstractness and generality rather than on the computational complexity of their results.

In §1 we prove the existence of algebraic closures of countable discrete fields (Poor Man's Algebraic Closure). In §2 these are used to construct algebraic closures of countable factorial discrete fields (Rich Man's Algebraic Closure). Within such algebraic closures we can factor nonzero polynomials into irreducible factors over many subfields. We apply these results to $\mathbf{Q}$ and, in §3, establish isomorphisms with the algebraic closure $\mathbf{C}^a$ of $\mathbf{Q}$ in $\mathbf{C}$. Then we use the algebraic closedness of $\mathbf{C}^a$ to show that many more polynomials over $\mathbf{C}$ have roots in $\mathbf{C}$, strengthening the results of [1] and [12].

§1. The Poor Man's Algebraic Closure

It is not necessary to recapitulate all of algebra just because we use constructive methods. It is easily seen that many basic results from classical algebra are constructive. Therefore we concentrate on the less obvious results, or results that require an original proof, together with some glue to create one coherent presentation.

First and foremost, sets need not be discrete. A set is *discrete* if for all of its elements a, b we can determine whether $a = b$ or not. The natural numbers $\mathbf{N}$, integers $\mathbf{Z}$, and rationals $\mathbf{Q}$ are discrete sets. Obviously, polynomial rings $R[X]$ over a discrete commutative ring R are also discrete. But the reals $\mathbf{R}$ are not: For a real to exist it suffices, for each natural number $m > 0$, to be able to give a rational interval of length at most $1/m$ 'in which the real number lies,' see §3. For each Turing machine we can construct a sequence $\{a_n\}_n$ by setting $a_n = 1/n$ if the machine does not stop in n steps, and $a_n = 1/m$ if the machine stops in $m \leq n$ steps. As a Cauchy sequence, $\{a_n\}_n$ determines a real number. By the Halting Theorem, we cannot show for each Turing machine whether the limit of its corresponding sequence $\{a_n\}_n$ equals 0 or not.

A discrete set is *finite* if there exists a bijection with an initial segment $\{0,\ldots,n-1\}$ of $\mathbf{N}$. The empty set (if $n=0$) is finite. Finite combinatorial theorems are essentially constructive. This is true for all finite group theory that we will need, including Sylow's Theorem. Some caution is required, though. Exceptions are statements like 'each subgroup of a finite group is finite.' For example, let $G = \{0,1\}$ be the group of two elements, and let H be the subgroup of G generated by the image of a binary sequence $\{a_n\}_n$. Then $H = G$ if and only if $a_n = 1$ for some n, and $H = \{0\}$ if $a_n = 0$ for all n. By the Halting Theorem, such a choice cannot always be made constructively.

In classical mathematics, groups, rings, and modules are defined by simple universal equational axioms like, for rings, $x(y+z) = xy+xz$. In constructive algebra we use the same schemas to axiomatize them. A ring is nontrivial when 1 is not equal to 0.

We do not require equality on groups, rings, and modules to be discrete. This creates problems when we want to define integral domain and field. In the case of integral domains, an axiom saying that from $xy = 0$ one can conclude $x = 0$ or $y = 0$ is too restricting because of the difficulty of establishing "or": Even the real numbers cannot be shown to satisfy this axiom. Instead, one has a binary relation $x \neq y$ on the ring, classically usually equivalent to "$x = y$ is false." On $\mathbf{R}$ and $\mathbf{C}$ we define $x \neq y$ if and only if $x - y$ is a unit. Being nonzero and being a unit cannot be shown to be the same. An integral domain then satisfies: If $x \neq 0$ and $y \neq 0$, then $xy \neq 0$. Similarly, $\mathbf{R}$ and $\mathbf{C}$—obviously—satisfy the field property: If $x \neq 0$, then x is a unit. The technical problems with inequalities grow fast, and we refer the reader to [7, pp. 41ff] and [9] for further details and developments. When we restrict ourselves to discrete structures, we avoid these problems because we can use the classical definitions: A discrete nontrivial commutative ring is a *discrete domain* if for all x, y such that $xy = 0$ we have $x = 0$ or $y = 0$. A discrete domain is a *discrete field* if all nonzero elements are units. One easily verifies that the standard construction of a quotient field of a discrete domain produces a discrete field.

One easily verifies that elementary finite-dimensional linear algebra over discrete fields (rank of a matrix, finite-dimensional null spaces and ranges, Gaussian elimination, determinant) is constructive. If A is a square matrix over a discrete field k, then the commutative matrix ring $k[A]$ is discrete. The *characteristic polynomial* of A is the polynomial $f(X) = \det(X - A)$ over $k \subseteq k[A]$. For all invertible S, $\det(X - A) = \det(X - S^{-1}AS)$. The *eigenvalues* of A are the roots of $f(X)$ in k or in a discrete field extension of k. The construction of roots of polynomials over discrete extension fields is a nontrivial matter. Even the existence of such roots is not guaranteed [7, p. 153], unless the base field k is countable (Theorem 1.6).

A module over a commutative ring R is *finite-rank free* if it is isomorphic to R^n, for some $n \in \mathbf{N}$.

1.0 Proposition (Cayley-Hamilton). *Let R be a commutative ring, and $f(X)$ be the characteristic polynomial of an endomorphism α of a finite-rank free R-module. Then $f(\alpha) = 0$.*

PROOF: For an algebraic proof, see [7, p. 72]. ⊣

Proposition 1.0 allows for a non-algebraic proof. Let A be an $n \times n$ matrix with variables $X_{i,j}$ as entries. Then the characteristic polynomial $f(A)$ over $\mathbf{Z}$ in n^2 variables reduces to 0, as is shown by classical means. A general theorem of logic says that the same reduction must work constructively. There are several results below that can be reduced to trivialities using general theorems from logic. We refrain from using these methods so as to increase the accessibility of our results.

A polynomial over a commutative ring is *monic* if it has leading coefficient 1. A polynomial $f = a_n X^n + \cdots + a_0$ has *degree at most* n, and *degree less than* m for all $m > n$. We may not know the degree of a polynomial, because we may not know whether a 'leading' coefficient equals 0 or not. Naturally, monic polynomials and polynomials over discrete commutative rings have a degree.

An R-module M is *faithful* if $rM = 0$ implies $r = 0$, for all $r \in R$.

1.1 Proposition. *Let $R \subseteq S$ be commutative rings, and $\alpha \in S$. Then the following are equivalent:*

(1) *α satisfies a monic polynomial of degree n over R.*
(2) *$R[\alpha]$ is generated by n elements as an R-module.*
(3) *S has a faithful R-submodule M, generated by n elements, such that $\alpha M \subseteq M$.*

Proof: Obviously, (1) implies (2), and (2) implies (3). Suppose (3) holds, and let $m_1, \ldots, m_n$ generate M. There are $\beta_{i,j} \in R$ such that $\alpha m_j = \sum_i \beta_{i,j} m_i$. Let f be the characteristic polynomial of the matrix $\{\beta_{i,j}\}$. Then $f(\alpha)M = 0$, so $f(\alpha) = 0$. So (1) holds. $\dashv$

A commutative ring $S \supseteq R$ is called *integral* over the commutative ring R if all $s \in S$ are roots of monic polynomials over R. From Proposition 1.1 it now follows that if α is root of a monic polynomial over R, then so are all elements of $R[\alpha]$. We say that α is *integral* over R if $R[\alpha]$ is integral over R. If R is a discrete field, then—following tradition—we commonly use the term *algebraic* instead of *integral*.

1.2 Proposition. *Let $R \subseteq S$ be commutative rings, and let $\alpha, \beta \in S$ be such that α is integral over R, and β is integral over $R[\alpha]$. Then $R[\alpha, \beta]$ is integral over R. The elements of S that are integral over R form a subring.*

Proof: It suffices to prove the first claim: $R[\alpha, \beta]$ is a finitely generated module over $R[\alpha]$, and $R[\alpha]$ is a finitely generated module over R. Multiplication of the generators of the two extensions yields a finite set of generators of $R[\alpha, \beta]$ as module over R. $\dashv$

1.3 Proposition. *Let R, S be commutative rings such that S is a finitely generated integral ring extension of R. Then S is a finitely generated R-module.*

Proof: There exist rings $R_0 \subseteq R_1 \subseteq \cdots \subseteq R_n$ such that $R_i = R[a_1, \ldots, a_i]$, and $R_n = S$. Then R_{i+1} is a finitely generated R_i-module, for all i. Multiplication of the generators from the different extensions produces a finite set of generators for $R_n = S$ as module over $R_0 = R$. $\dashv$

1.4 Proposition. *Let $R \subseteq S \subseteq T$ be commutative rings such that $T \supseteq S$ and $S \supseteq R$ are integral extensions. Then $T \supseteq R$ is integral.*

Proof: For each $\alpha \in T$ there is a monic polynomial $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ over S such that $f(\alpha) = 0$. Let $S' = R[a_1, \ldots, a_n]$. Then $S'[\alpha]$ is a finitely generated module over S', and S' is a finitely generated module over R. So $S'[\alpha]$ is finitely generated as module over R. Thus α is integral over R. $\dashv$

A set S is *countable* if there exists a function $s\colon \mathbf{N} \to S$ from the natural numbers onto S, that is, $S = \{s_0, s_1, s_2, \dots\}$.

A subset $Y \subseteq X$ is called *detachable* from X if for all $x \in X$ we can decide whether $x \in Y$ or $x \notin Y$, that is, x is not an element of Y. So a commutative ring R is discrete exactly when $\{0\}$ is detachable from R. More generally, an ideal $I \subseteq R$ is detachable from R if and only if the quotient ring R/I is discrete.

Countable discrete sets may be finite or (countably) infinite, but we cannot always know which one. For example, let $p_0, p_1, \dots$ be the ascending sequence of prime numbers, and let $\{a_n\}_n$ be a binary sequence with at most one 1. Let $P \subseteq \mathbf{Z}$ be the ideal generated by the sequence of elements $\{a_n p_n\}_n$. One easily verifies that P is a prime ideal that is detachable from $\mathbf{Z}$. The quotient ring $R = \mathbf{Z}/P$ is countable, but, by the Halting Theorem, we may not know whether it is finite or not. We may not know its characteristic either. The quotient field of R is a countable discrete field whose characteristic we cannot determine.

1.5 Proposition. *Let R be a countable commutative ring whose finitely generated ideals are detachable, and let I be a proper finitely generated ideal. Then I is contained in a maximal ideal that is detachable from R.*

Proof: $R = \{r_0, r_1, \dots\}$ for some enumeration r. Construct a sequence of finitely generated ideals $I_0 \subseteq I_1 \subseteq \dots$ as follows: Set $I_0 = I$; if $I_j + r_j R = R$, then set $I_{j+1} = I_j$, otherwise set $I_{j+1} = I_j + r_j R$. Let $M = \bigcup_j I_j$. Then $r_j \in M$ if and only if $r_j \in I_{j+1}$. So M is a detachable maximal ideal. $\dashv$

1.6 Theorem. *Let f be a nonconstant polynomial over a countable discrete field k. Then there is a countable discrete field $E \supseteq k$ and $\alpha \in E$ such that $f(\alpha) = 0$.*

Proof: By the Euclidean Algorithm all finitely generated ideals of the countable ring $k[X]$ are principal and detachable. So f is contained in a detachable maximal ideal M. Set $E = k[X]/M$. $\dashv$

Let $\{a_n\}_n$ be a binary sequence, and let k be the countable discrete field extension of $\mathbf{Q}$ generated by the sequence $\{a_n\sqrt{2}\}_n$. Then we may not know the factorization of $X^2 - 2$ over k. So in general one cannot give a minimal polynomial for α in Theorem 1.6.

A discrete field K is a *splitting field* for a monic polynomial f over a discrete field k if there exist $a_1, \dots, a_n \in K$ such that $f = (X - a_1) \dots (X - a_n)$ and $K = k[a_1, \dots, a_n]$. Repeated application of Theorem 1.6 now gives:

1.7 Theorem. *Let f be a monic polynomial over a countable discrete field k. Then there exists a countable discrete splitting field for f over k.* $\dashv$

In general one cannot show that countable discrete splitting fields are uniquely determined up to isomorphism [7, pp. 153ff].

The construction in the proof of Proposition 1.5 depends on the enumeration of the ring R. Different enumerations may give different maximal ideals. To avoid choice principles when we use Theorem 1.7 in the proof of the theorem below, we need to choose some canonical method to construct one unique splitting field K with enumeration from a given discrete field k with enumeration. Let $\{a_0, a_1, \dots\}$ be an enumeration of a countable discrete field k. Then the *canonical enumeration* of $k[X]$ (based on $\{a_n\}_n$) is the one that lists, for $i = 1, 2, \dots$ successively, all polynomials of degree at most i in the coefficients $a_0, a_1, \dots, a_i$ in lexicographical order with the leading term considered most significant. If we use the canonical enumeration, then, for all $f \in k[X]$, the field extension $k[\alpha]$ of Theorem 1.6 is uniquely determined, and $k[\alpha]$ receives its (canonical) enumeration from $k[X]$. Repeating this process, using canonical enumerations at each step, the splitting field of Theorem 1.7 is uniquely determined by the enumeration of k, and by f.

1.8 Theorem (Poor Man's Algebraic Closure). *Each countable discrete field k is contained in a countable discrete field that is algebraically closed and algebraic over k.*

Proof: Let $f_0, f_1, \dots$ be an enumeration of the monic polynomials over k. Construct a chain of countable discrete fields $k_0 \subseteq k_1 \subseteq \dots$ by setting $k_0 = k$, and by letting k_{i+1} be the canonical splitting field of f_i over k_i. Let $\Omega = \bigcup_i k_i$. Clearly, Ω is countable, discrete, and an algebraic field extension of k. Let f be a monic polynomial over Ω. By Proposition 1.6 there is a countable discrete field extension $E \supseteq \Omega$ such that $f(\alpha) = 0$ for some $\alpha \in E$. By Proposition 1.4 α is algebraic over k. So $f_i(\alpha) = 0$ for some i. But f_i splits in $k_{i+1} \subseteq \Omega$. Thus $\alpha \in \Omega$. $\dashv$

Note that the special construction of k_{i+1} from k_i enables us to avoid choice principles in the construction of Ω, since all k_i are uniquely determined by any enumeration of $k_0 = k$. By the uniqueness of the k_i, the union Ω is uniquely determined.

Splitting fields cannot be uniquely determined up to isomorphism, so one cannot show that countable discrete algebraic closures of a discrete field k are uniquely determined up to isomorphism.

1.9 Corollary. *The field $\mathbf{Q}$ of rational numbers has a countable discrete algebraic closure.* $\dashv$

In §2 we will show that for $\mathbf{Q}$ countable discrete algebraic closures are unique up to isomorphism.

§2. The Rich Man's Algebraic Closure

A discrete domain R is a GCD-*domain* if for all $a, b \in R$ there exists a greatest common divisor $c = \mathrm{GCD}(a, b)$. Obviously, c is unique up to a unit, and GCD-domains satisfy the familiar equations [7, pp. 108ff]

$$\mathrm{GCD}(\mathrm{GCD}(a,b),c) = \mathrm{GCD}(a,\mathrm{GCD}(b,c));$$
$$c \cdot \mathrm{GCD}(a,b) = \mathrm{GCD}(ca,cb);$$
$$\text{if } x = \mathrm{GCD}(a,b), \text{ then } \mathrm{GCD}(a,bc) = \mathrm{GCD}(a,xc); \quad \text{and}$$
$$\text{if } a \mid bc \text{ and } \mathrm{GCD}(a,b) = 1, \text{ then } a \mid c.$$

All equations are up to a unit. Equality-up-to-a-unit need not be a discrete equality relation on the equivalence classes. (Consider, for example, the subring of $\mathbf{Q}$ generated by the sequence $\{a_n/2\}_n$, for some binary sequence $\{a_n\}_n$.) Note that, by the Euclidean Algorithm, $k[X]$ is a GCD-domain for all discrete fields k.

Let f be a polynomial over a GCD-domain. Then $\text{cont}(f)$, the *content* of f, is the greatest common divisor of the coefficients of f; f is *primitive* if $\text{cont}(f) = 1$.

2.0 Lemma (Gauss's Lemma). *Let f and g be nonzero polynomials over a GCD-domain R. Then $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$.*

Proof: We may assume that f and g are primitive. Let m and n be the degrees of f and g respectively, let $c = \text{cont}(fg)$, and let $d = \text{GCD}(c, a_m)$, where a_m is the leading coefficient of f. We complete the proof by induction on $m + n$. If $f = a_m X^m$, then we are done. Otherwise, $d \mid (f - a_m X^m)g$, so, by induction, $d \mid \text{cont}(f - a_m f)\text{cont}(g)$. Since g is primitive, $d \mid (f - a_m X^m)$, thus also $d \mid f$, proving $d = \text{GCD}(c, a_m) = 1$. Similarly, $\text{GCD}(c, b_n) = 1$, where b_n is the leading coefficient of g. So $\text{GCD}(c, a_m b_n) = 1$. Thus fg is primitive. $\dashv$

Let f and g be polynomials over a commutative ring R such that g is monic. By the Remainder Theorem there are unique polynomials q and r over R, with r of a degree less than the degree of g, such that $f = qg + r$. The coefficients of q and r are polynomials in the coefficients of f and g.

2.1 Theorem (Unique Interpolation). *Let $a_0, \ldots, a_n$ and $v_0, \ldots, v_n$ be elements of a commutative ring R such that $a_i - a_j$ is a unit, for all $i \neq j$. Then there is a unique polynomial of degree at most n over R such that $f(a_i) = v_i$ for all i.*

Proof: By induction on n. If $n = 0$, choose $f = v_0$. If $n > 0$, then there is a polynomial g of degree at most $n - 1$ such that $g(a_i) = (v_i - v_n)/(a_i - a_n)$ for all $i < n$. Take $f = (X - a_n)g + v_n$.

For uniqueness it suffices to show that if $f(a_i) = 0$ for all i, and f is of degree at most n, then $f = 0$. The case for $n = 0$ is trivial. Suppose $n > 0$. By the Remainder Theorem, $f = g(X - a_n)$ for some g of degree at most $n - 1$ with $g(a_i) = 0$ for all $i < n$. By induction on n, $g = 0$. So $f = 0$. $\dashv$

A nonzero element p of a discrete domain R is *irreducible* if it is not a unit, and if $p = qr$ implies that q or r is a unit, for all $q, r \in R$.

A discrete domain is a *unique factorization domain* or *UFD* if each nonzero element is a unit or equals a product of irreducibles, and such that if $p_1 \ldots p_m = q_1 \ldots q_n$ are two products of irreducibles, then $m = n$ and there is a permutation π such that p_i and $q_{\pi i}$ differ by a unit, for all i. Discrete fields and $\mathbf{Z}$ are unique factorization domains. A discrete domain R is *factorial* if $R[X]$ is a discrete UFD. This definition seems unnatural at first, but is a natural generalization of the notion of factorial field: A discrete field is factorial when we can factor polynomials over it into irreducibles. See also Theorem 2.3. Algebraically closed discrete fields are factorial, since all nonconstant polynomials factor into linear terms.

A set is *infinite* if it contains arbitrarily large finite subsets. Without choice principles we cannot show that an infinite set contains a countably infinite subset.

2.2 Theorem (Kronecker 1). *If R is an infinite UFD with finitely many units, then so is $R[X]$. Thus R is factorial.*

Proof: Obviously $R[X]$ has finitely many units since it has the same units as R. Let $f \in R[X]$ be of degree $n > 0$. We complete the proof by induction on n. It suffices to provide a finite collection of polynomials that includes all possible factors of f. Let $a_0, \ldots, a_n$ be distinct elements of R. If $f(a_i) = 0$ for some i, then we divide a factor $X - a_i$ out of f and apply induction. So we may assume $f(a_i) \neq 0$ for all i. Each nonzero element of R has finitely many divisors, so there are finitely many sequences $b_0, \ldots, b_n$ such that b_i divides $f(a_i)$, for all i. By the Unique Interpolation Theorem 2.1, there is for each such sequence a unique polynomial g over the quotient field of R, of degree at most n, such that $g(a_i) = b_i$. Since R is detachable from its quotient field, we can find a finite subcollection of g with coefficients in R that includes all factors of f. $\dashv$

An essentially identical proof of Theorem 2.2 was given, about nine decades before Kronecker, by the astronomer Friedrich Theodor von Schubert (1758–1825) in 1793 [10]. See also [3, pp. 136ff].

2.3 Theorem (Kronecker 2). *If R is a factorial domain, then so is $R[X]$.*

Proof: For $m > 0$, let $R[X,Y]_m$ be the submodule of $R[X,Y]$ of polynomials of X-degree less than m. The submodule $R[X,Y]_m$ is closed under taking factors. Let $\varphi_m \colon R[X,Y]_m \to R[X]$ be the R-module map that is the restriction of the ring morphism that is the identity on $R[X]$ and maps Y to X^m, and let $\psi_m \colon R[X] \to R[X,Y]_m$ be the R-module map that takes X^n to $Y^q X^r$, where $n = qm + r$ with $0 \leq r < m$. Then φ_m and ψ_m are each other's inverses. Each factorization of a polynomial $f \in R[X,Y]$ of X-degree less than m must be of the form $f = \psi_m(g)\psi_m(h)$. So it suffices to factor $\varphi_m(f)$ in $R[X]$. $\dashv$

Note that, in the proof of Theorem 2.3, $\varphi_m(f)$ may have factorizations that do not translate into factorizations of f.

By Kronecker 1 the domain $\mathbf{Z}$ is factorial, so, by Gauss's Lemma, $\mathbf{Q}$ is factorial too. Thus, by Kronecker 2, $\mathbf{Q}(X_1, X_2, \ldots)$ is factorial, and so is $k(X_1, X_2, \ldots)$, for all algebraically closed discrete fields k. Next we will show that finite algebraic extensions of $\mathbf{Q}$ are also factorial. Since $\mathbf{Q}$ has characteristic 0, several results are proven for discrete fields of characteristic 0 only. Generalizations involving separability conditions are discussed in [7].

Elements a, b of a commutative ring R are *strongly relatively prime* if $aR + bR = R$. The derivative f' of a polynomial f is defined as usual. A polynomial f over a commutative ring is *separable* if f and f' are strongly relatively prime. This is different from tradition: One usually defines separable polynomials over discrete fields as the ones that are products of our separable polynomials [8]. Clearly, factors of separable polynomials are again separable, for if fg is separable, then there exist polynomials s, t such that $sfg + t(f'g + fg') = 1$; so $(sg + tg')f + tgf' = 1$. Let $R[\alpha] \supseteq R$ be commutative rings. Then α is *separable* over R if it is root of a separable polynomial over R.

Each $n \times n$ matrix over a discrete field k is also a vector of an n^2-dimensional vector space. We can find a smallest m such that the vectors $I, A, A^2, \ldots, A^m$ are linearly dependent. Then A is root of a monic polynomial p over k of degree m, the so-called *minimal polynomial* of A. Since A is root of its characteristic polynomial of degree n, we have that $m \leq n$. The matrix ring $k[A]$ forms a discrete commutative ring such that $k[A] \cong k[X]/(p)$. If S is an invertible $n \times n$ matrix, then $k[A] \cong k[S^{-1}AS]$ by the isomorphism that is the identity on k and that sends A to $S^{-1}AS$. The matrix A is *separable* if its minimal polynomial p is separable.

2.4 Theorem. *Let A be an $n \times n$ matrix over a discrete field k. Then the minimal polynomial of A is separable and splits into linear factors if and only if A is diagonalizable. If A is diagonalizable, then the projections of k^n onto the eigenspaces of A can be written as polynomials in A of degree at most $n-1$.*

Proof: If A is diagonalizable, with set of eigenvalues Λ, then it is root of the separable polynomial $\prod_{\lambda\in\Lambda}(X-\lambda)$. Conversely, if the minimal polynomial of A is separable and splits into linear factors, then the eigenspaces V_λ of A, being the null spaces of matrices $A-\lambda$ that are associated with the strongly relatively prime linear factors $X-\lambda$ of the minimal polynomial of A, are direct summands such that $\sum_\lambda V_\lambda = k^n$.

Suppose A is diagonalizable, and write $f = (X-\lambda)g_\lambda(X)$ for each root λ of the minimal polynomial f. As $f(A) = 0$, the matrix $g_\lambda(A)$ maps into V_λ. If $\mu \neq \lambda$ are eigenvalues, then $X-\mu$ divides $g_\lambda(X)$, so $g_\lambda(A)V_\mu = 0$. The polynomial $1 - \sum_{\lambda\in\Lambda} g_\lambda(X)/g_\lambda(\lambda)$ has a degree less than the cardinality of Λ, but has all the eigenvalues as roots; so it is identical to 0. Thus $\sum_{\lambda\in\Lambda} g_\lambda(A)/g_\lambda(\lambda)$ is the identity, and $g_\lambda(A)/g_\lambda(\lambda)$ is the projection onto V_λ. $\dashv$

2.5 Theorem. *Let A and B be commuting diagonalizable $n\times n$ matrices over a discrete field k. Then k^n admits a basis relative to which A and B diagonalize simultaneously.*

Proof: Let V^A_λ and V^B_λ be the λ-eigenspaces of A and B respectively. Since B commutes with $A-\lambda$, for all λ, the eigenspaces of A are invariant under B, hence also under the projections onto the eigenspaces V^B_μ, which are polynomials in B. Therefore, $V^A_\lambda = \sum_\mu V^A_\lambda \cap V^B_\mu$. So $k^n = \sum_{\lambda,\mu} V^A_\lambda \cap V^B_\mu$ $\dashv$

The class of discrete fields admits *linear elimination*: Let k be a discrete field, and $v_1, \ldots, v_n, w$ be vectors in k^n. Then w is a linear combination of the vectors v_i with coefficients in some discrete field extension of k if and only if the rank of the matrix $(v_1, \ldots, v_n, w)$ is equal to the rank of the matrix $(v_1, \ldots, v_n)$. So if w is a linear combination of the v_i over some discrete extension field, then it is already a linear combination with coefficients in k.

2.6 Theorem. *If A and B are commuting separable $n\times n$ matrices over a discrete field k of cardinality greater than $n(n-1)/2$, then there exists c such that $k[A,B] = k[A+cB]$.*

Proof: Let K be a countable discrete subfield that includes the coefficients of the matrices A and B, and contains at least $1+n(n-1)/2$ elements from k. By Theorem 1.7 we can construct a countable discrete field $L \supseteq K$ over which the minimal polynomials of A and B split into linear factors. So A and B are—simultaneously—diagonalizable over L with diagonal elements $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$. Choose $c \in K$ distinct from $(a_j - a_i)/(b_i - b_j)$, for all pairs i, j with $b_i \neq b_j$. Then $a_i + cb_i \neq a_j + cb_j$ whenever $(a_i, a_j) \neq (b_i, b_j)$. By Theorem 2.4, A and B can be written as polynomials of degree at most $n-1$ in $A+cB$. So A and B, as vectors in n^2 variables, are linear combinations of the vectors $I, A+cB, \ldots, (A+cB)^{n-1}$ with coefficients in L. By linear elimination, A and B are polynomials in $A+cB$ over K, hence over k. ⊣

The proofs of Theorems 2.4, 2.5, and 2.6 are based on [8]. For further improvements and strengthenings, see [7, pp. 158ff] and [8].

2.7 Lemma. *Let R be a commutative ring containing a discrete field k, and let $\alpha, \beta \in R$ and polynomials f, g over k be such that $f(\alpha) = g(\beta) = 0$. Then there are commuting square matrices A, B of the same size over k such that $f(A) = g(B) = 0$, and a ring map from $k[A,B]$ onto $k[\alpha,\beta]$ that is the identity on k, sends A to α, and sends B to β.*

Proof: The ring $k[x,y] = k[X,Y]/(f(X), g(Y))$ is a finite-dimensional vector space over k. Multiplication by x and y are linear transformations on this vector space. With respect to some basis, these transformations are represented by commuting matrices A and B satisfying $f(A) = g(B) = 0$, and $k[A,B] \cong k[x,y]$. So we can construct the ring map from $k[A,B]$ onto $k[\alpha,\beta]$ that is the identity on k, sending A and B to α and β respectively. ⊣

2.8 Corollary (Primitive Element). *Let R be a commutative ring containing an infinite discrete field k, and let α and β be elements of R that are separable over k. Then there exists θ such that $k[\alpha,\beta] = k[\theta]$.*

Proof: There are separable polynomials $f, g \in k[X]$ such that $f(\alpha) = g(\beta) = 0$, so there is a commutative matrix ring with surjective ring map $\sigma\colon k[A,B] \to k[\alpha,\beta]$, and such that $f(A) = g(B) = 0$. By Theorem 2.6 there is $C \in k[A,B]$ such that $k[C] = k[A,B]$. Choose $\theta = \sigma(C)$. ⊣

Let $K \supseteq k$ be discrete fields such that K is finite-dimensional as a vector space over k. We shall write $[K:k]$ for the dimension. If L is a discrete field extension of K that is finite-dimensional, then so is L over k, and $[L:k] = [L:K][K:k]$. If two of the three dimensions are finite, then so is the third and the equation holds.

2.9 Theorem. *Let $k \subseteq k[\alpha]$ be discrete fields of characteristic 0 such that k is factorial. Then $k[\alpha]$ is factorial too.*

Proof: Let f be a polynomial over $k[\alpha]$ of degree $n > 1$. It suffices to give an irreducible factor. We complete the proof by induction on n. We may assume that f is separable; otherwise, the greatest common divisor of f and f' is a proper factor, and we are done by induction. Let $k[\alpha,\beta] = k[\alpha][X]/(f(X))$; $k[\alpha,\beta]$ is a finite-dimensional vector space over k. Then $k[\alpha,\beta] = k[\theta]$, with $g(\theta) = 0$ for some polynomial g over k of degree $[k[\theta]:k]$. If g is irreducible, then so is f. Otherwise, let p be a proper factor of g. Then $k[\theta]$ maps onto $k[X]/(p)$ with nonzero kernel $p(\theta)\cdot k[\theta]$. Hence $h(\beta) = p(\theta)$ is mapped to 0, for some $h(X) \in k[\alpha][X]$. Then the greatest common divisor of f and h is a proper factor of f. ⊣

Recall that there exist countable discrete fields whose characteristic we cannot determine. Theorem 2.9 can be generalized to some of such discrete fields, and to some discrete fields of finite characteristic, by replacing the characteristic 0 condition by Seidenberg's 'Condition P' [7, p. 188].

2.10 Theorem (Rich Man's Algebraic Closure). *Each countable factorial field k of characteristic 0 has a countable discrete algebraic closure Ω such that for each finitely generated subfield $K \supseteq k$, each element of Ω is root of an irreducible polynomial over K.*

Proof: The construction of Ω is identical to that in the proof of Theorem 1.8. By Corollary 2.8, each finitely generated intermediate field is of the form $K = k[\alpha]$. Let $\beta \in \Omega$. Then $K[\beta] = k[\theta]$ for some $\theta \in \Omega$. Both θ and α are roots of irreducible polynomials over k, so $k[\theta]$ and $k[\alpha]$ are finite-dimensional vector spaces over k. Then $K[\beta]$ is a finite-dimensional vector space over K of degree

$$[K[\beta] : K] = [k[\theta] : k]/[k[\alpha] : k].$$

So θ is root of an irreducible polynomial over K of degree $[K[\beta] : K]$. $\dashv$

2.11 Corollary. *The field of rational numbers $\mathbf{Q}$ has a countable discrete algebraic closure C such that for each finitely generated subfield $k \supseteq \mathbf{Q}$, each element of C is root of an irreducible polynomial over k.* $\dashv$

Without additional choice principles we cannot show that all algebraic closures of a countable factorial field of characteristic 0 are countable. But the countable algebraic closures are all isomorphic.

Let k, K be discrete fields, and $\sigma: k \to K$ a morphism. Let $k[\alpha]$ be a discrete field extension of k, and α a root of an irreducible polynomial f over k. If $\beta \in K$ is a root of $\sigma(f)$, then σ extends to a morphism from $k[\alpha]$ into K that takes α to β.

2.12 Theorem. *All countable discrete algebraic closures of a countable factorial field of characteristic 0 are isomorphic.*

Proof: Let $K = \{a_0, a_1, \ldots\}$ and $L = \{b_0, b_1, \ldots\}$ be countable discrete algebraic closures of the countable factorial field k. By induction we construct embeddings $\sigma_n: k_n = k[a_0, \ldots, a_{n-1}] \to L$. Naturally, $k_0 = k$ embeds into L. Suppose σ_n exists. Then a_n is root of an irreducible polynomial f over k_n, and there is a smallest, hence unique, i such that b_i is root of $\sigma_n(f)$. Extend σ_n to σ_{n+1} by setting $\sigma_{n+1}(a_n) = b_i$. The union of the σ_i is an isomorphism from K to L. $\dashv$

§3. The Fundamental Theorem of Algebra

There are several ways to define the set of real numbers, hence at least as many ways to define the set of complex numbers. Some of these cannot be shown to be equivalent in constructive mathematics. Each choice yields another field of complex numbers for which one may try to prove some form of the Fundamental Theorem of Algebra. Below we restrict ourselves to the ones that seem most relevant to constructivists.

A (rational) Cauchy sequence is a sequence of rational numbers $\{r_n\}_n$ such that for all integers $m > 0$ there exists M such that $|r_p - r_q| < 1/m$ for all $p, q \geq M$. A Cauchy sequence is *modulated* if $M = M(m)$ is a function from $\mathbf{N}$ to $\mathbf{N}$ [11, pp. 253ff]. [1, pp. 18ff] uses a 'fixed' modulus function $M(m)$. This further restriction will be inessential in what follows below. Define a binary relation $\sim$ on the collection of Cauchy sequences by

$\{r_n\}_n \sim \{s_n\}_n$ if and only if for all $m > 0$ there exists M such that $|r_p - s_q| < 1/m$ for all $p, q \geq M$. One easily verifies $\sim$ to be an equivalence relation. A similar modulated equivalence relation exists where $M = M(m)$ is a function $\mathbf{N} \to \mathbf{N}$. A *Cauchy real* is an equivalence class. A *modulated Cauchy real* is a 'modulated' equivalence class of modulated Cauchy sequences. Both kinds of Cauchy reals with the canonical operations form commutative rings. A (modulated) Cauchy real is invertible exactly when it has a (modulated) Cauchy sequence $\{r_n\}_n$ for which there exist $m > 0$ and M according to the definition above, and $|r_M| > 2/m$.

A subset $Q \subseteq \mathbf{Q}$ of the rationals is a left Dedekind cut if it satisfies

(1) $p < q \in Q$ implies $p \in Q$.
(2) For all $p \in Q$ there exists q such that $p < q \in Q$.
(3) For all integers $m > 0$ there exist $p < q$ such that $|p - q| < 1/m$, $p \in Q$, and $q \notin Q$, that is, q is not an element of Q.

Left Dedekind cuts form the set of *Dedekind reals* $\mathbf{R}$. We easily verify that $\mathbf{R}$, with the canonical operations, is a commutative ring. We write $Q > 0$, Q is positive, when $p \in Q$ for some $p > 0$, and $Q < 0$, Q is negative, when $q \notin Q$ for some $q < 0$. A Dedekind real Q is invertible, written $Q \neq 0$, exactly when $Q > 0$ or $Q < 0$. Note that this makes $\neq$ on $\mathbf{R}$ different from denial of equality. If $Q \neq 0$ is false, then $Q = 0$. Analogous to (modulated) Cauchy reals and Dedekind reals we have (modulated) Cauchy complex numbers and Dedekind complex numbers, the last ones forming the set $\mathbf{C} = \mathbf{R} + i\mathbf{R}$, with $a + ib \neq 0$ exactly when $a + ib$ is invertible. Then $a + ib \neq 0$ exactly when $a \neq 0$ or $b \neq 0$, for all $a, b \in \mathbf{R}$. The relation $\neq$ is an apartness [9].

We may consider $\mathbf{Q}$ a subring of the modulated Cauchy reals by identifying each rational with the equivalence class that contains the corresponding constant Cauchy sequence. The modulated Cauchy reals may be considered a subring of the Cauchy reals. The Cauchy reals may be considered a subring of $\mathbf{R}$ by identifying each Cauchy sequence $\{r_n\}_n$ with the Dedekind cut Q defined by $p \in Q$ if and only if for some $m > 0$ and M satisfying the definition of Cauchy sequence, $p + 2/m < r_M$.

If c is a (modulated) Cauchy complex number, then the absolute value $|c|$ exists and is a (modulated) Cauchy real. Similarly, if $c \in \mathbf{C}$, then $|c| \in \mathbf{R}$. A *Cauchy sequence* is a sequence $\{c_n\}_n$ of elements of $\mathbf{C}$ such that for all $m > 0$ there exists M such that $|c_p - c_q| < 1/m$ for all $p, q \geq M$. The sequence is *modulated* if $M = M(m)$ is a function. A (modulated) Cauchy sequence of modulated Cauchy sequences is a (modulated) Cauchy sequence, and a Cauchy sequence of Dedekind reals is a Dedekind real. But a Cauchy sequence of modulated Cauchy sequences is only a Cauchy sequence, and a modulated Cauchy sequence of Cauchy sequences is only a Dedekind real. With Countable Choice one can show that each Dedekind real is a modulated Cauchy real, and thus the Cauchy reals are closed under taking Cauchy sequences. Therefore, in the presence of Countable Choice, modulated Cauchy sequences are the common way by which to define reals; without choice it is the (left) Dedekind cuts [5, pp. 415ff].

A set $U \subseteq \mathbf{R}$ is open if for all $u \in U$ there exist rational numbers p, q such that $p < u < q$, and $v \in U$ whenever $p < v < q$. Open sets on $\mathbf{R}^n$ are defined by the product topology. If $\mathbf{c}, \mathbf{d} \in \mathbf{R}^n$ are such that $c_i \neq d_i$ ($c_i - d_i$ is a unit) for some i, then there exist open sets $U, V \subseteq \mathbf{R}^n$ such that $\mathbf{c} \in U$, $\mathbf{d} \in V$, and $U \cap V = \emptyset$. Functions f are *continuous* if $f^{-1}(U)$ is open, for all open U. Constant functions, the identity, and the basic ring theoretic functions are continuous. Compositions of continuous functions are continuous. So all polynomial functions are continuous.

A commutative ring is *impotent* if it satisfies the axioms

$$a^2 = 0 \text{ implies } a = 0, \quad \text{and}$$
$$a^2 = a \text{ implies } a = 0 \text{ or } a = 1.$$

One easily verifies that $\mathbf{R}$ and $\mathbf{C}$ are impotent rings.

If R is impotent and $a, b \in R$ are such that $a + b = 1$ and $ab = 0$, then $a = 1$ or $a = 0$ and, therefore, $b = 0$ or $b = 1$. For if we multiply the first equation by a, and apply the second equation, we get $a^2 = a^2 + ab = a$.

3.1 Lemma. *Let $R \subseteq S$ be impotent commutative rings, and $\alpha \in S$. If $f, g \in R[X]$ are strongly relatively prime, and $f(\alpha)g(\alpha) = 0$, then $f(\alpha)$ is a unit or $g(\alpha)$ is a unit. So $g(\alpha) = 0$ or $f(\alpha) = 0$.*

Proof: $sf + tg = 1$ for some $s, t \in R[X]$. So $s(\alpha)f(\alpha) = 1$ or $t(\alpha)g(\alpha) = 1$. $\dashv$

3.2 Theorem. *Let R be an impotent commutative ring with discrete subfield k. If $\alpha \in R$ is algebraic over k, then $k[\alpha]$ is a discrete field. The set of elements in R algebraic over k is a discrete subfield.*

Proof: It suffices to prove the first claim. By Proposition 1.2 each $\beta \in k[\alpha]$ is algebraic over k, hence root of a monic polynomial $g \in k[X]$. We can write $g = X^m h$ with $h(0) \neq 0$. Then X^m and h are strongly relatively prime, so β^m is a unit or $h(\beta)$ is a unit. So β is a unit or $\beta = 0$. $\dashv$

Let $\mathbf{C}^a$ be the set of *algebraic numbers*, that is, the set of complex numbers that are algebraic over $\mathbf{Q}$, and $\mathbf{R}^a = \mathbf{C}^a \cap \mathbf{R}$ be the set of *algebraic reals*. Then $\mathbf{C}^a$ and $\mathbf{R}^a$ are discrete.

3.3 Lemma. *Let $f \in \mathbf{R}^a[X]$, and $a, b \in \mathbf{R}$ such that $f(a) < 0 < f(b)$. Then there exists a modulated Cauchy real $c \in \mathbf{R}^a$ with $f(c) = 0$. If $a < b$, then $a < c < b$; otherwise, $a > c > b$.*

Proof: We may assume that $a < b$. By continuity there are $a', b' \in \mathbf{Q}$ such that $a < a' < b' < b$ and $f(a') < 0 < f(b')$. For each $r \in \mathbf{R}^a$ we have $f(r) < 0$, $f(r) = 0$, or $f(r) > 0$, so we can construct sequences $\{a_n\}_n$, $\{b_n\}_n$, and $\{c_n\}_n$, where $c_n = (a_n + b_n)/2$, by:

(1) $a_0 = a'$ and $b_0 = b'$.
(2) $a_{n+1} = b_{n+1} = c_n$ if $f(c_n) = 0$.
(3) $a_{n+1} = c_n$ and $b_{n+1} = b_n$ if $f(c_n) < 0$.
(4) $a_{n+1} = a_n$ and $b_{n+1} = c_n$ if $f(c_n) > 0$.

Then $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ and $|a_n - b_n| \leq (b' - a')(1/2)^n$, for all n. So $\{c_n\}_n$ is a modulated Cauchy sequence with limit $c \in \mathbf{R}$. By the Remainder Theorem, applied to $\mathbf{Q}[Y][X]$, there is $g \in \mathbf{Q}[X, Y]$ such that $f(X) = (X - Y)g(X, Y) + f(Y)$. There is an M such that $|g(x, y)| \leq M$ whenever $a \leq x, y \leq b$. So $|f(x) - f(y)| \leq M|x - y|$ whenever $a \leq x, y \leq b$; thus $\{f(c_n) - f(a_n)\}_n$ and $\{f(c_n) - f(b_n)\}_n$ converge to 0, with $f(a_n) \leq 0 \leq f(b_n)$. By continuity, $f(c) = 0$; and $c \in \mathbf{R}^a$ by Proposition 1.4. $\dashv$

3.4 Corollary. *All nonzero polynomials $f \in \mathbf{R}^a[X]$ have a finite set of roots in $\mathbf{R}^a$. If f is of odd degree, then it has at least one root.*

Proof: Suppose f is of odd degree. We may assume f to be monic. Let b be 1 plus the sum of the absolute values of the coefficients of f, and let $a = -b$. Then $f(a) < 0 < f(b)$.

Let f be nonzero and of degree $n > 1$. We complete the proof by induction on n. We may assume f to be separable. By induction, f' has a finite set of roots $r_1 < \cdots < r_m$. If f' has no roots, then f has one. Otherwise, f has one root in the interval (r_j, r_{j+1}) exactly when $f(r_j)f(r_{j+1}) < 0$, one root less than r_1 exactly when $f(r_1-1)f'(r_1-1) > 0$, and one root bigger than r_m exactly when $f(r_m+1)f'(r_m+1) < 0$. ⊣

Obviously, the element $i = \sqrt{-1}$ is algebraic. Let $a, b \in \mathbf{R}$ be such that $a + ib$ is an algebraic number. Then $a + ib$ is root of a polynomial with rational coefficients, so, by conjugation, $a - ib$ is root of the same polynomial. So a and b are algebraic numbers too. Thus $\mathbf{C}^a = \mathbf{R}^a + i\mathbf{R}^a$. If $c \in \mathbf{C}^a$, then the absolute value $|c| \in \mathbf{R}^a$. The order relation $<$ with restriction to $\mathbf{R}^a$ is decidable: If $a \in \mathbf{R}^a$ is nonzero, then a is invertible, so $a > 0$ or $a < 0$. Obviously we can enumerate the monic polynomials over $\mathbf{Q}$, and for each such polynomial we can enumerate its roots in $\mathbf{R}^a$ in a unique manner 'from left to right.' So $\mathbf{R}^a$ is countable, hence $\mathbf{C}^a$ is countable. Combining this with Theorem 3.2 we get:

3.5 Corollary. *The set of algebraic numbers $\mathbf{C}^a$ is a countable discrete field.* ⊣

3.6 Corollary. *All algebraic numbers are modulated Cauchy.*

Proof: Let $c \in \mathbf{R}^a$. Then c is the unique root of the polynomial $f(X) = X - c$ satisfying $f(c-1) < 0 < f(c+1)$. ⊣

Let $\{a_n + ib_n\}_n$ be a (modulated) Cauchy sequence of algebraic numbers. Construct the (modulated) rational sequence $\{c_n/n + id_n/n\}_n$ by setting c_n equal to the largest integer less than or equal to na_n, and d_n equal to the largest integer less than or equal to nb_n. Then the rational sequence has the same limit as the sequence over $\mathbf{C}^a$. So each (modulated) Cauchy sequence of algebraic numbers has as limit a (modulated) Cauchy number.

3.7 Lemma. *Let $a, b \in \mathbf{R}^a$. Then there exist $c, d \in \mathbf{R}^a$ such that $(c + id)^2 = a + ib$.*

Proof: First suppose that $b = 0$. As $\mathbf{C}^a$ is discrete, either $a > 0$ or $a = 0$, or $a < 0$. If $a > 0$, then $\sqrt{a} \in \mathbf{R}^a$ is a root of $X^2 - a$, by Lemma 3.3. If $a < 0$, then we get $i\sqrt{-a}$. In the general case we choose c and d from the roots of $X^2 - (a + \sqrt{a^2 + b^2})/2$ and $X^2 - (-a + \sqrt{a^2 + b^2})/2$ respectively. ⊣

The theory of finite groups is essentially completely constructive. One easily sees that most proofs of the class equation for finite groups are easily constructivized. So Sylow's theorem is constructive: If G is a finite group and p is a prime number such that p^n divides the order of G, then G has a finite subgroup of order p^n. A subgroup of order p^n with n maximal is called a *p-Sylow subgroup.*

Let R be a commutative ring. A polynomial $f \in R[X_1, \ldots, X_n]$ is *symmetric* in the variables $X_1, \ldots, X_n$ if $f(X_1, \ldots, X_n) = f(X_{\pi 1}, \ldots, X_{\pi n})$, for all permutations π. Clearly, the coefficients σ_i of the polynomial

$$(Y + X_1)(Y + X_2) \ldots (Y + X_n) = Y^n + \sigma_1 Y^{n-1} + \cdots + \sigma_n$$

are symmetric. They are the *elementary symmetric polynomials.* Each symmetric polynomial is element of the ring $R[\sigma_1, \ldots, \sigma_n]$ [7, pp. 73ff].

Let $K \supseteq k$ be discrete fields. An element $\alpha \in K$ *splits* over k if it is root of a polynomial over k that factors into linear factors over K. The field K is *normal* over k if each $\alpha \in K$ splits over k.

Let $K \supseteq k$ be discrete fields such that $K = k[\theta]$. Then θ splits over k if and only if K is normal over k. For if θ splits, then there is a monic polynomial f over k that splits with roots $\theta = \theta_1, \ldots, \theta_n$. The elementary symmetric polynomials in the θ_j are coefficients of f, hence elements of k. Let $\alpha \in K$. We can write $\alpha = p(\theta)$, for some $p \in k[X]$. Then α is root of the polynomial $g = \prod_j (X - p(\theta_j))$, whose coefficients are symmetric in the θ_j. So $g \in k[X]$.

Let $K = k[\theta]$ and $\theta = \theta_1, \ldots, \theta_n$ be as above, and suppose, additionally, that f is irreducible and the characteristic of k equals 0. Then all θ_j are distinct, and for each j we have a unique automorphism of K that is the identity on k and maps θ to θ_j. These automorphisms form the *Galois group* G of the extension $K \supseteq k$. If H is a finite subgroup of G, then θ is root of the polynomial $h = \prod_{\sigma \in H}(X - \sigma(\theta))$ over the field $L \supseteq k$ generated by the coefficients of h. The field L is called the *fixed field* of H, since its elements are exactly the ones that are fixed by the automorphisms of H. Obviously, h is irreducible over L. So $[K : L] = |H|$, the cardinality of H.

3.8 Lemma. *Each polynomial over* $\mathbf{Q}$ *has a root in* $\mathbf{C}^a$.

Proof: Let f be a monic polynomial over $\mathbf{Q}$, and let K be a splitting field of f over $\mathbf{Q}$ which, by Corollary 2.8, has a finite Galois group G. It suffices to embed K in $\mathbf{C}^a$. Let H be the 2-Sylow subgroup of G with fixed field k. Then $[k : \mathbf{Q}] = |G|/|H|$ is odd. By Corollary 2.8 there exists α such that $k = \mathbf{Q}[\alpha]$, and α is root of an irreducible polynomial of odd degree over $\mathbf{Q}$. So by Corollary 3.4 there exists an embedding of k into $\mathbf{C}^a$. The group H contains a chain of subgroups $H_0 \subseteq \cdots \subseteq H_n = H$ of order $|H_j| = 2^j$, with fixed fields $K = K_0 \supseteq \cdots \supseteq K_n = k$. So $[K_j : K_{j+1}| = 2$ for all j. By the quadratic formula, if $M \supseteq L$ are discrete fields of characteristic greater than 2 such that $[M : L] = 2$, then $M = L[\beta]$, with $\beta^2 \in L$. So by Lemma 3.7 we can extend an embedding from k_{j+1} into $\mathbf{C}^a$ to one from k_j, for all j. So K embeds into $\mathbf{C}^a$. $\dashv$

3.9 Theorem (Discrete Fundamental Theorem). $\mathbf{C}^a$ *is algebraically closed.*

Proof: Let f be a nonconstant polynomial over $\mathbf{C}^a$. By Theorem 1.7 there exists a countable discrete splitting field of f. Let $g \in \mathbf{Q}[X]$ have all roots of f as roots, including multiplicities; so $f \mid g$. By Corollary 2.8 there is a splitting field $\mathbf{Q}[\alpha]$ of g. Let $h \in \mathbf{Q}[X]$ be the minimal polynomial of α. Then $h(\beta) = 0$ for some $\beta \in \mathbf{C}^a$. So g, and thus f, splits into linear factors over $\mathbf{Q}[\beta] \subseteq \mathbf{C}^a$. $\dashv$

The Discrete Fundamental Theorem enables us to study the roots of polynomials over $\mathbf{C}$ more generally through approximation by polynomials over $\mathbf{C}^a$. To make this work we must show that if two polynomials are close to each other, then their roots are close too.

Let $f = \sum_j a_{n-j}X^j$ be a polynomial over $\mathbf{C}$. Define $|f| = \sum_j |a_j|$.

Let $f = X^n + a_1X^{n-1} + \cdots + a_n$ be a monic polynomial over $\mathbf{C}$, and let $c \in \mathbf{C}$. Then $|f(c)| \geq |c|^n - |a_1c^{n-1} + \cdots + a_n| \geq |c|^n - \max\,(1, |c|^{n-1})(|f| - 1)$. So if $|c| \geq |f|$, then $|f(c)| \geq |c|^{n-1}(|c| - |f| + 1) \geq |f|^{n-1}$; and if $|f(c)| < |f|^{n-1}$, then $|c| < |f|$. If g is a monic factor of f, then for all $\varepsilon > 0$ there exists a polynomial $g^* = \prod_j (X - c_j)$ over $\mathbf{C}^a$ with $|c_j| < |f|$ for all c_j, and $|g - g^*| < \varepsilon$. So $|g| \leq \varepsilon + |g^*| < \varepsilon + (1 + |f|)^n$. So $|g| \leq (1 + |f|)^n$.

If $f = (X - c_1)\ldots(X - c_n)$, $\varepsilon > 0$, and c are such that $|f(c)| < \varepsilon^n$, then $\prod_j |c - c_j| < \varepsilon^n$. Thus $|c - c_j| < \varepsilon$ for some j. Let, additionally, $R \geq |f|$, and $g = (X - d_1)\ldots(X - d_n)$. Suppose that $|f - g| < (\varepsilon/R)^n$ for some $\varepsilon > 0$. Then $|g(c_j)| < \varepsilon^n$ for all j. So for all j there exists k such that $|c_j - d_k| < \varepsilon$.

By the Remainder Theorem, there exists for all polynomials $f(X)$ a polynomial $G_f(X, Y)$ such that $f(X) - f(Y) = (X - Y)G_f(X, Y)$. The coefficients of G_f are polynomials in the coefficients of f. So given $R > 0$ and an integer $n > 0$, there exists M such that for all monic f of degree n and $z, w \in \mathbf{C}$, if $|f| < R$, $|z| < R$, and $|w| < R$, then $|G_f(z, w)| < M$.

3.10 Lemma. *Let $n > 0$ be an integer, and $R, \varepsilon \in \mathbf{R}$ be such that $\varepsilon > 0$. Then there exists $\delta > 0$ such that for all $f = (X - c_1)\ldots(X - c_n)$ and $g = (X - d_1)\ldots(X - d_n)$ over $\mathbf{C}$, if $|f| < R$, $|g| < R$, and $|f - g| < \delta$, then there is a permutation π such that $|c_j - d_{\pi j}| < \varepsilon$ for all j.*

Proof: We may assume that $\varepsilon < 1$. Let $S = (1 + R)^n$. Choose $M \geq 1$ such that for all monic f of degree at most n and all z, w, if $|f| < S$, $|z| < S$, and $|w| < S$, then $|f(z) - f(w)| \leq |z - w|M$. Choose $0 < \varepsilon_{2n} < \cdots < \varepsilon_1 = \varepsilon$ such that $\varepsilon_{2j} < \varepsilon_{2j-1}^j$ and $\varepsilon_{2j-1} < \varepsilon_{2j-2}^3/(100M^2S^{n+1})$, for all j. Set $\delta = \varepsilon_{2n}/S^{n-1}$. Let $f = \prod_j (X - c_j)$ and $g = \prod_j (X - d_j)$ be monic polynomials of degree n such that $|f| < R$, $|g| < R$, and $|f - g| < \delta$. Then $|f(z) - g(z)| \leq |f - g|S^{n-1} < \varepsilon_{2n}$ for all z satisfying $|z| < S$. We complete the proof by induction on n. Suppose $n > 1$. Then there exists d_k such that $|c_n - d_k| < \varepsilon_{2n-1}$. We may assume that $k = n$. Let $f^*(z) = f(z)/(z - c_n)$ and $g^*(z) = g(z)/(z - d_n)$. For all z satisfying $|z| < S$, $|z - c_n| > \varepsilon_{2n-2}/5M$, and $|z - d_n| > \varepsilon_{2n-2}/5M$, we have

$$\begin{aligned}|f^*(z) - g^*(z)| &= \left|\frac{f(z)(z - c_n) + f(z)(c_n - d_n) - g(z)(z - c_n)}{(z - c_n)(z - d_n)}\right| \\ &\leq |f(z) - g(z)|5M/\varepsilon_{2n-2} + |f(z)|\varepsilon_{2n-1}(5M/\varepsilon_{2n-2})^2 \\ &< \varepsilon_{2n}5M/\varepsilon_{2n-2} + RS^n\varepsilon_{2n-1}25M^2/\varepsilon_{2n-2}^2 \\ &< 50M^2S^{n+1}\varepsilon_{2n-1}/\varepsilon_{2n-2}^2 < \varepsilon_{2n-2}/2.\end{aligned}$$

Let $|w| < S$. Then there exists z as above such that $|w - z| < \varepsilon_{2n-2}/4M$. So $|f^*(w) - g^*(w)| \leq |f^*(w) - f^*(z)| + |f^*(z) - g^*(z)| + |g^*(z) - g^*(w)| < \varepsilon_{2n-2}/4 + \varepsilon_{2n-2}/2 +$

$\varepsilon_{2n-2}/4 = \varepsilon_{2n-2}$. By induction there exists a permutation π such that for all $j < n$ there is $\pi j < n$ such that $|c_j - d_{\pi j}| < \varepsilon$. Set $\pi n = n$. $\dashv$

We cannot show that all nonzero polynomials over $\mathbf{C}$ have an invertible leading coefficient, so we need to consider polynomials that are 'almost-monic.'

3.11 Lemma. *Let f and g be polynomials over $\mathbf{C}^a$ such that f is monic and of degree n, and g is of degree at most m. Let $0 < \varepsilon < 1/2$ be such that $|g| < (\varepsilon/(2|f|))^{m+n+1}$. If c is a root of $g(X)X^{n+1} + f(X)$, then exactly one of the following holds:*

1. *$|c| > |f|/\varepsilon$, and $|1/c - 1/d| < \varepsilon/|f|$ for some root d of $g(X)X + 1$.*
2. *$|c| < |f|$, and $|c - d| < \varepsilon$ for some root d of $f(X)$.*

Proof: Let c be a root of $g(X)X^{n+1} + f(X)$. Then $|c| \geq 2|f|$ or $|c| < 2|f|$. Suppose $|c| \geq 2|f|$. Then $|g(c)c + 1| \leq (|f| - 1)/|c| < 1/2$. So $|c|^{m+1}|g| \geq |g(c)c| > 1/2$. Thus $|c|^{m+1} > (|f|/\varepsilon)^{m+1}$, hence $|c| > |f|/\varepsilon$. Also, $|(g(c)c + 1)/c^{m+1}| < (\varepsilon/|f|)^{m+1}$. So $|1/c - e| < \varepsilon/|f|$ for some root $e = 1/d$ of the monic polynomial $(g(1/X)/X + 1)X^{m+1}$.

Suppose $|c| < 2|f|$. Then $|f(c)| \leq |g(c)c^{n+1}| \leq |g||c|^{m+n+1} < |g|(2|f|)^{m+n+1} < \varepsilon^n$. So there is a root d of $f(X)$ such that $|c - d| < \varepsilon$. $\dashv$

3.12 Lemma. *Let $F = a_nX^n + \cdots + a_0$ be a polynomial over $\mathbf{C}$ such that a_j is a unit. Then there exists $k \geq j$ such that a_k is a unit, and a monic polynomial F^* over $\mathbf{C}$ of degree k, such that F^* divides F. If the coefficients of F are (modulated) Cauchy numbers, then so are the coefficients of F^*.*

Proof: By induction on $n - j$. Write $F = a_j(b_nX^n + \cdots + b_0)$, let $r = |X^j + b_{j-1}X^{j-1} + \cdots + b_0|$, and $s = |b_nX^n + \cdots + b_{j+1}X^{j+1}|$. Then $s > 1/(2(6r)^n)$ or $s < 1/(6r)^n$. If $s > 1/(2(6r)^n)$, then a_k is a unit for some $k > j$: Apply induction. Suppose $s < 1/(6r)^n$. By continuity there exists $\gamma > 0$ such that $s + (n - j)\gamma < 1/(6(r - j\gamma))^n$. Let $\delta = |a_j|\gamma/4$. If h is a polynomial over $\mathbf{C}^a$ of degree at most n such that $|h - F| < \delta$, then it has exactly j roots $c_1, \ldots, c_j$, counting multiplicities, satisfying $|c_i| < |h|$. Define $h^* = \prod_i (X - c_i)$. Then h^* is a monic polynomial of degree j that divides h. By Lemmas 3.10 and 3.11, for all $\varepsilon > 0$ and for all G over $\mathbf{C}$ of degree at most n such that $|G - F| < \delta$ there exists $\delta_1 > 0$ such that if h_1, h_2 are polynomials over $\mathbf{C}^a$ of degree at most n satisfying $|h_i - G| < \delta_1$, then $|h_1^* - h_2^*| < \varepsilon$. So the maps $h \mapsto h^*$ and $h \mapsto h/h^*$ can be continuously extended to all G over $\mathbf{C}$ of degree at most n that satisfy $|G - F| < \delta$. In particular, F^* divides F. $\dashv$

The continuity of the map $h \mapsto h^*$ cannot be strengthened to a continuous map to some linear factor of h^*, since in general the permutation π in Lemma 3.10 need not be uniquely determined.

3.13 Theorem (Fundamental Theorem for (modulated) Cauchy complex numbers). *Each polynomial $f(X)$ over the (modulated) Cauchy complex numbers having an invertible coefficient for some positive power of X has a (modulated) Cauchy root.*

Proof: We may assume f to be a monic polynomial $X^n + a_1X^{n-1} + \cdots + a_n$, where each a_j is the limit of a (modulated) rational Cauchy sequence $\{a_{j,m}\}_m$. We construct a sequence $\{c_m\}_m$ of roots $c_m \in \mathbf{C}^a$ of $f_m = X^n + a_{1,m}X^{n-1} + \cdots + a_{n,m}$ as follows: Choose for c_0 one of the roots of f_0. From c_{m-1} we select for c_m from among the roots of f_m the one that is closest to c_{m-1}, that is, $|c_{m-1} - c_m| \leq |c_{m-1} - d|$ for all roots d of f_m. If there is no unique choice, then select the one with largest real part. If there are still two choices left, select the one with largest imaginary part. Then $\{c_m\}_m$ is a (modulated) Cauchy sequence whose limit is a root of f. ⊣

The uniqueness of the choice of c_m in the proof of Theorem 3.13 implies that the sequence $\{c_m\}_m$ is uniquely determined by a finite description, and no choice principles are needed.

Theorem 3.13 does not extend to all of $\mathbf{C}$: We cannot find a continuous solution $X(c)$ to the equation $X^2 + c = 0$ when $c \in \mathbf{C}$ is near 0.

3.14 Theorem. *Let $n > 1$, and let $F = X^n + a_1 X^{n-1} + \cdots + a_n$ be a polynomial over $\mathbf{C}$ such that there exists j satisfying $n^j a_j \neq \binom{n}{j} a_1^j$, that is, $n^j a_j - \binom{n}{j} a_1^j$ is a unit. Then F has a proper monic factor F^* such that F^* and F/F^* are strongly relatively prime.*

Proof: Given F, there exists $\gamma > 0$ such that $|(X + c)^n - F(X)| > \gamma$, for all c. So there exist ε, μ such that for all monic polynomials g over $\mathbf{C}^a$ of degree n, if $|g - F| < \mu$, then $|g| < 2|F| = R$ and g has roots c, d with $|c - d| > 2n\varepsilon$. For n, ε, R, there exists $\delta < \mu$ satisfying Lemma 3.10. Choose a monic polynomial $g = \prod_j (X - c_j)$ of degree n over $\mathbf{C}^a$ such that $|g - F| < \delta/3$. The equivalence relation on the roots of g generated by the binary relation $|c_j - c_k| < 2\varepsilon$ contains at least two distinct equivalence classes, and can be extended to a decidable equivalence relation $\sim$ that divides the collection of roots into exactly two equivalence classes C and D. For all monic polynomials $h = \prod_j (X - d_j)$ of degree n over $\mathbf{C}^a$ such that $|h - g| < \delta/2$, there is a permutation π such that $|c_j - d_{\pi j}| < \varepsilon$. The equivalence relation on the roots of g induces an equivalence relation on the roots of h, dividing them into two equivalence classes as well, say C' and D'. These classes are independent of π. Define $h^* = \prod_{d \in D'} (X - d)$. The map $h \mapsto h^*$ can be continuously extended to all monic G over $\mathbf{C}$ of degree n that satisfy $|G - g| < \delta/2$. Let $h^\circ = h/h^*$. There are unique polynomials h_* and $h_\circ$ with h_* of degree less than deg h° and $h_\circ$ of degree less than deg h^*, such that $h^* h_* + h^\circ h_\circ = 1$. The maps $h \mapsto h^\circ$, $h \mapsto h_*$, and $h \mapsto h_\circ$ are continuous wherever h^* is. So F^* is a proper monic factor of F, and F^* and $F^\circ = F/F^*$ are strongly relatively prime. ⊣

A polynomial f over $\mathbf{C}$ has a *simple root* α if $f(\alpha) = 0$ and $f'(\alpha)$ is invertible. The existence of a simple root for a monic polynomial can be expressed in terms of its coefficients. The following approach is from [13]. Let R be a commutative ring, and let $f = (Y + X_1)(Y + X_2) \ldots (Y + X_n) = Y^n + a_1 Y^{n-1} + \cdots + a_n$ be the polynomial over $R[X_1, \ldots, X_n]$ with as coefficients the elementary symmetric polynomials $a_j = \sigma_j(X_1, \ldots, X_n)$. To express that $-X_j$ is a simple root of f, we need that $E_j = \prod_{k \neq j} (X_j - X_k) \neq 0$, where $x \neq y$ stands for $x - y$ is a unit. So for f to have a simple root we need at least one $E_j \neq 0$. So $(Y + E_1)(Y + E_2) \ldots (Y + E_n) \neq Y^n$, that is, $\sigma_j(E_1, \ldots, E_n) \neq 0$ for some j. These polynomials are symmetric, so there exist polynomials $d_j(Y_1, \ldots, Y_n)$ such that $d_j(a_1, \ldots, a_n) = \sigma_j(E_1, \ldots, E_n)$. Define f to be *unramifiable*, if $d_j(a_1, \ldots, a_n) \neq 0$ for some j.

3.15 Theorem. *Each unramifiable monic polynomial over $\mathbf{C}$ has a simple root.*

Proof: By Theorem 3.14, an unramifiable monic polynomial f of degree $n > 1$ has a proper factorization $f = gh$, for monic g, h. Then g or h is unramifiable again. By induction on n, g or h has a simple root, which is a simple root of f. $\dashv$

3.16 Theorem. *Let $r \in \mathbf{R}$, and let $a_1(Y), \ldots, a_n(Y)$ be rational functions over $\mathbf{C}^a$ such that $a_j(r)$ exists, for all j. Then $f(X,r) = X^n + a_1(r)X^{n-1} + \cdots + a_n(r)$ splits in $\mathbf{C}$.*

Proof: We may assume that $n > 1$. We proceed by induction on n. There are rational numbers p and q such that $p < r < q$, and $a_j(s)$ exists for all $p \leq s \leq q$ and all j. If the inequality $\mathrm{GCD}(f(X,Y), \frac{\partial f}{\partial X}(X,Y)) \neq 1$ over $\mathbf{C}^a(Y)$ has infinitely many solutions $Y = s \in \mathbf{R}^a$ with $p \leq s \leq q$, then, by Theorem 2.1, $f(X,Y)$ and $\frac{\partial f}{\partial X}(X,Y)$ share a nonconstant factor $g(X,Y)$ over $\mathbf{C}^a(Y)$ that is monic in X. So $g(X,r)$ is a proper factor of $f(X,r)$: Apply induction. Otherwise, let $p \leq d_1 < \cdots < d_m \leq q$ be the finite set of solutions of the inequality. Set $p = d_0$ and $q = d_{m+1}$. By Lemma 3.10 we can find roots $c_1(t), \ldots, c_n(t)$ of $f(X,t)$ that are continuous in $t \in \mathbf{R}$ on each interval (d_j, d_{j+1}). Continuous roots of neighboring intervals can be pairwise connected to make a continuous solution on the whole interval (p,q), because the roots of $f(X, d_j)$ are discrete sets. $\dashv$

The constructions of the continuous solutions $c_k(t)$ in the proof above essentially use that the intervals (d_j, d_{j+1}) are simply connected. Theorem 3.16 does not apply to the polynomial $X^2 + c$ with $c \in \mathbf{C}$, since a complex number depends on two real values rather than one: Its real and its imaginary part.

References

[1] E. Bishop, D. Bridges, *Constructive Analysis*, Grundlehren der mathematischen Wissenschaften, Vol. 279, Springer, 1985.

[2] D. Bridges, F. Richman, *Varieties of Constructive Mathematics*, London Mathematical Society Lecture Note Series, Vol. 97, Cambridge University Press, 1987.

[3] M. Cantor, *Vorlesungen über Geschichte der Mathematik, Vol. 4*, Teubner Verlag, Leipzig, 1908.

[4] M. P. Fourman, C. J. Mulvey, D. S. Scott (editors), *Applications of Sheaves*, Lecture Notes in Mathematics, Vol. 753, Springer, 1979.

[5] R. Goldblatt, *Topoi, the categorial analysis of logic*, Studies in logic and the foundations of mathematics, Vol. 98, North–Holland, 1979.

[6] A. Joyal, G. E. Reyes, *Separably real closed local rings*, Journal of Pure and Applied Algebra **43** (1986), 271–279.

[7] R. Mines, F. Richman, W. Ruitenburg, *A Course in Constructive Algebra*, Universitext, Springer, 1988.

[8] F. Richman, *Separable extensions and diagonalizability*, the American Mathematical Monthly **97** (1990), 395–398.

[9] W. Ruitenburg, *Inequality in constructive mathematics*, Department of Mathematics, Statistics and Computer Science, Marquette University, Technical Report No. 285 (1988).

[10] [redacted] T. von Schubert, *De inventione divisorum*, ad annum 1793, Nova acta scient. imp. Petropolitanae. Petropoli **11** (1798), 172–182.

[11] [redacted] S. Troelstra, D. van Dalen, *Constructivism in Mathematics, An Introduction, Vol. I*, Studies in logic and the foundations of mathematics, Vol. 121, North–Holland, 1988.

[12] [redacted] S. Troelstra, D. van Dalen, *Constructivism in Mathematics, An Introduction, Vol. II*, Studies in logic and the foundations of mathematics, Vol. 123, North–Holland, 1988.

[13] [redacted] C. Wraith, *Generic Galois theory of local rings*, [4], 739–767.