Roots of polynomials in fields of generalized power series

Julia F. Knight*, Karen Lange, and Reed Solomon

September 11, 2017

Thanks to Rod for some mathematics

There is important work connecting computability with various branches of mathematics outside logic—algebra, number theory, geometry, and analysis. Rod Downey has done beautiful work of this kind.

Two papers

- "The isomorphism problem for torsion-free Abelian groups is analytic complete," Downey and Montalbán.
- "Reverse mathematics, Archimedean classes, and Hahn's Theorem," Downey and Solomon.

Familiar fields and their elementary first order theories

$\mathbb{C}$—field of complex numbers
$\mathbb{R}$—ordered field of real numbers

1. $Th(\mathbb{C})$ is the theory of algebraically closed fields of characteristic 0.

   Models of $Th(\mathbb{C})$ are determined, up to isomorphism, by their transcendence degree.

2. $Th(\mathbb{R})$ is the theory of real closed ordered fields.

   Models of $Th(\mathbb{R})$ with the Archimedean property are isomorphic to elementary substructures of $\mathbb{R}$. We can obtain non-archimedean real closed ordered fields using Compactness, or by algebraic constructions. I will describe two such.

Puiseux series

Definition. Let K be a field. The *Puiseux series* over K are formal power series $s = \sum_{i \geq z} a_i t^{\frac{i}{n}}$, where $n \in \mathbb{N} - \{0\}$, $z \in \mathbb{Z}$, $a_i \in K$.

Notation: $K\{\{t\}\}$—set of Puiseux series with coefficients in K.

Operations. Addition and multiplication—as for ordinary power series.

Valuation. $K\{\{t\}\}$ has valuation w, where

- $w(s)$ is exponent in first non-zero term, if $s \neq 0$,
- $w(s) = \infty$ if $s = 0$.

Order. If K is ordered, so is $K\{\{t\}\}$—$s > 0$ if $t^{w(s)}$ has positive coefficient.

Newton-Puiseux Theorem

Theorem (Newton, 1676; Puiseux, 1850-51).

- If $K \equiv \mathbb{C}$, then $K\{\{t\}\}$ is algebraically closed.
- If $K \equiv \mathbb{R}$, then $K\{\{t\}\}$ is real closed.

I will say how to find a root of a polynomial.

Finding roots, as Newton did

For simplicity, suppose $K \equiv \mathbb{C}$. Let $p(x) = A_0 + A_1 x + \cdots + A_n x^n$, where $A_j \in K\{\{t\}\}$. If $A_0 = 0$, then 0 is a root. Suppose $A_0 \neq 0$.

(Draw *Newton polygon*.)

Consider side with first point $(i, w(A_i))$, last point $(j, w(A_j))$.

- $\nu = \frac{w(A_i) - w(A_j)}{j - i}$ is valuation of a root.
- *carrier* Δ_ν—set of pairs $(i, w(A_i))$ on side.
- *ν-principal part*—polynomial $\sum_{k \in \Delta_\nu} c_k z^{k-i}$, where c_k—first non-zero coefficient in A_k.
- For a root with valuation ν, the coefficient b of t^ν is a root of the ν-principal part.

Given $r_1 = bt^\nu$ the first term of a root, find second term $b' t^{\nu'}$ using $q(x) = p(r_1 + x)$. Let $r_2 = bt^\nu + b' t^{\nu'}$. Continue.

Complexity and representation of Puiseux series

Question: How hard is it to find a root of a polynomial?

To answer the question, we must first say how we plan to represent elements of $K\{\{t\}\}$.

Representation. Use a function $f : \omega \to K \times \mathbb{Q}$ s.t. if $f(n) = (a_n, q_n)$, then

- q_n increases with n,
- there is a uniform bound on the denominators of the q_n's.

Note: q_n is defined for all n. This, plus fact that denominators are bounded, implies that $\lim_{n\to\infty} q_n = \infty$.

Complexity of basic operations

Lemma.

1. Applying uniform effective procedures to K and $s, s' \in K\{\{t\}\}$, we compute $s + s'$, $s \cdot s'$.
2. It is Π^0_1 in K and s to say $s = 0$.
3. If $s \neq 0$, then we can effectively find $w(s)$.

Complexity of root-taking process

Rough result. Let I be jump ideal. Suppose $K \in I$, and let R be set of elements of $K\{\{t\}\}$ with representation in I. Then R is algebraically closed.

We can do better.

More precise results

Theorem. There is uniform Δ_2^0 procedure that, given K and sequence of coefficients for non-trivial polynomial $p(x) = A_0 + A_1 x + \ldots + A_n x^n$ over $K\{\{t\}\}$, yields a root.

Proceed by Newton's method. Use Δ_2^0 to decide which coefficients are 0. The rest is computable.

Theorem. If I is a Turing ideal, then for $K \in I$, algebraically closed of characteristic 0, every non-trivial polynomial over $K\{\{t\}\}$ with coefficients in I has a root in I.

We proceed non-uniformly. We give ourselves enough information to say which coefficients in the initial polynomial are 0, and to find a bound on the denominators for the coefficients. For succeeding steps, we must play detective.

Hahn fields

Let K be a field, and let G is a divisible ordered Abelian group.

Definition. The *Hahn field* $K((G))$ consists of formal sums $s = \sum_{g \in S} a_g t^g$, where $S \subseteq G$ is well ordered and $a_g \in K$.

- The *support* of s is $\{g \in S : a_g \neq 0\}$.
- The *length* of s is the order type of $Supp(s)$.

Operations. Addition and multiplication, and the valuation function w, are defined as expected. If K is ordered, then so is $K((G))$, with expected ordering.

Generalized Newton-Puiseux Theorem

Theorem (Maclane, 1939). Let G be a divisible ordered Abelian group.

- If $K \equiv \mathbb{C}$, then $K((G))$ is algebraically closed.
- If $K \equiv \mathbb{R}$, then $K((G))$ is real closed.

Complexity and representation

Question. How hard is it to find a root of a polynomial?

We first say how we plan to represent Hahn series.

Representation. To represent $s \in K((G))$, we use a function f from an ordinal α to $K \times G$ s.t. the second component of $f(\beta)$ increases with $\beta < \alpha$.

Rough result for Hahn fields

Proposition (K-Lange-Solomon). Let A be a countable "admissible" set. Let $K \equiv \mathbb{C}$, and let G be a divisible ordered Abelian group, both in A. Let R be the set of elements of $K((G))$ represented in A. Then R is algebraically closed.

What is an admissible set?

Admissible sets

An *admissible set* is a transitive set A satisfying the axioms of Kripke-Platek set theory (KP). In KP, we have some of the axioms of ZF, but power set is dropped, and replacement and collection are restricted to formulas with just bounded quantifiers.

Example. $L_{\omega_1^{CK}}$ is the least admissible set that contains ω.

Important for us: In an admissible set, we can define functions f on ordinals by Σ_1 *recursion*—there is a finitary Σ_1-formula saying how to pass from $f|\alpha$ to $f(\alpha)$ (a Σ_1-formula has only existential and bounded quantifiers).

Computing in an admissible set

In an admissible set A, we have the following non-standard notions of computability.

1. $S \subseteq A$ is A-c.e. if it is defined in $(A, \in)$ by a Σ_1-formula.
2. A partial function f is A-computable if the graph is A-c.e. Most often, we define a partial recursive function f on ordinals in A by Σ_1 recursion.

Rough result

Rough Theorem (K-Lange-Solomon). Let A be a countable admissible set. Let K be an algebraically closed field and let G be a divisible ordered Abelian group, both elements of A. Let R be the set of elements s of $K((G))$ represented in A. Then R is algebraically closed.

Idea of proof: Given non-trivial polynomial $p(x)$ with coefficients in R, define, by Σ_1-recursion on ordinals α, a sequence of initial segments r_α of a root r. The length of r_α is α, until/unless we come to a root. After that, the sequence is constant.

We need to know that some r_α is a root. For this, we need bounds on lengths.

Lengths of roots

K-Lange. If $p(x)$ is a polynomial with coefficients of lengths $\alpha_0, \alpha_1, \ldots, \alpha_n$, and γ is a limit ordinal with $\alpha_0 + \alpha_1 + \ldots + \alpha_n < \gamma$, then all roots of $p(x)$ have length less than ω^{ω^γ}.

To complete proof of Rough Theorem, we note that for if the α_i's are in A, we can take $\gamma \in A$, and then $\omega^{\omega^\gamma} \in A$. So, for some $\alpha \in A$, r_α is a root, and $r_\alpha \in A$.

What if A is uncountable?

Corollary (K-Lange-Solomon). Let A be an uncountable admissible set. Suppose $K \equiv \mathbb{C}$, G a divisible ordered Abelian group, both in A. Let R be the set of elements of $K((G))$ represented in A. Then R is algebraically closed.

We can reduce to the countable case, using Downward Löwenheim-Skolem Theorem and Levy collapse.

Future work

Question: Given K, G, and a polynomial $p(x)$ with coefficients $A_i \in K((G))$, how hard is it (how many jumps) are need to compute r_α ?

How to get bounds on lengths

Definition. A subfield R of $K((G))$ is *truncation-closed* if it contains all truncations (initial segments) of its elements. We say that R is *closed* in $K((G))$ if

1. R is truncation closed,
2. $K \subseteq R$,
3. R is relatively algebraically closed in $K((G))$.

tc-basis, canonical sequence

Definitions. Let R be a closed subfield of $K((G))$. We call $(r_\alpha)_{\alpha<\gamma}$ a *tc-basis* for R, and we call $(R_\alpha)_{\alpha\leq\gamma}$ a *canonical sequence* for R if the following conditions hold:

1. R_α is the set of elements of $K((G))$ algebraic over $K \cup \{r_\beta : \beta < \alpha\}$,
2. $r_\alpha \in R - R_\alpha$,
3. for each $\alpha < \gamma$, either
   (a) $r_\alpha = t^g$ for some $g \in G$, or
   (b) r_α has limit length, with all proper truncations in R_α,
4. $R_\gamma = R$.

Bounding Theorem

Theorem (K-Lange). Let R be a closed subfield of $K((G))$, and suppose γ is a countable limit ordinal.

1. If R has a *tc*-basis of length γ, then all elements of R have length less than $\omega^{\omega^{\gamma}}$.
2. If R has a *tc*-basis of length $\gamma + n$, where n is a positive integer, then all elements have length less than $\omega^{\omega^{\gamma+n}} \cdot \omega^{\omega^{\gamma}}$.

Proposition (K-Lange). These bounds are sharp.