Puiseux Series and Integral Bases of Algebraic Functions

Christoph Koutschan

Johann Radon Institute for Computational and Applied Mathematics (RICAM)
Austrian Academy of Sciences

May 5, 2017
Linz-Wien Workshop in Klagenfurt

ÖAW Austrian Academy of Sciences

RICAM JOHANN · RADON · INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS

Outline of the Talk

1. Introduction
2. Main Theorem
3. Conclusion

References

- Ford and Zassenhaus, 1978
  $\longrightarrow$ algorithm for algebraic number fields
- Barry Trager: *Integration of algebraic functions*, Ph.D. thesis, 1984.
  $\longrightarrow$ generalization of Ford-Zassenhaus to algebraic function fields
- Mark van Hoeij: *An Algorithm for Computing an Integral Basis in an Algebraic Function Field*, Journal of Symbolic Computation **18**, 353–363, 1994.
  $\longrightarrow$ faster algorithm for algebraic function fields

Notation

We employ the following notation:

- L is an algebraically closed field of characteristic 0
- x is transcendental over L
- y is algebraic over $L(x)$ with minimal polynomial f
- n is the degree of f
- $K \leqslant L$ denotes the field of coefficients of f, i.e., $f \in K[x, y]$
- $\overline{L[x]}$ is the integral closure of $L[x]$ in $L(x, y)$

Vector Space Basis

We know that $L(x, y)$ is a $L(x)$-vector space of dimension n.

Elements $b_0, \ldots, b_{n-1} \in L(x, y)$ are a vector space basis if

$$L(x)\, b_0 + \cdots + L(x)\, b_{n-1} = L(x, y).$$

Vector Space Basis

We know that $L(x, y)$ is a $L(x)$-vector space of dimension n.

Elements $b_0, \ldots, b_{n-1} \in L(x, y)$ are a vector space basis if

$$L(x)\, b_0 + \cdots + L(x)\, b_{n-1} = L(x, y).$$

Standard vector space basis of $L(x, y)$:

$$b_0 = 1, \quad b_1 = y, \quad b_2 = y^2, \ldots, \quad b_{n-1} = y^{n-1}.$$

Vector Space Basis

We know that $L(x,y)$ is a $L(x)$-vector space of dimension n.

Elements $b_0, \ldots, b_{n-1} \in L(x,y)$ are a vector space basis if

$$L(x)\, b_0 + \cdots + L(x)\, b_{n-1} = L(x,y).$$

Standard vector space basis of $L(x,y)$:

$$b_0 = 1, \quad b_1 = y, \quad b_2 = y^2, \ldots, \quad b_{n-1} = y^{n-1}.$$

Example: $f = y^3 - x^2$, $b_0 = 1$, $b_1 = x^{2/3}$, $b_2 = x^{4/3}$

Integral Basis

Definition: An element $a \in L(x, y)$ is called **integral** if its minimal polynomial is monic over $L[x]$.

Integral Basis

Definition: An element $a \in L(x, y)$ is called **integral** if its minimal polynomial is monic over $L[x]$.

Proposition: An element $a \in L(x, y)$ is integral if and only if $v_P(a) \geqslant 0$ in all finite places P (i.e., all its Puiseux series expansions at all finite points involve only nonnegative exponents).

Integral Basis

Definition: An element $a \in L(x, y)$ is called **integral** if its minimal polynomial is monic over $L[x]$.

Proposition: An element $a \in L(x, y)$ is integral if and only if $v_P(a) \geqslant 0$ in all finite places P (i.e., all its Puiseux series expansions at all finite points involve only nonnegative exponents).

Definition: A $L(x)$-vector space basis $b_0, \ldots, b_{n-1}$ of $L(x, y)$ is called an **integral basis** if all the b_i are integral and if

$$L[x]\, b_0 + \cdots + L[x]\, b_{n-1} = \overline{L[x]}$$

where $\overline{L[x]}$ is the $L[x]$-module of all integral elements of $L(x, y)$.

Integral Basis

Definition: An element $a \in L(x, y)$ is called **integral** if its minimal polynomial is monic over $L[x]$.

Proposition: An element $a \in L(x, y)$ is integral if and only if $v_P(a) \geqslant 0$ in all finite places P (i.e., all its Puiseux series expansions at all finite points involve only nonnegative exponents).

Definition: A $L(x)$-vector space basis $b_0, \ldots, b_{n-1}$ of $L(x, y)$ is called an **integral basis** if all the b_i are integral and if

$$L[x]\, b_0 + \cdots + L[x]\, b_{n-1} = \overline{L[x]}$$

where $\overline{L[x]}$ is the $L[x]$-module of all integral elements of $L(x, y)$.
Example: $f = y^3 - x^2$, $b_0 = 1$, $b_1 = x^{2/3}$, $b_2 = x^{1/3}$

Conventions

W.l.o.g. we assume that y is an integral element.

Hence, every element in $L[x, y]$ is integral. We have

$$L[x, y] \subseteq \overline{L[x]} \subseteq L(x, y).$$

Conventions

W.l.o.g. we assume that y is an integral element.

Hence, every element in $L[x, y]$ is integral. We have

$$L[x, y] \subseteq \overline{L[x]} \subseteq L(x, y).$$

View elements of $L(x, y)$ as polynomials of degree less than n.

Hence, it is meaningful to talk about the **degree** of $a \in L(x, y)$.

Conventions

W.l.o.g. we assume that y is an integral element.

Hence, every element in $L[x, y]$ is integral. We have

$$L[x, y] \subseteq \overline{L[x]} \subseteq L(x, y).$$

View elements of $L(x, y)$ as polynomials of degree less than n.

Hence, it is meaningful to talk about the **degree** of $a \in L(x, y)$.

Goal: Find an integral basis $b_0, \ldots, b_{n-1}$ with $\deg(b_i) = i$ and with $b_i \in K(x, y)$ for all i.

Caveat: Note that Puiseux series expansions may require coefficients in a larger field than K.

Strategy of the Algorithm

Use an inductive argument:

- Start with $b_0 = 1$

Strategy of the Algorithm

Use an inductive argument:

- Start with $b_0 = 1$
- For $0 < d < n$ assume we have already found $b_0, \ldots, b_{d-1}$ such that

$$L[x]\, b_0 + \cdots + L[x]\, b_{d-1} = \left\{ a \in \overline{L[x]} \mid \deg(a) < d \right\}$$

Strategy of the Algorithm

Use an inductive argument:

- Start with $b_0 = 1$
- For $0 < d < n$ assume we have already found $b_0, \ldots, b_{d-1}$ such that

$$L[x]\, b_0 + \cdots + L[x]\, b_{d-1} = \left\{a \in \overline{L[x]} \mid \deg(a) < d\right\}$$

- Compute b_d with $\deg(b_d) = d$ such that

$$L[x]\, b_0 + \cdots + L[x]\, b_d = \left\{a \in \overline{L[x]} \mid \deg(a) \leqslant d\right\}$$

Strategy of the Algorithm

Use an inductive argument:

- Start with $b_0 = 1$
- For $0 < d < n$ assume we have already found $b_0, \ldots, b_{d-1}$ such that

$$L[x]\, b_0 + \cdots + L[x]\, b_{d-1} = \left\{ a \in \overline{L[x]} \mid \deg(a) < d \right\}$$

- Compute b_d with $\deg(b_d) = d$ such that

$$L[x]\, b_0 + \cdots + L[x]\, b_d = \left\{ a \in \overline{L[x]} \mid \deg(a) \leqslant d \right\}$$

- Iterate to obtain an integral basis $b_0, \ldots, b_{n-1}$

One Step of the Algorithm

Task: We have to find the next element b_d of the integral basis.

- Start with $b_d = y^d$ (optimization: use $b_d = yb_{d-1}$)
- $V := \{a \in \overline{L[x]} \mid \deg(a) \leqslant d\} \setminus \big(L[x]\, b_0 + \cdots + L[x]\, b_d\big)$

One Step of the Algorithm

Task: We have to find the next element b_d of the integral basis.

- Start with $b_d = y^d$ (optimization: use $b_d = y b_{d-1}$)
- $V := \{a \in \overline{L[x]} \mid \deg(a) \leqslant d\} \setminus \big(L[x]\, b_0 + \cdots + L[x]\, b_d\big)$

While $V \neq 0$ do the following:

1. Choose $a \in V$ such that a can be written as

$$a = \frac{1}{k}\big(a_0 b_0 + \cdots + a_d b_d\big)$$

with $a_0, \ldots, a_d, k \in K[x]$ and with $a_d = 1$.

One Step of the Algorithm

Task: We have to find the next element b_d of the integral basis.

- Start with $b_d = y^d$ (optimization: use $b_d = yb_{d-1}$)
- $V := \{a \in \overline{L[x]} \mid \deg(a) \leqslant d\} \setminus \big(L[x]\, b_0 + \cdots + L[x]\, b_d\big)$

While $V \neq 0$ do the following:

1. Choose $a \in V$ such that a can be written as
$$a = \frac{1}{k}\big(a_0 b_0 + \cdots + a_d b_d\big)$$
with $a_0, \ldots, a_d, k \in K[x]$ and with $a_d = 1$.
2. Since
$$L[x]\, b_0 + \cdots + L[x]\, b_{d-1} + L[x]\, b_d \subset$$
$$L[x]\, b_0 + \cdots + L[x]\, b_{d-1} + L[x]\, a \subset \overline{L[x]}$$
we can replace b_d by a in our basis and get a smaller V.

Problems

The strategy described before rises the following questions:

1. How can we ensure termination of the algorithm?
2. We have to show that in the case $V \neq 0$ the element a can be chosen in the described form.
3. How can we decide whether $V \neq 0$ and how can we compute $a_0, \ldots, a_d, k$?

Problem 1: Termination

Look at the discriminant (Trager's idea):

$$D := \mathrm{disc}(1, y, \ldots, y^{n-1}) = \mathrm{Res}_y\Big(f, \frac{\partial f}{\partial y}\Big) \in K[x]$$

Problem 1: Termination

Look at the discriminant (Trager's idea):

$$D := \operatorname{disc}(1, y, \ldots, y^{n-1}) = \operatorname{Res}_y\Big(f, \frac{\partial f}{\partial y}\Big) \in K[x]$$

Termination: In every step, when b_d is replaced by a, $\operatorname{disc}(b_0, \ldots, b_d, y^{d+1}, \ldots, y^{n-1})$ is divided by the polynomial k^2.

Problem 1: Termination

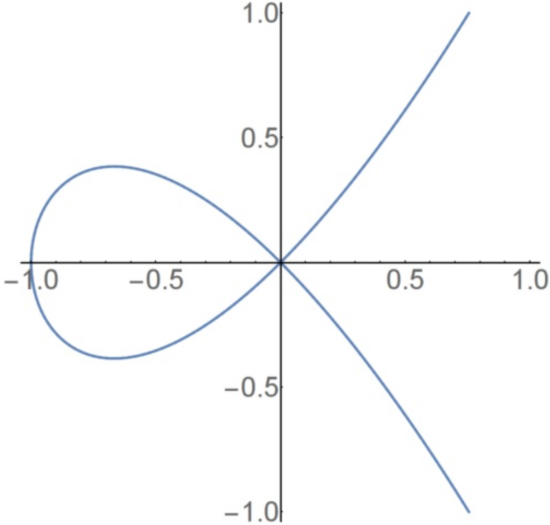
Look at the discriminant (Trager's idea):

$$D := \mathrm{disc}(1, y, \ldots, y^{n-1}) = \mathrm{Res}_y\Big(f, \frac{\partial f}{\partial y}\Big) \in K[x]$$

Termination: In every step, when b_d is replaced by a, $\mathrm{disc}(b_0, \ldots, b_d, y^{d+1}, \ldots, y^{n-1})$ is divided by the polynomial k^2.

Bonus: This reasoning tells us that the candidates for k are exactly the factors of D.

Picture



$$f = y^2 - x^3 - x^2$$

$$D = \mathrm{Res}_y\left(f, \frac{\partial f}{\partial y}\right) = -4x^2(x+1)$$

Problem 2: The Particular Form of a

Assumption: $L[x]\,b_0 + \cdots + L[x]\,b_{d-1}$ contains all integral elements of degree less than d.

Problem 2: The Particular Form of a

Assumption: $L[x]\,b_0 + \cdots + L[x]\,b_{d-1}$ contains all integral elements of degree less than d.

If $V \neq 0$ there exists $a \notin V$; by assumption, $\deg(a) = d$.

Problem 2: The Particular Form of a

Assumption: $L[x]\, b_0 + \cdots + L[x]\, b_{d-1}$ contains all integral elements of degree less than d.

If $V \neq 0$ there exists $a \notin V$; by assumption, $\deg(a) = d$.

Since $b_0, \ldots, b_d$ is a vector space basis, we get

$$a = \frac{1}{k}\Big(a_0 b_0 + \cdots + a_d b_d\Big)$$

for some polynomials $a_0, \ldots, a_d, k \in L[x]$. Note that $k \notin L$.

Problem 2: The Particular Form of a

Assumption: $L[x]\, b_0 + \cdots + L[x]\, b_{d-1}$ contains all integral elements of degree less than d.

If $V \neq 0$ there exists $a \notin V$; by assumption, $\deg(a) = d$.

Since $b_0, \ldots, b_d$ is a vector space basis, we get

$$a = \frac{1}{k}\Big(a_0 b_0 + \cdots + a_d b_d\Big)$$

for some polynomials $a_0, \ldots, a_d, k \in L[x]$. Note that $k \notin L$.

To do:

1. Show that we can choose $a_0, \ldots, a_d$ such that $a_d = 1$.
2. Show that we can choose $a_0, \ldots, a_d, k \in K[x]$ instead of $L[x]$.

$a_d = 1$

We may multiply a by some element in $L[x]$ such that

- the result is still in V,
- and the denominator k is irreducible.

$a_d = 1$

We may multiply a by some element in $L[x]$ such that

- the result is still in V,
- and the denominator k is irreducible.

Hence, we may assume that $k = x - \alpha$ for some $\alpha \in L$.

$a_d = 1$

We may multiply a by some element in $L[x]$ such that

- the result is still in V,
- and the denominator k is irreducible.

Hence, we may assume that $k = x - \alpha$ for some $\alpha \in L$.

But then, we can write $a_i = q_i \cdot (x - \alpha) + a_i'$ with $a_i' \in L$.

$a_d = 1$

We may multiply a by some element in $L[x]$ such that

- the result is still in V,
- and the denominator k is irreducible.

Hence, we may assume that $k = x - \alpha$ for some $\alpha \in L$.

But then, we can write $a_i = q_i \cdot (x - \alpha) + a'_i$ with $a'_i \in L$.

Still, $a'_d \neq 0$, so we can divide by a'_d, obtaining

$$\frac{a_0 b_0 + \cdots + a_d b_d}{x - \alpha} \quad \text{with } a_i \in L \text{ and } a_d = 1.$$

Next step: Argue that the a_i are actually in $K(\alpha)$.

$a_i \in K(\alpha)$

Lemma: Under the previous assumptions the $a_i \in L$ are unique.
Proof: Assume to the contrary, that there were two different sequences $a_0, \ldots, a_d$. Then the difference would be an element in V of degree less than d. Contradiction.

$a_i \in K(\alpha)$

Lemma: Under the previous assumptions the $a_i \in L$ are unique.
Proof: Assume to the contrary, that there were two different sequences $a_0, \ldots, a_d$. Then the difference would be an element in V of degree less than d. Contradiction.

Claim: For all i we have $a_i \in K(\alpha)$

$a_i \in K(\alpha)$

Lemma: Under the previous assumptions the $a_i \in L$ are unique.
Proof: Assume to the contrary, that there were two different sequences $a_0, \ldots, a_d$. Then the difference would be an element in V of degree less than d. Contradiction.

Claim: For all i we have $a_i \in K(\alpha)$

- If a_i was transcendental over $K(\alpha, a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d)$, then it could be replaced by another element from K. Contradiction to the lemma.

$a_i \in K(\alpha)$

Lemma: Under the previous assumptions the $a_i \in L$ are unique.
Proof: Assume to the contrary, that there were two different sequences $a_0, \ldots, a_d$. Then the difference would be an element in V of degree less than d. Contradiction.

Claim: For all i we have $a_i \in K(\alpha)$

- If a_i was transcendental over $K(\alpha, a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d)$, then it could be replaced by another element from K. Contradiction to the lemma.
- Hence the a_i are algebraic over $K(\alpha)$.

$a_i \in K(\alpha)$

Lemma: Under the previous assumptions the $a_i \in L$ are unique.
Proof: Assume to the contrary, that there were two different sequences $a_0, \ldots, a_d$. Then the difference would be an element in V of degree less than d. Contradiction.

Claim: For all i we have $a_i \in K(\alpha)$

- If a_i was transcendental over $K(\alpha, a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d)$, then it could be replaced by another element from K. Contradiction to the lemma.
- Hence the a_i are algebraic over $K(\alpha)$.
- Using the conjugates of a_i, we get a similar contradiction.

$a_i \in K(\alpha)$

Lemma: Under the previous assumptions the $a_i \in L$ are unique.
Proof: Assume to the contrary, that there were two different sequences $a_0, \ldots, a_d$. Then the difference would be an element in V of degree less than d. Contradiction.

Claim: For all i we have $a_i \in K(\alpha)$

- If a_i was transcendental over $K(\alpha, a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d)$, then it could be replaced by another element from K. Contradiction to the lemma.
- Hence the a_i are algebraic over $K(\alpha)$.
- Using the conjugates of a_i, we get a similar contradiction.
- Hence we conclude that $a_i \in K(\alpha)$ for all i.

Final Form of the a_i

Since $a_i \in K(\alpha)$, we can write each a_i as a polynomial in α of degree less than n.

Final Form of the a_i

Since $a_i \in K(\alpha)$, we can write each a_i as a polynomial in α of degree less than n.

Since we divide by $x - \alpha$, we can replace all occurrences of α in the a_i by x. Then $a_i \in K[x]$ for all i.

Final Form of the a_i

Since $a_i \in K(\alpha)$, we can write each a_i as a polynomial in α of degree less than n.

Since we divide by $x - \alpha$, we can replace all occurrences of α in the a_i by x. Then $a_i \in K[x]$ for all i.

The integrality of a translates to the condition $v_P(a_0 b_0 + \cdots + a_d b_d) \geqslant v_P(x - \alpha)$ in all finite places P.

Final Form of the a_i

Since $a_i \in K(\alpha)$, we can write each a_i as a polynomial in α of degree less than n.

Since we divide by $x - \alpha$, we can replace all occurrences of α in the a_i by x. Then $a_i \in K[x]$ for all i.

The integrality of a translates to the condition $v_P(a_0 b_0 + \cdots + a_d b_d) \geqslant v_P(x - \alpha)$ in all finite places P.

We have also $v_P(a_0 b_0 + \cdots + a_d b_d) \geqslant v_P(x - \alpha_i)$, where the α_i are the conjugates of α, because $a_0 b_0 + \cdots + a_d b_d \in K(x, y)$

Final Form of the a_i

Since $a_i \in K(\alpha)$, we can write each a_i as a polynomial in α of degree less than n.

Since we divide by $x - \alpha$, we can replace all occurrences of α in the a_i by x. Then $a_i \in K[x]$ for all i.

The integrality of a translates to the condition $v_P(a_0 b_0 + \cdots + a_d b_d) \geqslant v_P(x - \alpha)$ in all finite places P.

We have also $v_P(a_0 b_0 + \cdots + a_d b_d) \geqslant v_P(x - \alpha_i)$, where the α_i are the conjugates of α, because $a_0 b_0 + \cdots + a_d b_d \in K(x, y)$

Conclusion: We can find $a \in V$ of the form

$$a = \frac{1}{k}\big(a_0 b_0 + \cdots + a_d b_d\big) \quad \text{with } a_0, \ldots, a_d, k \in K[x],$$

where $k \in K[x]$ is the minimal polynomial of α.

Problem 3: Computation of the a_i

Let $k \in K[x]$ be an irreducible polynomial such that $k^2 \mid D$, and let α be a root of k.

Problem 3: Computation of the a_i

Let $k \in K[x]$ be an irreducible polynomial such that $k^2 \mid D$, and let α be a root of k.

Compute all n Puiseux series expansions of y at $x = \alpha$.

Problem 3: Computation of the a_i

Let $k \in K[x]$ be an irreducible polynomial such that $k^2 \mid D$, and let α be a root of k.

Compute all n Puiseux series expansions of y at $x = \alpha$.

Since $b_i \in K[x, y]$, this yields, for each b_i, a set of Puiseux series expansions. Hence we can write down the Puiseux expansions of

$$a = \frac{a_0 b_0 + \cdots + a_d b_d}{x - \alpha}$$

where now $a_0, \ldots, a_d$ are undetermined coefficients.

Problem 3: Computation of the a_i

Let $k \in K[x]$ be an irreducible polynomial such that $k^2 \mid D$, and let α be a root of k.

Compute all n Puiseux series expansions of y at $x = \alpha$.

Since $b_i \in K[x, y]$, this yields, for each b_i, a set of Puiseux series expansions. Hence we can write down the Puiseux expansions of

$$a = \frac{a_0 b_0 + \cdots + a_d b_d}{x - \alpha}$$

where now $a_0, \ldots, a_d$ are undetermined coefficients.

The ansatz a is integral if and only if the coefficients of all negative powers in all Puiseux expansions vanish. This yields a linear system of equations for the a_i over $K(\alpha)$.

Finite Algorithm

The Puiseux series are infinite objects! How to handle them?

Finite Algorithm

The Puiseux series are infinite objects! How to handle them?

Mark van Hoeij derives bounds where the series expansions can be truncated and the algorithm still gives the correct result (quite technical, skipped here).

Finite Algorithm

The Puiseux series are infinite objects! How to handle them?

Mark van Hoeij derives bounds where the series expansions can be truncated and the algorithm still gives the correct result (quite technical, skipped here).

Instead, one could also use lazy series evaluation.