# ALGEBRAIC CLOSURE OF FUNCTION FIELDS

RONAN ZWEIFLER

## 1. Abstract

This paper will assert and prove the Newton-Puiseux theorem formally and informally. We will also briefly discuss the significance and application of the theorems, followed by an exploration into fields of positive characteristic.

## 2. Introduction

The Newton-Puiseux theorem is a theorem that relates the algebraic closure of all two-variable polynomials to a special type of power series with fractional exponents. The theorem essentially says that all two-variable functions with coefficients in the complex numbers, with any number of terms and any size, can be factored into factors that resemble single-variable Puiseux series, or power series with fractional exponents. The theorem in its essentials was discovered by Issac Newton in 1675, but was later rediscovered and proven by Puiseux in 1850.

In 1675, Newton used his understanding of the theorem to create a method for estimating certain two-variable functions that were particularly difficult to solve for. Specifically, he developed a geometric method for determining the first few terms of a Puiseux series in one variable that would estimate some branch of a function, called the Newton Polygon, which we will go more in depth into later in this paper.

Puiseux's proof for the theorem would add the rigor to the understanding that Newton had made almost 200 years earlier. With the discovery and proliferation of abstract algebra, Puiseux was able to use the properties of fields and rings to prove the theorem across all two-variable polynomials with complex coefficients.

*Date*: July 14, 2025.

This paper will explain a few of the basic concepts of ring and field theory, prove the theorem, and then talk about some extensions of the proof into fields with different properties, and positive characteristic.

## 3. Definitions and basic concepts

### 3.1. Basic Concepts.

**Definition 3.1** (A Group)**.** A *group* is a set $G$ together with a binary operation $\times : G \times G \to G$ satisfying the following axioms:

(1) **Associativity:** For all $a, b, c \in G$, we have $(a \times b) \times c = a \times (b \times c)$.
(2) **Identity element:** There exists an element $e \in G$ such that for all $a \in G$, $e \times a = a \times e = a$.
(3) **Inverse element:** For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \times a^{-1} = a^{-1} \times a = e$.

If, in addition, the operation is commutative (ie, $a \times b = b \times a$ for all $a, b \in G$), then $G$ is called *abelian group*, which is the type of group that we will be working with in this paper.

**Definition 3.2** (A Ring)**.** A *ring* is a set $R$ equipped with two binary operations, addition $(+)$ and multiplication $(\times)$, such that:

(1) **Additive group:** $(R, +)$ is an abelian group. That is:
    (a) (Associativity) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
    (b) (Identity) There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.
    (c) (Inverses) For each $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$.
    (d) (Commutativity) $a + b = b + a$ for all $a, b \in R$.
(2) **Multiplication is associative:** For all $a, b, c \in R$, we have $(a \times b) \times c = a \times (b \times c)$.
(3) **Distributive laws:** For all $a, b, c \in R$, the following hold:
    (a) $a \times (b + c) = a \times b + a \times c$,
    (b) $(a + b) \times c = a \times c + b \times c$.

If multiplication is also commutative (i.e., $a \times b = b \times a$ for all $a, b \in R$), the ring is called a *commutative ring*. If there exists a multiplicative identity element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$, then $R$ is called a *ring with unity* or a *unital ring*.

**Definition 3.3** (A Field)**.** A Field is a commutative ring where each element has a multiplicative inverse. It is important to note that the rules of $F$ create divisions by zeros, and it should be assumed that all rules follow that undefined division, i.e. none of them create valid divisions by 0.

## 3.2. **Field Theory Concepts.**

**Definition 3.4** (A Quotient Field)**.** A quotient field is a field created by dividing all elements of a ring by all other elements, then rejecting all divisions by zero, and setting equivalence relations for all fractions that have the same ratios ($\frac{2}{6} = \frac{1}{3}$). A quotient field is also sometimes called a field of fractions, and it is denoted $\mathbf{Frac}(R)$, where $R$ is a ring.

**Example 3.1.** $\mathbf{Frac}(\mathbb{Z}) = \mathbb{Q}$.

**Example 3.2.** $\mathbf{Frac}(\mathbb{Q}[x]) = \mathbb{Q}(x)$*, the field of all rational functions with coefficients in* $\mathbb{Q}$.

**Definition 3.5** (Extensions)**.** An *extension*, typically to a ring or field, adds one or more elements to the ring or field, or extends the ring or field to give it more properties.

Let $R$ be a ring. $R[a]$ is the ring $R$ with $a$ adjoined to the ring.

*Remark* 3.1. While this may be clear to most of you, by adding $a$, the rules of rings dictate that $a^n$, $a^n + r \mid \forall r \in R$, and $a^n \times r \mid \forall r \in R$ where $n \in \mathbb{N}$.

Let $F$ be a field. $F(a)$ is the field $F$ with $a$ adjoined to the field.

*Remark* 3.2. The same thing that applies to rings also applies to fields, where extra elements are created by the rules of fields.

**Example 3.3.** *The ring of all polynomials in the indeterminate (or variable)* $x$ *with coefficients in the ring* $R$ *is written as* $R[x]$.

**Example 3.4.** *The field of all rational functions in indeterminate (or variable) $x$ with coefficients in the field $F$ is written as $F(x)$.*

There are also times when fields or rings are extended to include more than one elements, or extended to create a larger field with more properties.

Let $K, F \mid F \subset K$. We say $K/F$ is a field extension of $F$.

*Remark* 3.3. We use the operator / to denote setting all the elements in the below field equal to zero in the above field, so $K/F$ gives all the elements that are added to $F$ that create the larger extended field $K$.

In addition to extensions, fields have many interesting properties and adjectives that we use to describe them.

**Definition 3.6** (Characteristic)**.** A field or ring *Characteristic*, written $\mathbf{Char}(R)$, or $\mathbf{Char}(F)$, is the smallest sum of the ring's (or field's) multiplicative identity 1 that will sum to the additive identity 0. If no such number exists, the ring (or field) is said to have characteristic zero.

**Example 3.5.** *The ring of integers modulo some prime $p$, written $\mathbb{Z}_p$, $\boldsymbol{Char(\mathbb{Z}_p) = p}$, $\forall p \in \mathbb{P}$. Which I leave you to think about given the definition.*

**Definition 3.7** (Splitting Field)**.** Let $F$ be a field. Let $P(x)$ be some polynomial $P(x) \in F[x]$. A splitting field is a the smallest field extension that allows for the factorization, or splitting of $P(x)$.

**Example 3.6.** *Let $P(x) = x^2 - 2$ and $\mathbb{Q}$ be the field of all rational numbers. We know $P(x) \in \mathbb{Q}[x]$. To factor this, we would need $\sqrt{2}$ in our original field. So our splitting field would be $\mathbb{Q}(\sqrt{2})$. I'll let you think about this and figure it out.*

**Definition 3.8** (Algebraic Closure)**.** We say a field $F$ is algebraically closed if $F \supset F(P(x) = 0), \forall P(x) \in F[x]$. In simpler terms, all polynomials with coefficients in an algebraically closed

field, have their roots in that same algebraically closed field. Sometimes we want to denote an extended version of our field that is algebraically closed, we denote this new field as, $\bar{F}$.

**Example 3.7.** *The $\bar{\mathbb{Q}}$ is $\mathbb{C}$, and by definition is algebraically closed. I leave you to justify this.*

*Remark* 3.4. You can also think about algebraically closed fields as fields that are closed under exponentiation or that form a group with exponentiation as their binary operation.

**Definition 3.9** (Formal Power Series)**.** The formal power series is the ring of all power series with coefficients in some ring or field. With some ring $R$, the formal power series is denoted $R[[x]]$.

Formal Power series does not mean all convergent power series, some power series in the ring of formal power series, actually most, are not convergent. We use a special notation to denote the ring of all **convergent** power series: $R\{x\}$.

*Remark* 3.5. It should be noted that $R[x] \subset R[[x]]$. All elements of $R[[x]]$ can be expressed in the form:

$$\sum_{n=0}^{\infty} a_n x^n \mid a_n \in R.$$

But if $a_n$ can be any element of $R$, and $0 \in R$ then $a_n$ could be 0. So if we have what looks to be the polynomial $ax^2 + bx + c$, in our power ring, this polynomial is actually

$$c + bx + ax^2 + 0x^3 + 0x^4 + \cdots .$$

It just so happens that $R[[x]]$ is just $R[x]$ that includes all infinite series in $x$. The concept of a formal power series ring is vital to the understanding of this paper.

**Definition 3.10** (Function Fields)**.** A function field is any field who contains elements that are functions of some indeterminate, or variable. While this is not a formal definition, this is perfectly adequate for the purposes of this paper. We have some of these. $F(x)$ or the field $F$ adjoin $x$ is a function field.

**Definition 3.11** (order)**.** Order has lots of different definitions, but for the purposes of this proof its definition goes like this:

Let $\phi(z)$ be a polynomial. $\mathbf{ord}(\phi(z))$ is equal to the lowest degree term in $\phi(z)$

**Example 3.8.**

$$\phi(z) = 2z^2 + 3z^3 + 4z^4 + \cdots + nz^n.$$

$$\mathbf{ord}(\phi(z)) = 2.$$

3.3. **Less Abstract Terms.**

**Definition 3.12** (Formal Laurent Series)**.** The Laurent series is simply a power series that accounts for complex coefficients:

$$\sum_{n=0}^{\infty} a_n x^n \mid a_n \in \mathbb{C}.$$

However, the formal Laurent Series generalizes this concept to series that don't necessarily converge or follow typical power series behaviors. We will denote the ring of formal power series over $\mathbb{C}$ as $\mathbb{C}[[x]]$.

**Definition 3.13** (Formal Puiseux Series)**.** A Puiseux series is a Laurent series that accounts for fractional exponents. Its formalization is the same thing. It is written as $\mathbb{C}[[x^n]] \mid n \in \mathbb{N}$ or $\mathbb{C}\langle\langle x \rangle\rangle$.

Both of these definitions are considered to be function rings. Later in the formal proof we will create quotient fields out of both of these rings.

## 4. The Newton-Puiseux Theorem

4.1. **Preface.** It is important that, given the relative newness of all the topics mentioned previously in the basic concepts section of this paper, you actually conceptually understand the Newton-Puiseux theorem so that you understand why it is significant and how we can use it to do interesting math. This section will be broken up into two separate subsections; one, denoted "The Conceptual Proof" will be an informal walk-through of the theorem and

why it works. The second section, denoted "The Formal Proof" will be a classical and formal proof of theorem that checks all the boxes of a rigorous proof.

That being said, it is now time that we actually state the Newton-Puiseux theorem:

**Theorem 4.1** (The Newton-Puiseux Theorem)**.** *Given an algebraic polynomial whose coefficients are polynomials over a field of characteristic zero, every solution of the polynomial can be expressed as a Puiseux series.*

In its essence, the theorem relates the algebraic closure of any polynomial with polynomial coefficients to be the field of puiseux series, and with our notation, we can states the theorem properly, going from least general to most:

$$\overline{\mathbb{C}[x]} = \mathbb{C}\langle x\rangle,$$
$$\overline{\mathbb{C}[[x]]} = \mathbb{C}\langle\langle x\rangle\rangle,$$
$$\overline{\mathbb{C}[[x]]} = \mathbb{C}\langle\langle x\rangle\rangle \mid P(x,y) \in \mathbb{C}[[x]][[y]].$$

*Remark* 4.1. It should be noted here that when we say $\overline{\mathbb{C}[x]}$, we do not mean the algebraic closure of the field with respect to the indeterminate $x$, as this would be the complex numbers, rather we take all polynomials in $x$ (with coefficients in $\mathbb{C}$), and create new polynomials in $t$, or $y$ with coefficients that are themselves these polynomials in $x$, then we "algebraically close" that ring or field instead. This will be elaborated on further in the next section.

4.2. **The Conceptual Proof.** Let $P(x, y)$ be some two variable polynomial, with finite or infinity many terms, and with finite or infinity large coefficients. If this is true, and we allow these terms and coefficients to exist in the complex numbers, then we know $P(x, y) \in \mathbb{C}[[x]][[y]]$, or said, the ring of all power series in $y$ with coefficients in the ring of all power series in $x$ with coefficients in the field of all complex numbers $\mathbb{C}$.

**Example 4.1.** *Let us look at a possible $P(x, y)$, and we will organize our terms in a typical binomial fashion:*

$$P(x,y) = c_0y^a + c_1y^bx^A + c_2y^cx^B + \cdots + c_nx^n.$$

*Let us treat $x$ like a constant. Now we can consolidate our $P(x,y)$ into a one variable function $P(y)$:*

$$P(y) = c_xy^a + c_{x1}y^b + c_{x2}y^c + \cdots + c_n.$$

*The fundamental Theorem of algebra says that we can split this $P(y)$ into its liner factors, which might resemble:*

$$0 = P(y) = (y - a_x)(y - a_{x2})(y - a_{x3}) \cdots (y - a_{xn}).$$

*But remember, because each we treated our variable $x$ like a constant and consolidated it, each of our $a_{xn}$ roots are themselves functions of $x$.*

The Newton-Puiseux theorem just says that each of these $a_{xn}$ roots will be $\in \mathbb{C}\langle\langle x\rangle\rangle$. I.e, the extension from $\mathbb{C}[[x]]$ to $\mathbb{C}\langle\langle x\rangle\rangle$ algebraically closes, or allows us to factor all $P(x,y)$ in $\mathbb{C}[[x]][[y]]$.

## 5. The Formal Proof

5.1. **Preface to the Formal Proof.** There are many parts of a formal abstract algebra proof that are done in redundancy or are shown completely to prove rigor. Readers should consult the basic concepts section of this paper when confused.

5.2. **The Formal Proof.** Let $\mathbb{C}[[x]]$ and $\mathbb{C}\{x\}$ denote formal and convergent power series over $\mathbb{C}$.

Let $\mathbb{C}((x)) :=$ **Frac(**$\mathbb{C}[[x]]$**)** and $\mathbb{C}(\{x\}) :=$ **Frac(**$\mathbb{C}\{x\}$**)** .

Any Puiseux series in any form is some power series $f(z^{1/r}) \mid f(z) \in \mathbb{C}[[x]]$ (or $\mathbb{C}\{x\}$) where $r \in \mathbb{N}$.

Let $\mathbb{C}[[z^*]]$ and $\mathbb{C}\{z^*\}$ be the ring of formal puiseux and convergent puiseux series respectively.

Let $\mathbb{C}((x^*)) := \mathbf{Frac}(\mathbb{C}[[z^*]])$ and $\mathbb{C}(\{x^*\}) := \mathbf{Frac}(\mathbb{C}\{z^*\})$.

Any element $\phi(z) \in \mathbb{C}((x^*))$ can be written as $\sum_{k=n}^{\infty} a_k \cdot z^{k/r}$ with $r \in \mathbb{N}$, $n \in \mathbb{Z}$, $a_k \in \mathbb{C}$; when $a_n \neq 0$, we say that $\phi(z)$ is of order $n/r$, $\mathbf{ord}(\phi(z)) = n/r$. The units of the rings $\mathbb{C}[[z]]$, $\mathbb{C}\{z\}$, $\mathbb{C}[[z^*]]$, $\mathbb{C}\{z^*\}$ are exactly the elements of order zero.

**The Newton Puiseux Theorem (we already asserted the theorem)**

*Proof.* Any monic polynomial

$$P(z,T) = T^n + a_1(z)T^{n-1} + \cdots + a_n(z)$$

of $n > 1$ with coefficients in $\mathbb{C}((x^*))$ or $\mathbb{C}(\{x^*\})$ is reducible. Making use of the Tschirinhousen transformation of variables $T' = T + a_1(z)/n$, we can assume that $a_1(z) \equiv 0$. Put $r_k := \mathbf{ord}((a_k)(z)) \in \mathbb{Q}$ unless $a_1(z) \equiv 0$, and $r := \mathbf{min}\{r_k/k\}$, $r_k/k - r \geq 0$ and we have equality for at least one $k$. Take a positive integer $q$ so large that all the Puiseux series $a_k(z)$ are of the form $f_k(z^{1/q})$ with $f_k(z) \in \mathbb{C}[[z]]$ (or $\mathbb{C}\{z^*\}$), and let $r = p/q$ with $p \in \mathbb{Z}$. After the transformation of variables $z = w^q$, $T = Uw^p$ we get $P(z,T) = w^{np}Q(w,U)$ where

$$Q(w,U) = U^n + b_2(w)U^{n-2} + \cdots + b_n(w)$$

with $b_k(w) = a_k(w^q)w^{-kp}$. Since $\mathbf{ord}((b_k)(z)) \in \mathbb{Z}$ and

$$\mathbf{ord}((b_k)(z)) = qr_k - pk = qk(r_k/k - r) \geq 0$$

$Q(w,U)$ is a polynomial with coefficients in $\mathbb{C}[[z]]$ (or $\mathbb{C}\{z\}$). Furthermore, $\mathbf{ord}((b_k)(z)) = 0$ for at least one $k$ and thus $b_k(0) \neq 0$ for every such $k$. Therefore the complex polynomial

$$Q(0,U) = U^n + b_2(0)U^{n-2} + \cdots + b_n(0) \not\equiv (U-c)^n$$

for any $c \in \mathbb{C}$, and consequently, $Q(0,U)$ is the product of two relatively prime complex polynomials. Hence and by Hensel's lemma is the product of two polynomials $Q_1(w,U) \cdot Q_2(w,U)$ with coefficients in $\mathbb{C}[[z]]$ (or $\mathbb{C}\{z\}$). Then

$$p(z,T) = z^{nr} Q_1(z^{1/q}, z^{-r}T) \cdot Q_2(z^{1/q}, z^{-r}T)$$

and the theorem follows.

Let $\epsilon_n$ denote an $n$-th primitive root of unity.

**Lemma 5.1.** *If $f(z) \in \mathbb{C}[[z]]$ (or $\mathbb{C}\{z\}$) and $r \in \mathbb{N}$, then*

$$Q(z,T) := (T - f(z))(T - f(\epsilon_r z)) \cdots (T - f(\epsilon_r^{r-1} z)$$

*is a monic polynomial in $T$ with coefficients in $\mathbb{C}[[z^r]]$ (or $\mathbb{C}\{z^r\}$).*

*Proof.* For a proof, consider the elementary symmetric polynomials $s_j(U_1, \ldots, U_r)$ $(j = 1, 2, \ldots, r)$ in variables $U_1, \ldots, U_r$; let $S_j : \mathbb{C}[[z]] \longrightarrow \mathbb{C}[[z]]$ be defined by

$$S_j(f(z)) := s_j\left(f(z), f(\epsilon_r z), \ldots, f\left(\epsilon_r^{r-1} z\right)\right)$$

It is to be shown that $S_j(f(z)) \in \mathbb{C}[[z^r]]$ for all $f(z) \in \mathbb{C}[[z]]$. Since the mappings $S_j$ are continuous in the maximal-adic topology of $\mathbb{C}[[z]]$, it is sufficient to prove the above assertion only for polynomials $f(z) \in \mathbb{C}[z]$. But this follows from the fact that

$$\sigma_i : \mathbb{C}(z) \longrightarrow \mathbb{C}(z), \sigma_i(z) = \epsilon_r^i \cdot z \quad (i = 0, 1, \ldots, r-1)$$

form the Galois group $G$ of the field $\mathbb{C}(z)$ over $\mathbb{C}(z^r)$. Indeed, if $f(z) \in \mathbb{C}[z]$, then $S_j(f(z))$ is, of course, an invariant of $G$ whence

$$S_j(f(z)) \in \mathbb{C}(z^r) \cap \mathbb{C}[z] = \mathbb{C}[z^r]$$

as desired. ∎

**Proposition 5.2.** *The rings $\mathbb{C}[[z^*]]$ and $\mathbb{C}\{z^*\}$ are integral over the rings $\mathbb{C}[[z]]$ and $\mathbb{C}\{z\}$, respectively. If a Puiseux series $\phi(z)$ from $\mathbb{C}[[z^*]]$ (or from $\mathbb{C}\{z^*\}$) is a root of an irreducible monic polynomial $P(z,T)$ of degree $n$ with coefficients in $\mathbb{C}[[z]]$ (or $\mathbb{C}\{z\}$), then $\phi(z)$ is of*

*the form* $g\left(z^{1/n}\right)$ *where* $g(z)$ *belongs to* $\mathbb{C}[[z]]$ *(or* $\mathbb{C}\{z\}$*). Moreover, the elements conjugate to* $\phi(z)$ *are exactly* $g\left(\epsilon_n^i z^{1/n}\right), i = 0, 1, \ldots, n-1$.

The Puiseux series $\phi(z)$ is of the form $f\left(z^{1/r}\right)$ where $f(z)$ belongs to $\mathbb{C}[[z]]$ (or $\mathbb{C}\{z\}$). It follows immediately from the above lemma that

$$Q(z,T) := \prod_{i=0}^{r-1} \left(T - f\left(\epsilon_r^i z^{1/r}\right)\right)$$

is a monic polynomial in $T$ with coefficients in $\mathbb{C}[[z]]$ (or $\mathbb{C}\{z\}$ ). Therefore the polynomial $Q(z,T)$ is divisible by $P(z,T)$ whence every root of $P(z,T)$ is of the form $f\left(\epsilon_r^i z^{1/r}\right)$.

Conversely, each Puiseux series $f\left(\epsilon_r^i z^{1/r}\right)$ is a root of $P(z,T)$. Indeed, $f(z) = f\left(\left(z^r\right)^{1/r}\right)$ is a root of the polynomial $P\left(z^r, T\right)$, and thus $f\left(\epsilon_r^i z\right)$ is a root of $P\left(\left(\epsilon_r^i z\right)^r, T\right) = P\left(z^r, T\right)$. Hence $f\left(\epsilon_r^i z^{1/r}\right)$ is a root of $P(z,T)$, as asserted.

Summing up, the set $X$ of Puiseux series

$$f\left(\epsilon_r^i z^{1/r}\right) \quad (i = 0, 1, \ldots, r-1)$$

consists of precisely $n$ roots of the polynomial $P(z,T)$. Consider now an action of the group $\mathbb{Z}_r$ on the set $X$ defined by the formula

$$\left(j \bmod r, f\left(\epsilon_r^i z^{1/r}\right)\right) \longmapsto f\left(\epsilon_r^{i+j} z^{1/r}\right)\Big).$$

As the set $X$ is the orbit of the element $f\left(z^{1/r}\right)$, the stabilizer of $f\left(z^{1/r}\right)$ is a subgroup of $\mathbb{Z}_r$ of index $n$, and thus it is the subgroup $\mathbb{Z}_s \subset \mathbb{Z}_r$ where $r = n \cdot s$. This yields

$$f\left(\epsilon_s^i z^{1/r}\right) = f\left(z^{1/r}\right) \quad (i = 0, 1, \ldots, s-1).$$

Hence and by the lemma,

$$s \cdot f\left(z^{1/s}\right) = f\left(\left(z^n\right)^{1/r}\right) + f\left(\epsilon_s \left(z^n\right)^{1/r}\right) + \cdots + f\left(\epsilon_s^{s-1} \left(z^n\right)^{1/r}\right) =$$
$$= f\left(z^{1/s}\right) + f\left(\epsilon_s z^{1/s}\right) + \cdots + f\left(\epsilon_s^{s-1} z^{1/s}\right)$$

belongs to $\mathbb{C}[[z]]$ (or $\mathbb{C}\{z\}$). Therefore, $f\left(z^{1/s}\right) = g(z)$ with $\boldsymbol{g}(z)$ in $\mathbb{C}[[z]]$ (or $\mathbb{C}\{z\}$). Consequently,

$$\phi(z) = f\left(z^{1/r}\right) = f\left(\left(z^{1/n}\right)^{1/s}\right) = g\left(z^{1/n}\right),$$

and the proof is complete [1]. ■

## 6. The Newton Polygon

6.1. **Practical Application.** The Newton Polygon is a tool invented by Issac Newton that allows for the estimation and construction of a puiseux series on a certain branch of some algebraic curve. Specifically, the polygon helps to find the valuation of the puiseux series that make up the roots of our algebraic curve. whats great is that this can be done for essentially any algebraic curve, because as the theorem has proved, the ring of puiseux series is algebraically closed, meaning all polynomials with coefficients in the form of puiseux series can be factored into puiseux series.

The actual method for computing the zeros with the newton polygon seem strange at first, but produce really interesting math.

6.2. **Construction.**

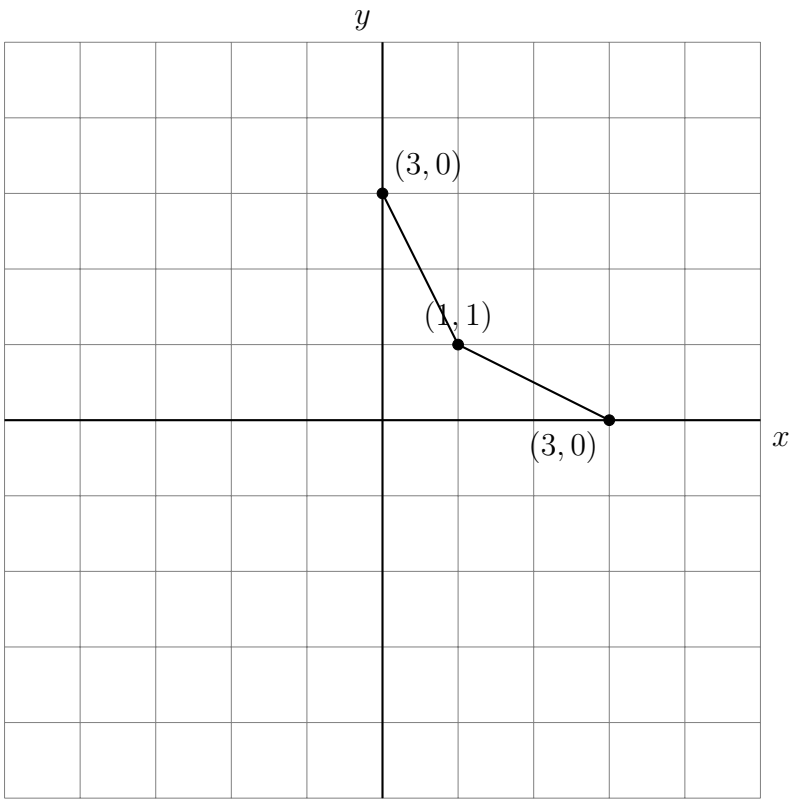
$$P(y) = \sum_{a_i \neq\ 0} a_i\left(x\right) y^i$$

Is some two variable function that we are interested in constructing a puiseux series for. Let $\mathbf{ord}(a_i(\mathbf{x}))$ be equal to the lowest $x$ exponent term in $a_i(x)$. In a normal cartesian plane, construct a series of points:

$$(i, \mathbf{ord}(a_i))\ \forall\ i \in P(y).$$

Then construct the lower convex hull of the points.

**Example 6.1.** *Let $P(y) = y^3 + 3xy + x^3$. In our cartesian plane our Newton polygon looks like:*




Now using the lines we have drawn, we can extract their slopes, and those slopes give the degrees of the first few terms of the puiseux series that approximate the curve near $(0, 0)$. We do this by then setting one of our variables equal to that exponential, and then solving for its coefficients.

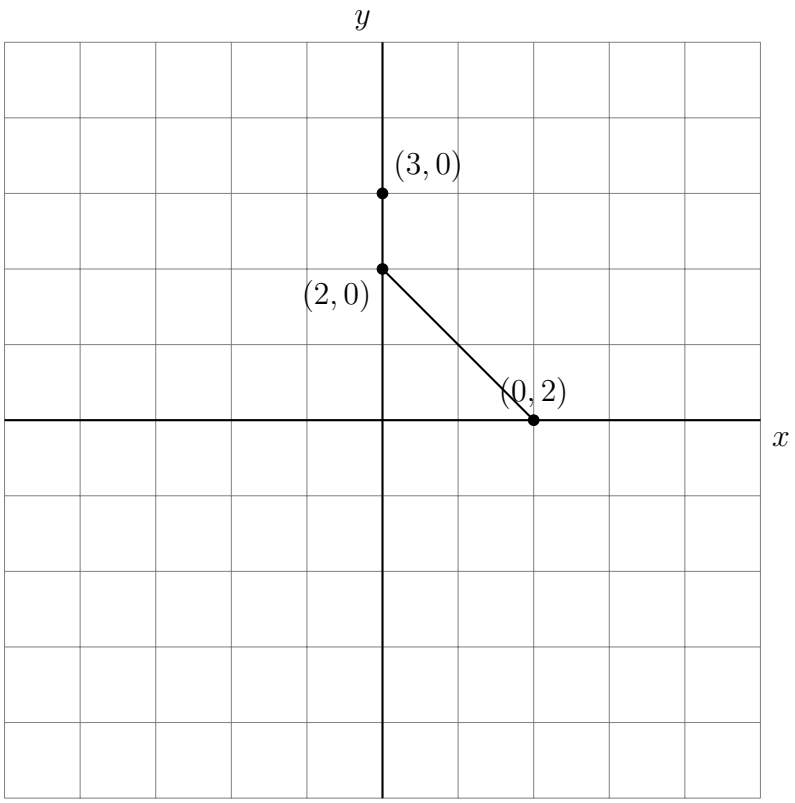
So if the first slope of our Newton polygon is $1/3$ then we set $y = cx^{\frac{1}{3}}$ and solve for $c$ in our original polynomial.

**Example 6.2.** *Using the Newton polygon, we can find the Newton for the polynomial*

$$p(x, y) = x^3 + x^2 - y^2$$

*where* $p(x, y) = 0$

*The lower convex looks like:*




*and the puiseux series (for one branch of our polynomial) is*

$$x + \frac{x^2}{2} + \sum_{n=1}^{100} (-1)^n \, x^{(n+2)} \frac{1}{2^{(n+2)}}$$

$$x + \frac{x^2}{2} - \frac{x^3}{8} + \frac{x^4}{16} + \cdots$$

## 7. Behavior of fields in positive characteristic

7.1. **Preface.** While the algebraic closure of out complex power series ring in characteristic zero is relatively simple, things complicate when we begin to construct new rings and fields with different properties, and in different characteristic.

Using more complex math, we can prove certain aspects about the properties and construction of these algebraic closures in certain fields.

Specifically, we can prove certain properties of the algebraic closure to a distinct class of fields: perfect fields.

**Definition 7.1** (Perfect Fields)**.** We say a field a field is perfect if every irreducible polynomial over k has no multiple roots in any field extension F/k.

A root $a$ is a multiple root of a polynomial $p(x)$ if that same root satisfies:

$$s(a) \neq 0 \mid p(x) = (x-a)^k s(x), k \geq 2.$$

where $s(x)$ is some polynomial with its coefficients in the same field in $p(x)$.

Perfect fields are not all algebraically closed, but all algebraically closed fields are perfect. There are many properties that are implicit to the indention of a perfect field, and thus there are many definitions a field can satisfy to be considered perfect.

It should also be noted that all fields of characteristic zero, like our original field, are perfect.

## 7.2. **The Algebraic Closure of Perfect Fields of Characteristic $p$.**

**Corollary 7.1.** *Let $L$ be a perfect (but not algebraically closed) field of characteristic $p$. The algebraic closure of $L((t))$ or the function field of all power series with coefficients in $L$ consists of all twist-recurrent series*

$$x = \sum_{i=0} x_i t^i$$

*with $x_i$ in a finite extension of $L$.*

**Theorem 7.1.** *The twist-recurrent series form an algebraic closure of $K((t))$.*

*Proof.* We verify the following three assertions: 1. Every twist-recurrent series is algebraic over $K((t))$. 2. The twist-recurrent series are closed under addition and scalar multiplication. 3. If $y$ is twist-recurrent and $x^p - x = y$, then $x$ is twist-recurrent.

From these, it will follow that the twist-recurrent series form a ring algebraic over $K((t))$ (which is automatically then a field) closed under Artin-Schreier extensions; by Lemma 3, this field is algebraically closed.

Before proceeding, we note that for each assertion, it suffices to work with series supported on $S_{a,b,c}$ with $a = 1$. 1. We proceed by induction on $c$ (with vacuous base case $c = 0$ ); by Lemma [7] we need only consider a series $x = \sum x_i t^i$ supported on $T_c$. Choose $d_0, \ldots, d_k$ as in Definition 2. and let

$$y = d_0 x^{1/p^k} + d_1 x^{1/p^{k-1}} + \cdots + d_k x$$

Clearly $y$ is supported on $T_c$; in fact, we claim it is supported on $S_{p^k,0,c-1}$. To be precise, if $j = -\sum b_i p^{-i}$ belongs to $T_c$ but not to $S_{p^{kc},0,c-1}$, then $\sum b_i = c$, and $b_i = 0$ for $i \leq k$. In particular $p^k j$ lies in $T_c$, and so

$$y_j = d_0 x_{p^k j}^{1/p^k} + d_1 x_{p^{k-1} j}^{1/p^{k-1}} + \cdots + d_k x_j = 0$$

because $x$ is twist-recurrent. We conclude that $y$ is twist-recurrent (we have just verified condition 1 , condition 2 follows from Corollary [5, and condition 3 is evident). By the induction hypothesis, $y$ is algebraic over $K((t))$, as then are $y^{p^k}$ and thus $x$. 2. Closure under addition follows immediately from Lemma [7] as for multiplication, it suffices to show that $xy$ is twist-recurrent whenever $x = \sum x_i t^i$ and $y = \sum y_i t^i$ are twist-recurrent on $T_c$. We will prove this by showing that any sequence of the form

$$c_n = (xy)_{-b_0 - b_1 p^{-1} - \cdots - b_{j-1} p^{-(j-1)} - p^{-n}(b_j p^{-j} + \cdots)}$$

becomes, after some initial terms, the sum of a fixed number of pairwise products of similar sequences derived from $x$ and $y$. Those sequences satisfy fixed LRRs, so $\{c_n\}$ will as well by Corollary 5

To verify this claim, recall that $(xy)_k$ is the sum of $x_i y_j$ over all $i, j \in T_c$ with $i + j = k$. Writing the sum $(-i) + (-j)$ in base $p$, we notice that for $n$ sufficiently large, there can be no carries across the "gap" between $p^{-(j-1)}$ and $p^{-j-n}$. (To be precise, the sum of the digits of $-k$ equals the sum of the digits of $(-i)$ and $(-j)$ minus ( $p - 1$ ) times the number of carries.) Thus the number of ways to write $-k$ as $(-i) + (-j)$ is uniformly bounded, and moreover as $k$ runs through a sequence of indices of the shape in (3)), the possible $i$ and $j$ are constrained to a finite number of similar sequences. This proves the claim. 3. Since the

map $x \mapsto x^p - x$ is additive, it suffices to consider the cases when $y$ is supported on $(-\infty, 0)$ and $(0, \infty)$.

First, suppose $y$ is supported on $(-\infty, 0) \cap S_{a,b,c}$ for some $a, b, c$; then

$$x = \sum_i \sum_{n=1}^{\infty} y_i^{1/p^n} t^{i/p^n} = \sum_i t^i \sum_n y_{ip^n}^{1/p^n}$$

is supported on $S_{a,b,b+c}$. We must show that if $-b \leq m \leq 0, b_i \in \{0, \ldots, p-1\}$ and $\sum b_i \leq c$, then for any $j$, the sequence

$$c_n = x_{m - b_1 p^{-1} - \cdots - b_{j-1} p^{-(j-1)} - p^{-n}(b_j p^{-j} + \cdots)}$$

satisfies a fixed LRR. If $m < 0$ or $j > 0$, then $\{c_n\}$ is the sum of a bounded number of sequences satisfying fixed LRRs, namely certain sequences of the $y_i$, so $x$ is twist-recurrent by Corollary 5. If $m = j = 0$, then

$$c_{n+1}^p - c_n = y_{-b_1 p^{-1} - \cdots - b_{j-1} p^{-(j-1)} - p^{-n}(b_j p^{-j} + \cdots)}$$

if $\left\{c_{n+1}^p - c_n\right\}$ is twist-recurrent with coefficients $d_0, \ldots, d_k$, then $\{c_n\}$ is twist-recurrent with coefficients $-d_0, d_0 - d_1, \ldots, d_k - d_{k-1}$.

Next, suppose $y$ is supported on $(0, +\infty) \cap S_{a,b,c}$; then

$$x = -\sum_i \sum_{n=0}^{\infty} y_i^{p^n} t^{ip^n} = -\sum_i t^i \sum_n y_{i/p^n}^{p^n}$$

is also supported on $S_{a,b,c}$. For $i < p^k$, we have $y_{i/p^n} = 0$ for $n > k + c$, since the first $c$ fractional digits of $-i/p^n$ in base $p$ will be $p - 1$. Thus each sequence defined by (4) is the sum of a bounded number of sequences satisfying fixed LRRs (the exact number and the coefficients of the LRRs depending on $m$ ), and so Corollary 5 again implies that $x$ is twist-recurrent.

■

To show conversely that any series which is algebraic over $L((t))$ has coefficients in a finite extension of $L$, let $E$ be a finite extension of $L((t))$, and $M$ the integral closure of $L$

in $E$. Then a slight modification of Lemma 3 implies that $E$ can be expressed as a tower of Artin-Schreier extensions over $M\left(\left(t^{1/n}\right)\right)$ for some $n \in \mathbb{N}$. Now the argument given for assertion 3 in the proof of Theorem 8 shows that if $y$ has coefficients in $M$ and $x^p - x = y$, then $y$ has coefficients in $M$ except possibly for its constant coefficient, which may lie in an Artin-Schreier extension of $M$. We conclude that the coefficients of any element of $E$ lie in a finite extension of $L$.

For $L$ not perfect, the situation is more complicated, since if $y$ has coefficients in $M$ and $x^p - x = y, x$ may have coefficients which generate inseparable extensions of $M$. We restrict ourselves to giving a necessary condition for algebraicity in this case.

[2]

## 8. Conclusion

Through this paper, we have seen how abstract algebra concepts can be used to study and prove certain statements about the structure of number systems. First we saw its applications to rings and fields that we are familiar with, then we saw its practical application to the approximation of two variable polynomials, and then we saw how similar proofs can be applied to other fields and the interesting and complex math that goes into studying those fields.

## References

[1] Krzysztof Jan Nowak (2000) *SOME ELEMENTARY PROOFS OF PUISEUX'S THEOREMS*, Universitatis Lagellonicae Acta Mathematica, Fasciculus XXXVIII.

[2] Kiran S. Kedlaya (2001) *THE ALGEBRAIC CLOSURE OF THE POWER SERIES FIELD IN POSITIVE CHARACTERISTIC*, Proceedings of the American Mathmatical Society.