FUCHSIAN DIFFERENTIAL EQUATIONS: NOTES FALL 2022

Herwig HAUSER, University of Vienna

NOTES PART VII&VIII: ALGEBRAIC SERIES

We will show in this double section that any algebraic power series is *D-finite*, i.e., satisfies a linear differential equation with polynomial coefficients. Further, that any algebraic power series with rational coefficients is *almost integral* (or: *globally bounded*), i.e., has integer coefficients if one multiplies the variable x with a suitable positive integer.

Proposition DIFF. (Abel 1827, Cockle 1860, Harley 1862) *Let $y(x) \in \mathbb{C}[[x]]$ be an algebraic power series. There exists a differential equation $Ly = 0$ with polynomial coeffficients which annihilates $y(x)$ and all its conjugates, that is, $y(x)$ is differentially finite. An equation of minimal order can be constructed from the minimal polynomial P of $y(x)$ or, alternatively, from the set of conjugates of $y(x)$. Its order is the dimension of the $\mathbb{C}$-vectorspace spanned by the conjugates of $y(x)$.* [Stan1, Thm. 2.1, p. 178, Stan3, vol II, Thm. 6.4.6, p. 190, Comt, p. 267, CSTU]

Remarks. (a) The statement holds more generally for algebraic Puiseux series $y(x) = \sum_{k=0}^{\infty} a_k x^{k/e}$, $e \geq 1$, with the same proof, and also over arbitrary fields of characteristic 0. Matzat claims that the minimal differential equation of an algebraic power series in $\mathbb{Q}[[x]]$ has 0 as a non-singular point [Matz, p. 684-685]. Note here that this is not the case for algebraic Puiseux series, as $y(x) = \sqrt{x}$ has differential equation $xy' - \frac{1}{2}y = 0$ with regular singularity at 0.

(b) Already Frobenius shows that if the conjugates of an algebraic series span a $\mathbb{C}$-vectorspace of dimension m then they satisfy a differential equation of order m [Frob2, p. 242].

(c) The construction of L given in the two proofs is not as explicit as one would wish. No direct formula for L in terms of the minimal polynomial P of $y(x)$ seems to be known, not a characterization of the differential equations which can arise in this way.

First proof. If $P(x, y)$ is the minimal polynomial of $y(x)$, it is irreducible in $K(x)[y]$, hence P and $\partial_y P$ have no common factor in $K(x)[y]$. Choose $A, B \in K(x)[y]$ such that $AP + B\partial_y P = 1$. It follows that $B(x, y(x)) \cdot \partial_y P(x, y(x)) = 1$ and hence $\frac{1}{\partial_y P(x,y(x))} \in K(x)[y(x)]$. Differentiating $P(x, y(x)) = 0$ with respect to x yields

$$y'(x) = -\frac{\partial_x P(x, y(x))}{\partial_y P(x, y(x))} \in K(x)[y(x)].$$

By the same argument with $y(x)$ replaced by $y'(x)$ (which is again algebraic over $K(x)$) we get that $y''(x) \in K(x)[y'(x)] \subset K(x)[y(x)]$. Iteration yields $y^{(k)}(x) \in K(x)[y(x)]$. But $K(x)[y(x)]$ is generated over $K(x)$ by $1, y(x), ..., y(x)^m$ with $m = \deg_y P - 1$, and is hence a $K(x)$-vectorspace of dimension less than or equal to the degree of algebraicity of $y(x)$. This implies that $y(x)$ and its the successive

herwig.hauser@univie.ac.at, Faculty of Mathematics, University of Vienna, Austria. Supported by the Austrian Science Fund FWF through project P-34765.

derivatives $y'(x), y''(x), ..., y^{(m)}(x)$ are linearly dependent over $K(x)$, so there exists a differential operator $L \in K[x][\partial]$ of order $\leq m$ with $Ly(x) = 0$. ○

*Second proof.** Let $S_P(x)$ be a splitting field of P over $\mathbb{C}(x)$. We may choose $S_P(x)$ inside $\mathrm{Puis}((x))$. The differentiation in $\mathrm{Puis}((x))$ with respect to x restricts to a derivation $\widetilde{\partial}$ on $S_P(x)$ since the derivative $y'(x)$ of a root $y(x)$ of P in $S_P(x)$ is a rational function of x and $y(x)$ and thus belongs again to $S_P(x)$: to see this, it suffices to derive $P(x, y(x)) = 0$ with respect to x, $\partial_x P(x, y(x)) + \partial_y P(x, y(x)) y'(x)$ and to express the resulting inner derivative $y'(x)$ in terms of x and $y(x)$.

Alternatively, by the theory of differential fields, one may also use that the derivative on $\mathbb{C}(x)$ extends uniquely to splitting fields of polynomials P in $\mathbb{C}(x)[y]$, see [vdPS, ex. 1.5.3(c), p. 5]: We will show this only for extensions $\mathbb{C}(x)[y]/\langle P(x,y)\rangle$ where P is irreducible. The argument works for any finite extension of a differential field. As $\partial_y P$ is relatively prime to P in $\mathbb{C}(x)[y]$, we may choose $A, B \in \mathbb{C}(x)[y]$ such that $AP + B\partial_y P = 1$. Define via $\partial y = -B(x,y)\partial_x P(x,y)$ a derivation on $\mathbb{C}(x)[y]$ extending ∂_x on $\mathbb{C}(x)$. It sends by construction P to the ideal $\langle P\rangle$ and thus induces a derivation on $\mathbb{C}(x)[y]/\langle P(x,y)\rangle$ as required. This proves the existence. Uniqueness goes as follows: Let $\overline{y}$ denote the residue class of y in $\mathbb{C}(x)[y]/\langle P(x,y)\rangle$. It is algebraic over $\mathbb{C}(x)$ with minimal polynomial P. Let δ be another derivation on $\mathbb{C}(x)[y]/\langle P(x,y)\rangle$ fixing $\mathbb{C}(x)$. Then $\varepsilon = \partial - \delta$ is zero on $\mathbb{C}(x)$. Write $P = \sum_{i=0}^d P_i(x) y^i$. We get

$$\varepsilon(P) = \sum_{i=0}^d \varepsilon(P_i(x)) y^i + \sum_{i=0}^d P_i(x)\varepsilon(y^i) = \varepsilon(y) \sum_{i=0}^d i P_i(x) y^{i-1}.$$

From $P(x, \overline{y}) = 0$ and the minimality of P with respect to $\overline{y}$ now follows that $\varepsilon(\overline{y}) = 0$. This proves uniqueness. Iterating this process for the successive extensions from $\mathbb{C}(x)$ to $S_P(x)$, we see that there exists a unique extension of the derivation ∂_x on $\mathbb{C}(x)$ to $S_P(x)$.

We continue with the construction of the minimal differential operator annihilating an algebraic power series. Choose a $\mathbb{C}$-basis $y_1, ..., y_n$ of the vectorspace $V_P(x) \subseteq S_P(x)$ generated by the roots of P (to easen the notation, we suppress the dependence of y_i on x). We have $V_P(x) = \bigoplus_{i=1}^n \mathbb{C} y_i \subseteq S_P(x) = \mathbb{C}(x, y_1, ..., y_n)$. In general, n will be smaller than the degree $\deg P$ of P. The Wronskian matrix of n series $y_1, ..., y_n$ is

$$W(y_1, ..., y_n) = \begin{pmatrix} y_1 & \cdots & y_n \\ y_1' & \cdots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-1)} & \cdots & y_n^{(n-1)} \end{pmatrix}.$$

Denote by $w(y_1, ..., y_n) = \det W(y_1, ..., y_n)$ its determinant. Let y be a variable, denote by $y', ..., y^{(n)}$ its formal derivatives and consider the Wronskian

$$W(y, y_1, ..., y_n) = \begin{pmatrix} y & y_1 & \cdots & y_n \\ y' & y_1' & \cdots & y_n' \\ \vdots & \vdots & & \vdots \\ y^{(n-1)} & y_1^{(n-1)} & \cdots & y_n^{(n-1)} \\ y^{(n)} & y_1^{(n)} & \cdots & y_n^{(n)} \end{pmatrix}$$

with determinant $w(y, y_1, ..., y_n)$. Now, for $y_1, ..., y_n$ a basis of V_P, define the n-th order differential operator $L \in \mathbb{C}(x, y_1, ..., y_n)[\partial] = S_P(x)[\partial]$ by

* We are indebted to Michael Singer for explaining to us this construction of L [e-mail October 30, 2020], see also [CSTU, p. 356].

$$Ly = \frac{w(y, y_1, ..., y_n)}{w(y_1, ..., y_n)}.$$

Clearly, L annihilates $y_1, ..., y_n$, by the properties of the Wronskian, and $L \in \mathbb{C}\langle x\rangle[\partial]$. We will show that $L \in \mathbb{C}(x)[\partial]$, i.e., that the coefficients of L are rational functions, and then, after multiplication of L with their common denominator, even polynomials.

The action of the Galois group G of $S_P(x)$ over $\mathbb{C}(x)$ extends trivially to $S_P(x)(y, y', ..., y^{(n)})$, leaving the variable y and its derivatives $y^{(i)}$ fixed. Note that the action of G commutes with differentiation (with respect to x) in $S_P(x)$,

$$(\sigma y_i)' = \sigma y_i'.$$

Indeed, the derivation δ on $S_P(x)$ given by $z \to \sigma^{-1}(\sigma z)'$ equals, when restricted to $\mathbb{C}(x)$, the differentiation ∂ of $\mathbb{C}(x)$. By the uniqueness of the extension $\widetilde{\partial}$ of ∂ to $S_P(x)$ we get $\delta = \widetilde{\partial}$. [•• ... one may also extend the action of G to $\mathrm{Puis}((x))$ and then restrict to $S_P(x)$].

Let $\sigma \in G$ be a group element, and denote by $[\sigma]$ the matrix of $\sigma \in \mathrm{GL}_n(\mathbb{C}(x))$ with respect to the basis $y_1, ..., y_n$ of $V_P(x)$. We claim that $\sigma L = L$. We have

$$\sigma w(y, y_1, ..., y_n) = w(\sigma y, \sigma y_1, ..., \sigma y_n) = w(y, \sigma y_1, ..., \sigma y_n) = \det[\sigma] w(y, y_1, ..., y_n)$$

and

$$\sigma w(y_1, ..., y_n) = w(\sigma y_1, ..., \sigma y_n) = \det[\sigma] w(y_1, ..., y_n),$$

which gives the claim. As this holds for all $\sigma \in G$, it follows that $L \in \mathbb{C}(x)[\partial]$. So we have found a differential equation $Ly = 0$ which is satisfied by all roots of P.

Let us show that it is minimal. Let L' be any other linear differential operator annihilating one of the roots of P. The elements of G act transitively on the roots of P. As they commute with the derivation on $S_P(x)$ we get that L' annihilates all roots of P, hence $V_P(x)$. We divide L' by L inside $\mathbb{C}(x)[\partial]$, $L' = ML + N$ with N an operator of order $< n$, the order of L. But also N annihilates $V_P(x)$, which has $\mathbb{C}$-dimension n. Hence $N = 0$ and L' is a (left)-multiple of L. This concludes the second proof. $\circlearrowleft$

Remark. The first proof does not give an explicit formula for the differential equation satisfied by $y(x)$. It shows, however, that the order of L is less than or equal to the degree of algebraicity of $y(x)$. The order of L may be much smaller, as show the examples where the dimension of the vectorspace generated by the conjugates of $y(x)$ is smaller that the degree of algebraicity. In [CSTU], various algorithms are discussed of how to determine the minimal differential operator L annihilating all roots of a polynomial $P \in K(x)[y]$. Note that L need not be irreducible, see [CSTU, Thm. 5.1, p. 376, Prop. 5.4, p. 378, Ex. 5.6, p. 385, Ex. 5.15, p. 391].

Examples. (R5) First order equations $y' - ry = 0$ can be rewritten $\log(y)' = r$ with solution $y(x) = \exp(R(x))$, where R is a primitive of r. If $y(x)$ is a rational function, $r(x) = \frac{y'(x)}{y(x)}$ will be rational as well, with only simple poles. We will investigate later on for which r the solution $y(x)$ is a rational function or an algebraic series. S. Yurkevich showed recently that if $r \in \mathbb{Q}(x)$ and $y' - ry = 0$ has a power series solution $y(x) \in \mathbb{Z}[[x]]$ with integer coefficients, then $y(x)$ is already algebraic. In fact, $y(x)$ will then be the m-th root of a rational function, for some $m \geq 1$.

(R6) Let $P \in \mathbb{C}(x)[y]$ be an irreducible polynomial of degree $d \geq 2$. Assume that the coefficient $a := a_{d-1}(x)$ of y^{d-1} in the expansion of P is non-zero. Set $L = \partial - \frac{a'}{a}$. This is a first order operator with rational coefficients. Let L' be any operator annihilating the roots $y_1, ..., y_d$ of P in $\mathrm{Puis}(x)$. Write $L' = ML + N$ with N an operator of order 0. As L and L' annihilate $z = y_1 + \ldots + y_d$ [•• ... ?] we get $N = 0$, hence $L' = ML$ is a multiple of L.

(R7) Let $y(x) = \sqrt{1+x} + \sqrt{2+x}$. This is an algebraic series with minimal polynomial $P = (y^2 - 2x - 3)^2 - 2(x^2 + 3x + 2)$ of degree 4. Its roots are $\pm\sqrt{1+x} \pm \sqrt{2+x}$, spanning the two-dimensional $\mathbb{C}$-vectorspace $V_P(x) = \mathbb{C}\sqrt{1+x} + \mathbb{C}\sqrt{2+x}$. By what we said earlier, we thus know that the minimal operator annihilating the roots of P has order 2. The coefficient $a_3(x)$ of P is 0, so we are not in the situation of example R6. But both $L_1 = \partial - \frac{1}{1+x}$ and $L_2 = \partial - \frac{1}{2+x}$ divide L from the right, $L = M_1 L_1 = M_2 L_2$. So L is reducible. Actually, it is the least common left multiple of L_1 and L_2.

(R8) The divergent series $y(x) = \sum_{k=0}^{\infty} k! x^{k+1} = x + x^2 + 2x^3 + 6x^4 + 24x^5 + \ldots$ (example 6' in the Introduction) is differentially finite with minimal equation $Ly = x^3 y'' + (x^2 - x)y' + y = 0$. The series is integral and transcendent (since divergent), and 0 is an irregular singularity of L. The initial form at 0 is given by the first order operator $L_0 = -x\partial + 1$, while L has order 2. Note that the function $y_1(x) = \exp(-\frac{1}{x})$ is also a solution of $Ly = 0$. Further, $y_2(x) = \exp(-\frac{1}{x}) \cdot Ei(-\frac{1}{x})$ is a second, linearly independent solution, with $Ei(x) = \displaystyle\int_{-\infty}^{x} \frac{e^t}{t} dt = -\gamma - \log(x) - \sum_k (-1)^k \frac{x^k}{k \cdot k!}$ the exponential integral, and γ the Euler-Mascheroni constant. To prove that $y_2(x)$ is a solution, use $Ei'(x) = -\frac{1}{x}\exp(-x)$.

The expansion at infinity is (see example (I11) in the introduction)

$$\widetilde{L} = \partial^2 + [2x + x^4 - x^3]\partial + x^7.$$

Funny enough, $y_1(\frac{1}{x}) = \exp(-x)$ is not a solution of the equation $\widetilde{L}y = 0$, nor $y(\frac{1}{x}) = \sum_{k=0}^{\infty} \frac{k!}{x^{k+1}}$.

(R9) In [Stan1, remark (g), p. 186] Stanley asks for an algorithm which should allow one to decide whether a differentially finite power series $y(x)$ is algebraic. In general, by studying the asymptotics of the series, transcendence is easier to prove. The series $y(x) = \sum_{k=0}^{\infty} \binom{2k}{k}^{2m}$ is transcendental for all integers $m \geq 1$; responding to a question of Stanley in [loc.cit.] it is proven in [ABD, p. 5] that also $z(x) = \sum_{k=0}^{\infty} \binom{2k}{k}^{2m+1}$ is transcendental.

The differential equations for $y(x)$ and $m = 1, 2, 3, 4$ are given by the irreducible operators

$m = 1$: $L = (1 - 4x)\partial - 2$,

$m = 2$: $L = (x - 16x^2)\partial^2 + (1 - 32x)\partial - 4$,

$m = 3$: $L = (x^2 - 64x^3)\partial^3 + (3x - 288x^2)\partial^2 + (1 - 208x)\partial - 8$

$m = 4$: $L = (x^3 - 256x^4)\partial^4 + (6x^2 - 2048x^3)\partial^3 + (7x - 3712x^2)\partial^2 + (1 - 1280x)\partial - 16$.

For $m = 3$, the operator L is the symmetric square of $L_1 = (64x^2 - x)\partial^2 + (96x - 1)\partial + 4$, and the solutions of $Ly = 0$ are hypergeometric series of the form

$y_1(x) = (F(1/4, 1/4; 1/2; 1 - 64x)^2$,

$y_2(x) = F(3/4, 3/4; 3/2; 1 - 64x)^2 \cdot (64x - 1)$,

$y_3(x) = F(1/4, 1/4; 1/2; 1 - 64x) \cdot F(3/4, 3/4; 3/2; 1 - 64x) \cdot \sqrt{64x - 1}$.

(R10) Take the polynomial $P(x, y) = x^2 y - x^4 - y^4$ defining an algebraic curve $X \subset \mathbb{C}^2$. The origin is a singular point of X, with tangent cone defined by $x^2 y = 0$. It turns out that X has two local analytic branches at 0, one smooth and tangent to the x-axis, the other singular with vertical tangent and cusp singularity isomorphic to $x^2 - y^3 = 0$, see Fig. CTBA.

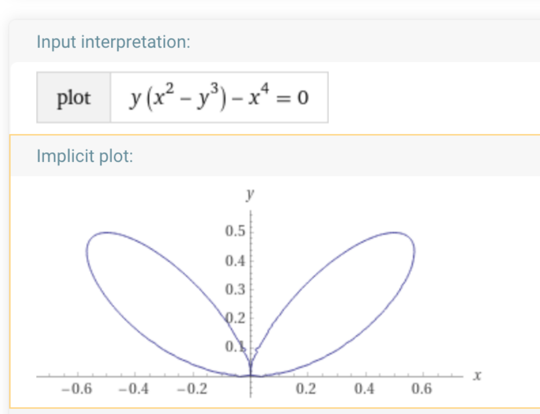

Figure CTBA: The real plane algebraic curve with equation $x^2 y = x^4 + y^4$.

The four solutions $y(x)$ of $P(x,y) = 0$ define local parametrizations of the branches. Computations with Maple yield

$$y_1(x) = x^2 + x^6 + 4x^{10} + 22x^{14} + 140x^{18} + O(x^{22}),$$

$$y_{234}(x) = \xi x^{\frac{2}{3}} - \tfrac{1}{3}x^2 - \tfrac{2}{9}\xi^2 x^{\frac{10}{3}} - \tfrac{20}{81}\xi x^{\frac{14}{3}} - \tfrac{1}{3}x^6 + O(x^{\frac{22}{3}}),$$

where ξ is a third root of unity. The minimal differential equation is

$$(27x^3 - 256x^7)y''' - (81x^2 + 768x^6)y'' + 141xy' - 120y = 0.$$

It can be proven that the equation is a symmetric square.

(R11) Take the polynomial $P(x,y) = xy - x^2 - y^4$ defining an algebraic curve $Y \subset \mathbb{C}^2$. The origin is a singular point of X, with tangent cone defined by $x(y - x) = 0$. It turns out that X has two local analytic branches at 0, both smooth and tangent to the y-axis, respectively, the first diagonal, see Fig. CTBB.

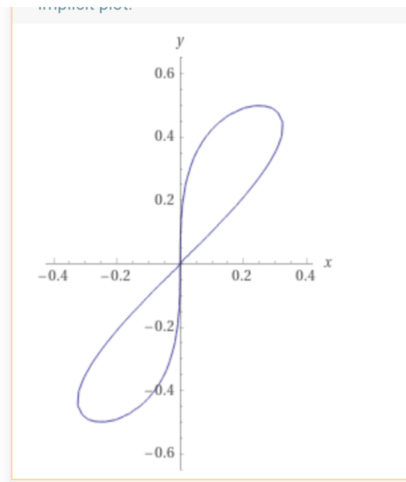

Figure CTBB: The real plane algebraic curve with equation $xy = x^2 + y^4$.

The roots are the (algebraic) series

$$y_1(x) = x + x^3 + 4x^5 + 22x^7 + 140x^9 + 969x^{11} + 7084x^{13} + 53820x^{15} + 420732x^{17} + O(x^{19})$$

and

$$y_2(x) = x^{\frac{1}{3}} - \tfrac{1}{3}x - \tfrac{2}{9}x^{\frac{5}{3}} - \tfrac{20}{81}x^{\frac{7}{3}} - \tfrac{1}{3}x^3 - \tfrac{364}{729}x^{\frac{11}{3}} - \tfrac{5236}{6561}x^{\frac{13}{3}} - \tfrac{4}{3}x^5 - \tfrac{135850}{59049}x^{\frac{17}{3}} + O(x^{\frac{19}{3}}).$$

The minimal differential equation is

$$(27x^3 - 256x^5)y''' - 768x^4y'' + (15x - 192x^3)y' - 15y = 0.$$

Its unique power series solution is

$$y(x) = x \cdot F(\tfrac{-1}{24}, \tfrac{5}{24}; \tfrac{2}{3}; \tfrac{256}{27}x^2) \cdot F(\tfrac{7}{24}, \tfrac{13}{24}; \tfrac{4}{3}; \tfrac{256}{27}x^2),$$

the other two solutions being Puiseux series. The equation is a symmetric square, for instance of

$$(108x^2 - 1024x^4)y'' - 1024x^3y' + (15 + 64x^2)y = 0.$$

(R12) In the example of [Stan1, ex. 2.5, p. 179] it is mentioned that the secans function $y(x) = \sec(x) = \frac{1}{\cos(x)}$ is not differentially finite, whereas its inverse inverse $z(x) = \cos(x)$ is differentially finite with equation $z'' + z = 0$.

An algebraic power series $h(x)$ with $h(0) = 0$ is called *étale algebraic* if its minimal polynomial $P(x, y)$ satisfies the assumption $\partial_y P(0, 0) \neq 0$ of the implicit funtion theorem. It is then the *unique* power series solution of $P(x, y) = 0$ at 0. It can be constructed iteratively up to any degree by Newton's algorithm. The respective definition also applies for algebraic series with non-zero constant term, assuming that $\partial_y P(0, h(0)) \neq 0$. The next lemma says that any algebraic series becomes étale algebraic after clipping off its expansion up to sufficiently high degree. It also holds for series in several variables.

Simple Root Lemma. (one variable case) *For any algebraic series $h(x) = \sum_{k=0}^{\infty} c_k x^k$ in one variable over a field of characteristic 0, there is an integer $e \geq 1$ such that the series $a(x) = \sum_{k=e+1}^{\infty} c_k x^{k-e}$ is a simple root of its minimal polynomial. Said differently, every univariate algebraic series decomposes into a sum*

$$h(x) = k(x) + x^e \cdot a(x)$$

of a polynomial k and a monomial multiple $x^e \cdot a$ of an étale algebraic series a.

Remarks. (a) For the proof it is convenient to choose the decomposition such that $a(0) = 0$.

(b) For e one can choose the order of $\partial_y P(x, h(x))$. How does it relate to the degree of the minimal polynomial without knowing h? Is there an effective way to determine e?

Proof. Let $P(x, y)$ be the minimal polynomial of h. It has minimal degree, hence its partial derivative $\partial_y P$ has non-zero evaluation at h, say, $\partial_y P(x, h(x)) \neq 0$ [... in positive characteristic $p > 0$, it could happen that $\partial_y P$ is identically zero, but then P would have been a polynomial in y^p as e.g. $y^p - (1 + x)$.]. Let $e \geq 0$ be the order of $\partial_y P(x, h(x))$. Write $h(x) = k(x) + a(x) \cdot x^e$ with a polynomial $k(x)$ of degree $\leq e$ (the truncation of h at degree e) and a series $a(x)$ vanishing at 0, $a(0) = 0$. Taylor expansion gives

$$0 = P(x, h) = P(x, k + a \cdot x^e) = P(x, k) + \partial_y P(x, k) \cdot a \cdot x^e + S(x, a \cdot x^e),$$

with $S(x, y)$ a polynomial of order at least two in y. Now observe that

$$\partial_y P(x, k) = \partial_y P(x, h - a \cdot x^e) = \partial_y P(x, h) - \partial_y^2 P(x, h) \cdot a \cdot x^e + T(x, a \cdot x^e),$$

with $T(x, y)$ a polynomial of order at least two in y. As $a(0) = 0$ and hence $\mathrm{ord}(a \cdot x^e) > e$, and as $\mathrm{ord}(T(x, a \cdot x^e)) > e$, it follows that $\partial_y P(x, k)$ and $\partial_y P(x, h)$ have the same order e. From the first displayed equation we now conclude that $P(x,k)$ has order at least $2e$. Write it as $P(x,k) = x^{2e} \cdot R(x)$ for some polynomial $R(x)$. Divide the first displayed equation by x^{2e} and get

$$a + Q(x,a) + R(x) = 0$$

with $Q(x,y) = x^{-2e} \cdot S(x, y \cdot x^e)$ a polynomial of order at least two in y. Thus the series $a(x) = x^{-e} \cdot (h(x) - k(x))$ is a simple root of the equation

$$\widetilde{P}(x,y) := y + Q(x,y) + R(x) = 0.$$

Remarks. (a) The attentive reader will observe that the proof is a predecessor of the proof of the Artin approximation theorem given below.
(b) If the series h is defined over $\mathbb{Q}$, the polynomials $\widetilde{P}$ and $\widetilde{Q}$ will involve finitely many rational coefficients. Replacing then x by an integer multiple $L \cdot x$ with L having sufficiently many prime divisors (e.g., taking for L the least common multiple of all occurring denominators of $\widetilde{P}$ and $\widetilde{Q}$), one achieves via $\widetilde{P}(L^2 \cdot x, Ly)$ a minimal polynomial for $a(L \cdot x)$ with integer coefficients. This observation will be useful in the proof of the Eisenstein theorem below.
(c) It seems that the above proof does not use that K has characteristic zero.

(d) Algebraic series with complex coefficients are holomorphic.

Eisenstein's theorem (Eisenstein 1852) [Hei, Herm, Sus] *Let* $h(x) = \sum c_k x^k \in \mathbb{Q}\langle x\rangle$ *be an algebraic series in one variable with rational coefficients* $c_k \in \mathbb{Q}$.
(i) *The denominators of the coefficients* a_k *have only finitely many prime divisors.*
(ii) *There exists a non-zero integer* $\ell \in \mathbb{N}$ *so that* $h(\ell \cdot x) \in \mathbb{Z}\langle x\rangle$ *has integer coefficients, i.e.,* h *is globally bounded.*

Remarks. (a) Clearly, assertion (ii) implies (i). Eisenstein stated the theorem without proof in 1852 in the case where h is an étale algebraic series. Heine proposed in 1853 a proof which seems to be incomplete, and then gave in [...] a rigorous proof, cited by Pólya and Szegö in [PoSz]. They also cite Weierstrass. See also [Ber] for an alternative proof within classical algebraic geometry and using the Riemann-Roch theorem. Other proofs were proposed by Hermite and Susák.
(b) We have already seen that rational series are globally bounded. The example $\sqrt{1+x}$ of the introduction is also globally bounded.
(c) There are various attempts to bound the smallest integer ℓ, the so called Eisenstein bound [DvP, Schm, BiBo, DwR].
(d) The theorem implies that univariate algebraic series with rational coefficients which are not polynomials have finite radius of convergence. Indeed, a series in $\mathbb{Z}\langle x\rangle$ is either a polynomial or has radius of convergence ≤ 1.
(e) Denef and Lipshitz prove in [DeLi1, Thm. 6.2, page 60] that any algebraic series in n variables is the diagonal of a rational series in $2n$ variables. From this follows immediately Eisenstein's theorem in several variables, see below. Safonov [Saf1] states and seems to prove the multivariate version of Eisenstein's theorem using the description of multivariate algebraic series as certain diagonals of rational series in just one more variable.

Proof. We give two proofs. (i) (via implicit function theorem) By the univariate Simple Root Lemma we may assume (after truncation at a suitable degree and division of the remainder series by a monomial) that h is an étale algebraic series. Write the minimal polynomial of h as $P(x,y) = \ell y + Q(x,y) + R(x)$, for

$\ell \in \mathbb{Z} \setminus \{0\}$, with polynomials Q and R with integer coefficients and such that Q is at least quadratic with respect to y.
After substitution of x by $\ell^2 \cdot x$ and multiplication of y by ℓ we may assume that P is in fact of the form $P(x,y) = y + Q(x,y) + R(x)$ with polynomials Q and R with integer coefficients. The Newton algorithm described to construct the solution of $P(x,y) = 0$ at 0 then yields the series $h(x)$. It must have integer coefficients since no divisions occur. This is what had to be shown.

(ii) (via diagonals) One may also use Furstenberg's theorem: Every univariate algebraic series $h(x)$ with coefficients in $\mathbb{Q}$ is the diagonal of a rational series in two variables: $r(y,z) = \sum_{ij} c_{ij} y^i z^j$, $\mathrm{diag}(r)(x) := \sum_i c_{ii} x^i$. It is easy to see that rational series are globally bounded, and hence also their diagonals are. ⟳