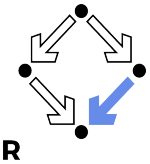
RISC



RESEARCH INSTITUTE FOR
SYMBOLIC COMPUTATION

JKU

JOHANNES KEPLER
UNIVERSITY LINZ

General solutions of first-order algebraic ODEs in simple constant extensions

Johann J. Mitteramskogler, Franz Winkler

September 2021

RISC Report Series No. 21-18

ISSN: 2791-4267 (online)

Available at https://doi.org/10.35011/risc.21-18

JOHANNES KEPLER UNIVERSITY LINZ
Altenberger Str. 69
4040 Linz, Austria
www.jku.at
DVR 0093696

General solutions of first-order algebraic ODEs in simple constant extensions

Johann J. Mitteramskogler Franz Winkler

If a first-order algebraic ODE is defined over a certain differential field, then the most elementary solution class, in which one can hope to find a general solution, is given by the adjunction of a single arbitrary constant to this field. Solutions of this type give rise to a particular kind of generic point—a rational parametrization—of an algebraic curve which is associated in a natural way to the ODE's defining polynomial. As for the opposite direction, we show that a suitable rational parametrization of the associated curve can be extended to a general solution of the ODE if and only if one can find a certain automorphism of the solution field. These automorphisms are determined by linear rational functions, i.e. Möbius transformations. Intrinsic properties of rational parametrizations, in combination with the particular shape of such automorphisms, lead to a number of necessary conditions on the existence of general solutions in this solution class. Furthermore, the desired linear rational function can be determined by solving a simple differential system over the ODE's field of definition. All results are derived in a purely algebraic fashion and apply to any differential field of characteristic zero with arbitrary derivative operator.

1 Introduction and preliminaries

In recent years, a number of algorithms have been published which construct explicit general solutions of first-order algebraic ODEs from a rational parametrization of an associated geometric object.[1] Most notable among such methods, but non-exhaustive in enumeration, are the approaches described in Feng and Gao [1], Ngô and Winkler [6] and Vo, Grasegger and Winkler [11]. Each of these methods starts from a particular rational parametrization of the associated geometric object, which is modified in a subsequent step such that the result can be extended to a general solution of the differential equation. All solutions that are found in this way can be chosen from a simple constant extension of the ODE's differential field of definition.[2]

[1] In fact, these methods follow a general strategy for solving algebraic differential equations, which is known as the *algebro-geometric solution method* [12].

[2] Cf. Mitteramskogler and Winkler [4] for a proof that the method of Ngô and Winkler [6] cannot find general solutions beyond this solution class.

The mentioned algorithms are limited to specific differential fields, i.e. they consider algebraic ODEs over a differential field of rational functions in the variable x, exclusively, where the derivative operator is restricted to $\mathrm{d}/\mathrm{d}x$. Furthermore, the modification step of the latter two algorithms requires solving an associated (system of) differential equation(s). This part relies on additional literature with similar restrictions on the differential field and, in some cases, analytical methods are required for the proofs. Such constraints make a direct extension to other fields or derivative operators difficult.

In this paper, we propose a generalization of the algebro-geometric method to arbitrary differential fields of characteristic zero. First, we establish certain preliminary results on differential extensions by arbitrary constants in Section 2. With this foundation, we prove the existence of special general solutions of first-order algebraic ODEs in Section 3, granted that the differential equation has a general solution in such a constant differential extension field. One property of these special solutions is that they are deducible, via a particular automorphism, from a so-called proper rational parametrization of the curve which we associate to an algebraic ODE. From this link and known properties of proper rational parametrizations, we obtain a number of necessary conditions when an algebraic ODE has a general solution of this type. Finally, we conclude the paper in Section 4 with a possible extension to second-order algebraic ODEs.

We end this section by recalling certain basic notions and results form differential algebra, field theory, and rational algebraic curves. Definitions of the objects under consideration and necessary terminology will be introduced along the way.

Basic differential algebra

We briefly recall a couple of basic notions from differential algebra. Further elaboration can be found in the books of Ritt [8] or Kolchin [3]. Let $\mathcal{R}$ be a ring. An operator δ on $\mathcal{R}$ is called a *derivative operator* if δ is additive and satisfies the Leibniz product rule, i.e. $\delta(a+b) = \delta a + \delta b$ and $\delta(ab) = (\delta a)b + a\delta b$ for all $a, b \in \mathcal{R}$. A ring or field together with a derivative operator is called a *differential ring* or *differential field*, respectively.[3] Elements $c \in \mathcal{R}$ which satisfy $\delta c = 0$ are called *constants* and the set of all constants forms a subring of $\mathcal{R}$. If $\mathcal{R}$ is a field, then the ring of constants is a field as well, called the *field of constants*. Note that the prime field of a differential field is always part of the field of constants.

Let $\mathcal{F}$ be a differential field with derivative operator δ. For convenience, all extensions of $\mathcal{F}$ will be contained in a differential superfield $\mathcal{U}$, which is, roughly speaking, large enough to house an isomorphic copy of any reasonable differential extension of $\mathcal{F}$. More precisely, $\mathcal{U}$ will be a *universal differential extension field* of $\mathcal{F}$, cf. Kolchin [3, Ch. III, Sec. 7] for details.[4] The derivation on $\mathcal{F}$ extends to $\mathcal{U}$ and, by an abuse of notation, δ is also used to denote the derivative operator on $\mathcal{U}$. At times we require that $\mathcal{U}$ contains a certain number of arbitrary constants. By an *arbitrary constant* we understand a constant $c \in \mathcal{U}$ which is transcendental over $\mathcal{F}$. More generally, a collection of *independent arbitrary constants* $c_1, c_2, \ldots \in \mathcal{U}$ denotes a collection of constants such that $\{c_1, c_2, \ldots\}$ is algebraically independent over $\mathcal{F}$. This entails,

[3] Actually, this describes an *ordinary* differential ring or field.

[4] Note that a universal differential extension field is separably closed.

in particular, that each constant c_i is transcendental over $\mathcal{F}$ and over every extension of $\mathcal{F}$ generated via the adjunction of finitely many elements of $\{c_1, c_2, \ldots\} \setminus \{c_i\}$.

An algebraic substructure of $\mathcal{U}$ is called *differential* if it is closed under δ. For $S \subseteq \mathcal{U}$ we denote by $\mathcal{F}[S]$, $\mathcal{F}(S)$, $\mathcal{F}\{S\}$, and $\mathcal{F}\langle S\rangle$ the smallest subring, subfield, differential subring, and differential subfield of $\mathcal{U}$ containing $\mathcal{F}$ and S, respectively. If the cardinality is finite, we will frequently replace S by its elements in the previous notations. Finally, $e_{(n)}$ is used throughout the text to denote $\delta^n e$, the n-th derivative of an element $e \in \mathcal{U}$, with $e_{(0)} = e$.

Interlude from field theory

Let $\mathcal{F}$ be an arbitrary field. If $\mathcal{G} \supseteq \mathcal{F}$ is a field extension, which we denote by $\mathcal{G}/\mathcal{F}$, then the degree of $\mathcal{G}$ over $\mathcal{F}$ and the transcendence degree of $\mathcal{G}$ over $\mathcal{F}$ is denoted by $\deg \mathcal{G}/\mathcal{F}$ and $\operatorname{tr.deg} \mathcal{G}/\mathcal{F}$, respectively. Recall that an extension $\mathcal{G}/\mathcal{F}$ is said to be *purely transcendental* if $\mathcal{G}$ is isomorphic to a field of rational functions over $\mathcal{F}$ in finitely or infinitely many variables.

For a polynomial $F \in \mathcal{F}[\ldots, X, \ldots]$ we write $\deg_X F$ for its degree in the variable X. The notion is extended to the quotient field in the usual way: let $G \in \mathcal{F}(\ldots, X, \ldots)$ be in reduced form,[5] then $\deg_X G$ is defined to be the maximum of the degrees of numerator and denominator in X.[6] It is well-known that every subfield of a univariate rational function field, properly containing the base field, is generated by a single rational function. This classical result is known as *Lüroth's theorem*. An elementary proof can be found in van der Waerden [10, Sec. 73] or Morandi [5, Theorem 22.19].

Theorem 1.1 (Lüroth). *Let $\mathcal{F}(X)$ be the field of rational functions over $\mathcal{F}$ in the variable X. Every intermediate field $\mathcal{F} \subsetneq \mathcal{G} \subseteq \mathcal{F}(X)$ is a purely transcendental extension of the form $\mathcal{G} = \mathcal{F}(G)$ for some $G \in \mathcal{F}(X) \setminus \mathcal{F}$. Furthermore, $\mathcal{F}(X)$ is a finite algebraic extension of $\mathcal{F}(G)$ such that $\deg \mathcal{F}(X)/\mathcal{F}(G) = \deg_X G$.*

Let us briefly touch upon regular field extensions, a concept of considerable interest in algebraic geometry as these characterize absolutely irreducible varieties. An extension $\mathcal{G}/\mathcal{F}$ is said to be *regular* if $\mathcal{G}$ is separable over $\mathcal{F}$ and $\mathcal{F}$ is algebraically closed in $\mathcal{G}$.[7] The following proposition can be found in Fried and Jarden [2, Corollary 10.2.2(b)].

Proposition 1.2. *Consider an irreducible polynomial $F \in \mathcal{F}[X_1, \ldots, X_n]$ and let $e_1, \ldots, e_n$ be elements in a field extension of $\mathcal{F}$ such that $F(e_1, \ldots, e_n) = 0$ and $\operatorname{tr.deg} \mathcal{F}(e_1, \ldots, e_n)/\mathcal{F} = n - 1$. The polynomial F is absolutely irreducible if and only if $\mathcal{F}(e_1, \ldots, e_n)/\mathcal{F}$ is a regular extension.*

In fact, this is a special case of the result that an irreducible $\mathcal{F}$-variety is absolutely irreducible if and only if its quotient field is a regular extension of $\mathcal{F}$. In this text, however, we shall be contented with the specialized version.

Remark 1.3. *Every purely transcendental extension is a regular extension.*

[5] Numerator and denominator are relatively prime.

[6] In either case, we use the convention that $\deg_X 0 := -\infty$.

[7] Alternatively, $\mathcal{G}/\mathcal{F}$ is regular if $\mathcal{G}$ is linearly disjoint from $\widetilde{\mathcal{F}}$ over $\mathcal{F}$, where $\widetilde{\mathcal{F}}$ is the algebraic closure of $\mathcal{F}$.

Rational algebraic curves

Our approach towards rational algebraic curves comes from a field theoretic perspective. The material presented in this section is well-known and can be found in Morandi [5, Ch. V, Sec. 21 and Sec. 22] or Fried and Jarden [2, Ch. 10]. Content specific to rational parametrizations is taken from Sendra, Winkler and Pérez-Díaz [9], which treats rational algebraic curves in characteristic zero, exclusively.

Let $\mathcal{F}$ be a field of characteristic zero and denote by $\mathcal{U}$ an algebraically closed extension field. Further assume that $\mathcal{U}$ contains an element t which is transcendental over $\mathcal{F}$. We limit our exposition on algebraic curves to the case of affine algebraic plane curves defined by irreducible polynomials. Let $\mathcal{R} := \mathcal{F}[X, Y]$ be the bivariate polynomial algebra over $\mathcal{F}$. For $S \subseteq \mathcal{R}$ let

$$\mathbf{Z}(S) := \{(x, y) \in \mathbb{A}^2(\mathcal{U}) \mid F(x, y) = 0 \text{ for all } F \in S\}$$

be the *zero locus* of S, where $\mathbb{A}^2(\mathcal{U})$ denotes the two-dimensional affine space over $\mathcal{U}$. In case of a finite set $S = \{F_1, \ldots, F_n\}$ we also write $\mathbf{Z}(F_1, \ldots, F_n)$.

Definition 1.4. *A subset $\mathcal{C} \subseteq \mathbb{A}^2(\mathcal{U})$ is called an* irreducible algebraic $\mathcal{F}$-curve*, or just* $\mathcal{F}$-curve *for the sake of brevity, if $\mathcal{C} = \mathbf{Z}(F)$ for some non-trivial irreducible polynomial $F \in \mathcal{R}$. Denote by $\mathcal{C}_F := \mathbf{Z}(F)$ the $\mathcal{F}$-curve defined by the zero locus of the polynomial F.*[8]

Evidently, for any $F \in \mathcal{R}$ we have $\mathbf{Z}(F) = \mathbf{Z}((F))$, where $(F) \subseteq \mathcal{R}$ is the ideal generated by F. Let $\mathcal{A} \subseteq \mathbb{A}^2(\mathcal{U})$ and denote by

$$\mathbf{I}(\mathcal{A}) := \{F \in \mathcal{R} \mid F(x, y) = 0 \text{ for all } (x, y) \in \mathcal{A}\}$$

the *vanishing ideal* of $\mathcal{A}$ in $\mathcal{R}$. It applies that $\mathbf{I}(\mathcal{C}_F) = (F)$ for any $\mathcal{F}$-curve $\mathcal{C}_F$. Under the precondition that F is irreducible, we see that the vanishing ideal of an $\mathcal{F}$-curve is a principal prime ideal.

Definition 1.5. *Let $\mathcal{C}$ be an $\mathcal{F}$-curve. The* function field *of $\mathcal{C}$, denoted by $\mathcal{F}(\mathcal{C})$, is the quotient field of the integral domain $\mathcal{R}/\mathbf{I}(\mathcal{C})$. We call $\mathcal{C}$* rational *if $\mathcal{F}(\mathcal{C})/\mathcal{F}$ is a purely transcendental extension.*[9]

Definition 1.6. *Denote by $\widetilde{\mathcal{F}}$ the algebraic closure of $\mathcal{F}$ in $\mathcal{U}$. An $\mathcal{F}$-curve $\mathcal{C}$ is called* absolutely parametrizable *if there exist rational functions $p_X, p_Y \in \widetilde{\mathcal{F}}(t)$ such that $\{(p_X(e), p_Y(e)) \mid e \in \mathcal{U}\}$ is a dense subset of $\mathcal{C}$ wrt. the Zariski $\mathcal{F}$-topology on $\mathbb{A}^2(\mathcal{U})$.*[10] *Furthermore, if such p_X, p_Y can be found in $\mathcal{F}(t)$, then $\mathcal{C}$ is called* parametrizable*. In the latter case, the tuple (p_X, p_Y) is called a* rational parametrization *of $\mathcal{C}$.*

Remark 1.7. *It is impossible for a rational parametrization (p_X, p_Y) of an $\mathcal{F}$-curve $\mathcal{C}_F$ that both $p_X, p_Y \in \mathcal{F}$. This would parametrize an $\mathcal{F}$-closed set—a point—which is certainly not dense in $\mathcal{C}_F$. Conversely, any pair of rational functions $q_X, q_Y \in \mathcal{F}(t)$, not both of them contained in $\mathcal{F}$, which satisfy $F(q_X, q_Y) = 0$ constitute a rational parametrization of $\mathcal{C}_F$ [9, Theorem 4.7].*

[8] The defining polynomial of an $\mathcal{F}$-curve is unique up to multiplication by units in $\mathcal{R}$.

[9] Any $\mathcal{F}$-curve $\mathcal{C}$ satisfies $\operatorname{tr.deg} \mathcal{F}(\mathcal{C})/\mathcal{F} = 1$. Consequently, the function field of a rational $\mathcal{F}$-curve is a simple transcendental extension of $\mathcal{F}$.

[10] The Zariski $\mathcal{F}$-topology on $\mathbb{A}^2(\mathcal{U})$ is defined in terms of its closed sets. A subset $\mathcal{A} \subseteq \mathbb{A}^2(\mathcal{U})$ is closed if it is the zero locus of some set of polynomials over $\mathcal{F}$, viz. $\mathcal{A} = \mathbf{Z}(S)$ for some $S \subseteq \mathcal{R}$.

Remark 1.8. *A rational parametrization is a generic point of the curve's vanishing ideal.*

In general, not every absolutely parametrizable $\mathcal{F}$-curve is parametrizable [9, Ch. 5, Sec. 1]. However, for certain fields these two notions are equivalent, e.g. this is trivially the case when $\mathcal{F}$ is algebraically closed. Furthermore, every simple transcendental extension of an algebraically closed field of characteristic zero has this property [11, Theorem 4.3].

Definition 1.9. *The field $\mathcal{F}$ is called an* optimal parametrization field *if every absolutely parametrizable $\mathcal{F}$-curve is parametrizable.*

Theorem 1.10. *Let $\mathcal{C}_F$ be an $\mathcal{F}$-curve and consider the subsequent statements. We have that (i) is equivalent to (ii) and each imply (iii). All statements are equivalent if $\mathcal{F}$ is an optimal parametrization field.*

(i) The curve $\mathcal{C}$ is rational.
(ii) The curve $\mathcal{C}$ is parametrizable.
(iii) The polynomial F is absolutely irreducible and $\mathcal{C}$ has genus zero.[11]

Proof. The equivalence of (i) and (ii) is shown in Morandi [5, Proposition 22.18]. Any rational parametrization satisfies the conditions of Proposition 1.2, which implies that F is absolutely irreducible. It is well-known that only absolutely irreducible curves can be parametrized by rational functions and this is the case precisely when the curve has genus zero [9, Theorem 4.4 and Theorem 4.63]. The rest follows from the definitions. □

Finally, we come to the concept of proper rational parametrizations. Lüroth's theorem implies that the field $\mathcal{F}(p_X, p_Y)$ generated by the rational parametrization (p_X, p_Y) is an $\mathcal{F}$-isomorphic subfield of $\mathcal{F}(t)$. Properness is attained when the fields are actually equal. Geometrically, this means that a point on the curve is obtained at most once under the parametrization. Any non-proper parametrization can be converted into a proper one.

Definition 1.11. *A rational parametrization (p_X, p_Y) is called* proper *if $\mathcal{F}(p_X, p_Y) = \mathcal{F}(t)$.*

Theorem 1.12 (Sendra, Winkler and Pérez-Díaz [9, Theorem 4.21])**.** *A proper rational parametrization (p_X, p_Y) of the $\mathcal{F}$-curve $\mathcal{C}_F$ satisfies the following conditions on the degrees:* $\deg_t p_X = \deg_Y F$ *and* $\deg_t p_Y = \deg_X F$.

Proper rational parametrizations are far from being unique. However, any two proper parametrizations can be obtained through a linear rational function, also called a *Möbius transformation*. These are precisely the $\mathcal{F}$-automorphisms of $\mathcal{F}(t)$.

Proposition 1.13 (Sendra, Winkler and Pérez-Díaz [9, Lemma 4.17])**.** *Let (p_X, p_Y) and (q_X, q_Y) be two proper rational parametrizations of the same $\mathcal{F}$-curve. There exists a rational function of the form*

$$g = \frac{at + b}{ct + d}, \text{ where } a, b, c, d \in \mathcal{F} \text{ such that } \begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0,$$

with the property that $p_X(g) = q_X$ and $p_Y(g) = q_Y$. Equivalently, there exists an $\mathcal{F}$-automorphism α of $\mathcal{F}(t)$ such that $(\alpha(p_X), \alpha(p_Y)) = (q_X, q_Y)$. Any application of such an automorphism on a proper rational parametrization produces another proper rational parametrization.

[11] Consult Sendra, Winkler and Pérez-Díaz [9, Ch. 3] for details on the genus of an algebraic curve.

2 Constant differential extensions

Throughout this section, let $\mathcal{F}$ be an arbitrary differential field with derivation operator δ and field of constants $\mathcal{K}$. Denote by $\mathcal{U}$ a fixed universal differential extension field of $\mathcal{F}$ containing an infinite number of independent arbitrary constants. All subsequent (differential) fields are subfields of $\mathcal{U}$. Finally, the quantities $c_1, \ldots, c_n$ and c denote distinct independent arbitrary constants.

Extending a differential field by constants behaves like an ordinary field extension, in other words, $\mathcal{F}\langle c_1, \ldots, c_n\rangle$ is identical to $\mathcal{F}(c_1, \ldots, c_n)$ as a field. Such an extension is purely transcendental since $c_1, \ldots, c_n$ are algebraically independent over $\mathcal{F}$. Notice that $\mathcal{F}\langle c_1, \ldots, c_n\rangle$ is the quotient field of the differential integral domain $\mathcal{F}\{c_1, \ldots, c_n\}$ and, therefore, satisfies the classical quotient rule of differentiation. The following lemma shows that the differential extension $\mathcal{F}\langle c_1, \ldots, c_n\rangle$ does not introduce extra constants, viz. constants beyond the adjunction of $c_1, \ldots, c_n$ to the constant field $\mathcal{K}$.

Lemma 2.1. *$\mathcal{K}(c_1, \ldots, c_n)$ is the field of constants of the differential field $\mathcal{F}\langle c_1, \ldots, c_n\rangle$.*

Proof. Obviously, $\mathcal{K}(c_1, \ldots, c_n)$ is contained in the field of constants of $\mathcal{F}\langle c_1, \ldots, c_n\rangle$ and it is enough to show that no additional constants arise. Furthermore, it suffices to show that $\mathcal{K}(c_1)$ is the field of constants of $\mathcal{F}\langle c_1\rangle$, in which case the lemma follows immediately from the fact that $\mathcal{F}\langle c_1, \ldots, c_n\rangle = (\mathcal{F}\langle c_1\rangle)\langle c_2, \ldots, c_n\rangle$.

At first, consider an element $f \in \mathcal{F}[c_1]$ of the form $f = \sum_i f_i c_1^i$ for some $f_i \in \mathcal{F}$. If f is a constant, then we have

$$0 = \delta f = \sum_i (\delta f_i) c_1^i,$$

which forces each δf_i to be zero by the transcendentality of c_1 over $\mathcal{F}$. In other words, $f_i \in \mathcal{K}$ for all i and, consequently, $f \in \mathcal{K}[c_1]$. Now let $g \in \mathcal{F}(c_1)$ be a constant. The case $g = 0$ is trivial and will be neglected in the following reasoning. We may write $g = g_n/g_d$ for some $g_n, g_d \in \mathcal{F}[c_1] \setminus \{0\}$ such that $\gcd(g_n, g_d) = 1$ and g_d is monic.[12] By the quotient rule

$$0 = \delta g = \frac{(\delta g_n) g_d - g_n \delta g_d}{g_d^2},$$

which implies that $(\delta g_n) g_d = g_n \delta g_d$. Both sides of this equation must be zero, for otherwise $g_d \mid g_n \delta g_d$ cannot be satisfied since g_n is relatively prime to g_d and $\deg_{c_1} g_d > \deg_{c_1} \delta g_d$. As $\mathcal{F}[c_1]$ is an integral domain and $g_n \neq 0 \neq g_d$ per assumption, we conclude that $\delta g_n = \delta g_d = 0$. But this implies that $g_n, g_d \in \mathcal{K}[c_1]$ by the previous result, whereby $g \in \mathcal{K}(c_1)$ as required. □

Linear disjointness of algebras over a field is an important concept in field theory for studying arbitrary extensions. In the differential setting, any subset of a differential field which is linearly independent over the field of constants remains linearly independent over the field of constants of any differential extension field [3, Ch. II, Sec. 1, Corollary 1]. This property lies at the basis of the subsequent lemma.

[12] Since $\mathcal{K}$ contains the prime field of $\mathcal{F}$, for any non-zero monic polynomial $f \in \mathcal{F}[c_1]$ we see that $\deg_{c_1} f$ is strictly greater than $\deg_{c_1} \delta f$ (recall that $\deg_{c_1} 0 = -\infty$).

Lemma 2.2 (Kolchin [3, Ch. II, Sec. 1, Corollary 2])**.** *Let $\mathcal{M}$ be the field of constants of a differential extension field of $\mathcal{F}$. Consider the mapping φ that associates to each intermediate differential field $\mathcal{F} \subseteq \mathcal{G} \subseteq \mathcal{F}(\mathcal{M})$ the constant field $\mathcal{G} \cap \mathcal{M}$, and the mapping ψ which associates to an intermediate constant field $\mathcal{K} \subseteq \mathcal{L} \subseteq \mathcal{M}$ the differential field $\mathcal{F}(\mathcal{L})$. The mappings φ and ψ are bijective and inverse to each other.*

Equipped with this lemma, we are in the position to state the main result of this section. Namely, every differential subfield of a simple differential extension by an arbitrary constant is generated by a constant.

Theorem 2.3. *Let $\mathcal{G} \supsetneq \mathcal{F}$ be a differential subfield of the simple constant differential extension $\mathcal{F}\langle c\rangle$. In this case, $\mathcal{G} = \mathcal{F}\langle g\rangle$ for some $g \in \mathcal{K}(c) \setminus \mathcal{K}$.*

Proof. From Lemma 2.1 we know that the field of constants of $\mathcal{F}\langle c\rangle$ is $\mathcal{K}(c)$. Obviously, the differential composite field $\mathcal{F}\langle\mathcal{K}(c)\rangle$ is precisely $\mathcal{F}\langle c\rangle$. Now we are in the position to use the one-to-one correspondence of differential subfields and intermediate constant fields from the antecedent lemma. The subsequent diagram follows directly from Lemma 2.2.

$$\begin{array}{ccccccc}
\mathcal{F} & \overset{\subsetneq}{\text{———}} & \mathcal{G} & = & \mathcal{F}\langle\mathcal{L}\rangle & \overset{\subseteq}{\text{———}} & \mathcal{F}\langle\mathcal{K}(c)\rangle = \mathcal{F}\langle c\rangle \\
\vdots & & \overset{\varphi}{\curvearrowright} & & \overset{\psi}{\curvearrowleft} & & \vdots \\
\mathcal{K} & \overset{\subsetneq}{\text{———}} & \mathcal{G}\cap\mathcal{K}(c) & =: & \mathcal{L} & \overset{\subseteq}{\text{———}} & \mathcal{K}(c)
\end{array}$$

Since $\mathcal{L}$ is a subfield of a simple transcendental extension of $\mathcal{K}$, properly containing the latter, $\mathcal{L} = \mathcal{K}(g)$ for some $g \in \mathcal{K}(c) \setminus \mathcal{K}$ by Theorem 1.1. Considering that $\mathcal{G}$ is the composite of $\mathcal{F}$ and $\mathcal{L}$, it follows that $\mathcal{G} = \mathcal{F}\langle\mathcal{K}(g)\rangle = \mathcal{F}\langle g\rangle$. □

Notice that, since $\mathcal{G}$ is contained in a simple transcendental extension of $\mathcal{F}$, Lüroth's theorem alone would have been enough to predict that $\mathcal{G}$ is generated over $\mathcal{F}$ by a single element $g \in \mathcal{F}(c) \setminus \mathcal{F}$. Theorem 2.3 sharpens this result by stating that g can be selected from the constant field.

Corollary 2.4. *For every intermediate differential field $\mathcal{F} \subsetneq \mathcal{G} \subseteq \mathcal{F}\langle c\rangle$ it applies that $\mathcal{G}$ and $\mathcal{F}\langle c\rangle$ are differentially isomorphic over $\mathcal{F}$.*

Proof. By Theorem 2.3, $\mathcal{G} = \mathcal{F}\langle g\rangle$ for some constant $g \in \mathcal{K}(c) \setminus \mathcal{K}$ which is transcendental over $\mathcal{F}$. The map $\alpha : \mathcal{G} = \mathcal{F}\langle g\rangle \to \mathcal{F}\langle c\rangle$ defined by $\alpha|_{\mathcal{F}} = \mathrm{id}_{\mathcal{F}}$ and $\alpha(g) = c$ is an isomorphism of $\mathcal{F}$-algebras which leaves elements of $\mathcal{F}$ invariant and satisfies $\alpha(\delta g) = 0 = \delta\alpha(g)$. Hence, $\alpha(\delta e) = \delta\alpha(e)$ for all $e \in \mathcal{G}$, which makes α a differential isomorphism over $\mathcal{F}$. □

Remark 2.5. *If we require that the constant field $\mathcal{K}$ is algebraically closed, then Theorem 2.3 and Corollary 2.4 can be generalized to the case $\mathcal{F}\langle c_1, c_2\rangle$. From Lemma 2.1 we know that the constant field of $\mathcal{F}\langle c_1, c_2\rangle$ is $\mathcal{K}(c_1, c_2)$ and, by Castelnuovo's theorem, every intermediate constant field $\mathcal{K} \subsetneq \mathcal{L} \subseteq \mathcal{K}(c_1, c_2)$ is a purely transcendental extension of $\mathcal{K}$. The remaining steps of the proofs are analogous.*

We conclude the section by a handy result on differential fields generated by linear fractional elements. Consider a not necessarily constant element $g \in \mathcal{F}\langle c\rangle$ such that $\deg_c g = 1$. Since $\mathcal{F}\langle g\rangle$ contains a subfield generated by an element of degree one,[13] $\mathcal{F}\langle g\rangle = \mathcal{F}(c) = \mathcal{F}\langle c\rangle$ by Theorem 1.1. As a consequence, δg must be contained in the field $\mathcal{F}(g)$. The following proposition shows how δg can be constructed in terms of the generator g.

Proposition 2.6. *Consider an element $g \in \mathcal{F}\langle c\rangle$ of the form*

$$g = \frac{pc+q}{rc+s},$$

where $p, q, r, s \in \mathcal{F}$. The derivative of g has the representation

$$\begin{vmatrix} p & q \\ r & s \end{vmatrix} \delta g = \begin{vmatrix} p & \delta p \\ q & \delta q \end{vmatrix} + \left(\begin{vmatrix} q & \delta q \\ r & \delta r \end{vmatrix} - \begin{vmatrix} p & \delta p \\ s & \delta s \end{vmatrix} \right) g + \begin{vmatrix} r & \delta r \\ s & \delta s \end{vmatrix} g^2. \tag{1}$$

Proof. The validity of Equation (1) follows from a suitable expansion of the left-hand side. Let $g_\Delta := ps - qr$ and denote by $g_n := pc + q$ and $g_d := rc + s$ the numerator and denominator of g, respectively. By the quotient rule

$$g_\Delta \delta g = \frac{g_\Delta}{g_d^2}((\delta g_n) g_d - g_n \delta g_d) = \frac{1}{g_d^2}\big(g_\Delta (p_{(1)}c + q_{(1)}) g_d + g_n(-g_\Delta)(r_{(1)}c + s_{(1)})\big).$$

Now, $g_\Delta(p_{(1)}c+q_{(1)}) = psp_{(1)}c - qrp_{(1)}c + psq_{(1)} - qrq_{(1)} = (pq_{(1)} - p_{(1)}q)g_d + (p_{(1)}s - q_{(1)}r)g_n$ and, by symmetry, $(-g_\Delta)(r_{(1)}c + s_{(1)}) = (rs_{(1)} - r_{(1)}s)g_n + (r_{(1)}q - s_{(1)}p)g_d$. These identities can be used to rewrite the antecedent equation in the following way

$$\begin{aligned} g_\Delta \delta g &= \frac{1}{g_d^2}\big((pq_{(1)} - p_{(1)}q)g_d^2 + (p_{(1)}s - q_{(1)}r)g_n g_d + (rs_{(1)} - r_{(1)}s)g_n^2 + (r_{(1)}q - s_{(1)}p)g_n g_d\big) \\ &= (pq_{(1)} - p_{(1)}q) + (p_{(1)}s - q_{(1)}r + r_{(1)}q - s_{(1)}p)\frac{g_n}{g_d} + (rs_{(1)} - r_{(1)}s)\frac{g_n^2}{g_d^2}, \end{aligned}$$

which is precisely the right-hand side of Equation (1). □

Remark 2.7. *Under the assumption that g is in reduced form,[14] which is the case precisely when $\left|\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right| \neq 0$, then both sides of Equation (1) can be divided through that quantity and $\delta g \in \mathcal{F}[g] \subseteq \mathcal{F}(g)$.*

3 First-order algebraic ODEs and general solutions

In this section we restrict ourselves to fields of characteristic zero, exclusively. That being said, $\mathcal{F}$ denotes a fixed differential field of characteristic zero with derivative operator δ and field of constants $\mathcal{K}$. Unless specified otherwise, all (differential) field extensions of $\mathcal{F}$ are contained in a predetermined universal differential extension field $\mathcal{U}$ which, in turn, includes the arbitrary constant c.

[13] Namely, the subfield $\mathcal{F}(g)$.
[14] Numerator and denominator have no common factor or, in the present case, $g \notin \mathcal{F}$.

Let Y be a differential variable and consider the differential polynomial algebra $\mathcal{F}\{Y\}$. As an $\mathcal{F}$-algebra, $\mathcal{F}\{Y\}$ corresponds to the polynomial algebra $\mathcal{F}[Y_{(0)}, Y_{(1)}, Y_{(2)}, \ldots]$ in infinitely many variables, where the derivation on $\mathcal{F}$ extends to $\mathcal{F}\{Y\}$ by setting $\delta Y_{(i)} = Y_{(i+1)}$ for all $i \in \mathbb{N}$. Let $F \in \mathcal{F}\{Y\}$ be a non-trivial differential polynomial. The *order* of F, denoted by $\operatorname{ord} F$, is the smallest non-negative number k such that $F \in \mathcal{F}[Y_{(0)}, Y_{(1)}, \ldots, Y_{(k)}]$ or, equivalently, the highest derivative of Y which effectively occurs in F. Furthermore, F is called *irreducible* if it is irreducible as a polynomial over $\mathcal{F}$.

As a differential ring, $\mathcal{F}\{Y\}$ satisfies the ascending chain condition on radical differential ideals.[15] Every proper radical differential ideal is the intersection of a finite number of prime differential ideals and, up to reordering and the usual elimination, such a decomposition is unique. The irredundant prime ideals of such a decomposition are called the *essential prime divisors*.[16] Let $F \in \mathcal{F}\{Y\}$ be a non-trivial irreducible differential polynomial of order k. One can show that the radical differential ideal generated by F, most commonly denoted by $\{F\}$, can be decomposed as

$$\{F\} = (\{F\} : S_F) \cap \{F, S_F\},$$

where $S_F \coloneqq \partial F / \partial Y_{(k)}$ is the separant of F. As F is irreducible, the component $\{F\} : S_F$ is a prime differential ideal and, in fact, an essential prime divisor of $\{F\}$. The radical $\{F, S_F\}$ might further decompose into (possibly zero) primes, all of which contain the separant S_F.[17] These are the so-called *singular components* and are of no further interest in this text. The component $\{F\} : S_F$, on the other hand, is characterized by the fact that it is the unique essential prime divisor which does not contain the separant. [8, Ch. 1 (Decomposition of perfect ideals) and Ch. 2 (General solutions)]

Definition 3.1. *Let $F \in \mathcal{F}\{Y\}$ be a non-trivial irreducible differential polynomial. The essential prime divisor $\{F\} : S_F$ of the radical differential ideal $\{F\}$ is called the* general component *of F.*

Let $y \in \mathcal{U}$ and consider the map $\kappa_y : \mathcal{F}\{Y\} \to \mathcal{F}\langle y \rangle, G(Y) \mapsto G(y)$ which evaluates differential polynomials G at the differential point y. This map is a differential homomorphism of $\mathcal{F}$-algebras whose kernel is a differential prime ideal. We call y a *generic point* of a prime differential ideal $P \subseteq \mathcal{F}\{Y\}$ if $\ker \kappa_y = P$. Note that every prime differential ideal has a generic zero in some differential extension field and we shall use such objects to characterize the general solution of an algebraic ODE.

Definition 3.2. *An* algebraic ODE *or* AODE *is an equation of the form $F = 0$ given by a non-trivial differential polynomial $F \in \mathcal{F}\{Y\}$. The* order *of an AODE is defined as the order of its defining differential polynomial. Under the assumption that F is irreducible, we call $\hat{y} \in \mathcal{U}$ a* general solution *of the AODE $F = 0$ if $\hat{y}$ is a generic point of the general component of F.*

In particular, a general solution annihilates the defining differential polynomial of an AODE and serves as test point for the membership problem of the general component. Henceforth, we tacitly assume that the defining differential polynomial of any AODE is

[15] Authors like Ritt [8] and Kolchin [3] use the term *perfect (differential) ideal* in place of radical differential ideal.
[16] In general, a (differential) ideal I is said to be a *divisor* of a (differential) ideal J if $J \subseteq I$.
[17] Each essential prime divisor of $\{F, S_F\}$ is again of the form $\{G\} : S_G$ for some non-trivial irreducible differential polynomial $G \in \mathcal{F}\{Y\}$ with $\operatorname{ord} G < \operatorname{ord} F$ [3, Ch. IV, Sec. 14, Corollary of Theorem 5].

irreducible. In the contrary case, one may factor the differential polynomial first and collect the solutions of the individual factors. The subsequent proposition gives another very useful description of the general component of a differential polynomial in terms of differential pseudo-remainders, cf. Ritt [8, Ch. 1 (Reduction)] for details on differential reduction.

Proposition 3.3 (Ritt [8, Ch. 2 (General solutions)])**.** *For a non-trivial irreducible differential polynomial $F \in \mathcal{F}\{Y\}$ we have $G \in (\{F\} : S_F) \Leftrightarrow \operatorname{prem}(G, F) = 0$, where $\operatorname{prem}(G, F)$ denotes the differential pseudo-remainder of G wrt. F.*

Remark 3.4. *Proposition 3.3 confirms the preconception that we must extend the base field in order to find a general solution of an AODE of positive order. If $F = 0$ is an AODE of positive order, by the proposition, the general component of F cannot contain a non-zero element of order less than* ord F*. Therefore, $\hat{y} \in \mathcal{F}$ cannot be a general solution of the AODE for this implies that $Y_{(0)} - \hat{y} \in \ker \kappa_{\hat{y}} = (\{F\} : S_F)$, which is impossible since* ord $Y_{(0)} - \hat{y} = 0$*.*

Before we turn our attention to first-order AODEs and their general solutions in constant differential extension fields, the following elementary lemma characterizes simple differential extensions of finite transcendence degree in terms of ordinary (non-differential) field extensions.

Lemma 3.5. *If the simple differential extension $\mathcal{F}\langle e\rangle$ has finite transcendence degree over $\mathcal{F}$, say* tr.deg $\mathcal{F}\langle e\rangle/\mathcal{F} = n$*, then $\mathcal{F}\langle e\rangle = \mathcal{F}(e, \delta e, \ldots, \delta^n e)$.*[18]

Proof. Under the assumption that $\mathcal{F}\langle e\rangle/\mathcal{F}$ has finite transcendence degree, the derivatives of e are algebraically dependent over $\mathcal{F}$. Let m be the smallest non-negative number such that there exists a non-zero polynomial $P \in \mathcal{F}[X_0, \ldots, X_m]$ with $P(e_{(0)}, \ldots, e_{(m)}) = 0$. From among those polynomials, choose P such that it is of minimal degree in X_m. Let $d := \deg_{X_m} P$.

We proceed by showing that $e_{(m+1)} \in \mathcal{F}(e_{(0)}, \ldots, e_{(m)})$, in which case all higher derivatives of e are contained in $\mathcal{F}(e_{(0)}, \ldots, e_{(m)})$ as well. Let $P = \sum_{i=0}^{d} Q_i X_m^i$, where $Q_i \in \mathcal{F}[X_0, \ldots, X_{m-1}]$, and let $q_i := Q_i(e_{(0)}, \ldots, e_{(m-1)})$. Since $\delta e_{(k)}^i = i e_{(k)}^{i-1} e_{(k+1)}$ for all $i > 0$, differentiation of $P(e_{(0)}, \ldots, e_{(m)}) = 0$ yields

$$0 = \delta P\big(e_{(0)}, \ldots, e_{(m)}\big) = \sum_{i=0}^{d} (\delta q_i) e_{(m)}^i + \sum_{i=1}^{d} i q_i e_{(m)}^{i-1} e_{(m+1)}.$$

Notice that each q_i contains derivatives of e of order at most $m-1$, thus $\delta q_i \in \mathcal{F}[e_{(0)}, \ldots, e_{(m)}]$. Rearranging the terms of the antecedent equation yields

$$-\sum_{i=0}^{d} (\delta q_i) e_{(m)}^i = e_{(m+1)} \underbrace{\sum_{i=0}^{d-1} (i+1) q_{i+1} e_{(m)}^i}_{=:r}. \tag{2}$$

Since not all Q_i for $i > 0$ can be zero, the quantity r corresponds to the evaluation of a non-zero polynomial $R \in \mathcal{F}[X_0, \ldots, X_m]$ with $\deg_{X_m} R < d$. By the choice of P, $r = R(e_{(0)}, \ldots, e_{(m)}) \neq 0$. Dividing both sides of Equation (2) by r shows that $e_{(m+1)} \in \mathcal{F}(e_{(0)}, \ldots, e_{(m)})$.

[18] The basic strategy for proving the lemma is borrowed from Pogudin [7, Lemma 1]. However, we do not require that $\mathcal{F}$ is a constant field.

To conclude the proof, it remains to show that $m = \operatorname{tr.deg} \mathcal{F}\langle e\rangle/\mathcal{F} =: n$. It is clear that the set $\{e_{(0)}, \ldots, e_{(n-1)}\}$ cannot be algebraically dependent over $\mathcal{F}$, for otherwise $\mathcal{F}\langle e\rangle = \mathcal{F}(e_{(0)}, \ldots, e_{(n-1)})$ by the previous results and the transcendence degree of $\mathcal{F}\langle e\rangle/\mathcal{F}$ would be strictly smaller than n. Thus, $\{e_{(0)}, \ldots, e_{(n-1)}\}$ is an algebraically independent set of cardinality equal to the transcendence degree, viz. a maximal algebraically independent set. But this implies that $\{e_{(0)}, \ldots, e_{(n)}\}$ is algebraically dependent over $\mathcal{F}$, forcing $m = n$ to be, indeed, the least choice for m. □

For the remainder of the section we restrict our investigations to first-order AODEs. Per assumption, any such differential equation is given by an irreducible differential polynomial $F \in \mathcal{F}[Y_{(0)}, Y_{(1)}]$ such that $\deg_{Y_{(1)}} F > 0$. If we forget about the differential aspect for the moment and view F simply as a bivariate polynomial in the (non-differential) subalgebra $\mathcal{R} = \mathcal{F}[Y_{(0)}, Y_{(1)}] \subseteq \mathcal{F}\{Y\}$, the vanishing locus of F in the affine space $\mathbb{A}^2(\mathcal{U})$ constitutes an $\mathcal{F}$-curve. Recall that the universal differential extension $\mathcal{U}$ is separably closed, which implies in characteristic zero that $\mathcal{U}$ is algebraically closed.

Definition 3.6. *Let $F = 0$ be a first-order AODE and view F as a bivariate polynomial over $\mathcal{F}$. The $\mathcal{F}$-curve $\mathcal{C}_F \subseteq \mathbb{A}^2(\mathcal{U})$ is called the* associated curve *(of the AODE).*

Theorem 3.7. *Let $F = 0$ be a first-order AODE. The existence of a general solution $\hat{y} \in \mathcal{F}\langle c\rangle$ entails the following consequences:*

(i) The differential polynomial F is absolutely irreducible.
(ii) The associated curve $\mathcal{C}_F$ is rational and $(\hat{y}_{(0)}, \hat{y}_{(1)})$ is a rational parametrization.
(iii) There exists a general solution $\hat{z} \in \mathcal{F}\langle c\rangle$ of the AODE such that $(\hat{z}_{(0)}, \hat{z}_{(1)})$ is a proper rational parametrization of $\mathcal{C}_F$.

Proof. (i): Since c is transcendental over $\mathcal{F}$ and $\mathcal{F}\langle c\rangle = \mathcal{F}(c)$, we may view $\hat{y}$ and its derivative as rational functions in the variable c. Remark 3.4 implies that $\hat{y} \notin \mathcal{F}$, in which case Theorem 1.1 (Lüroth's theorem) yields that $\mathcal{F}(\hat{y}_{(0)}, \hat{y}_{(1)})/\mathcal{F}$ is a simple transcendental extension, hence regular. Now, absolute irreducibility of F follows from Proposition 1.2.

(ii): Since $\hat{y} \notin \mathcal{F}$ and $F(\hat{y}_{(0)}, \hat{y}_{(1)}) = 0$, Remark 1.7 asserts that $(\hat{y}_{(0)}, \hat{y}_{(1)})$ is a rational parametrization of $\mathcal{C}_F$. In this case, $\mathcal{C}_F$ must be rational by Theorem 1.10.

(iii): Recall that $\hat{y}$ is a general solution of the AODE if the kernel of the differential evaluation homomorphism $\kappa_{\hat{y}} : \mathcal{F}\{Y\} \to \mathcal{F}\langle\hat{y}\rangle, G(Y) \mapsto G(\hat{y})$ is precisely the general component of F. By Corollary 2.4, there exists a differential $\mathcal{F}$-isomorphism $\alpha : \mathcal{F}\langle\hat{y}\rangle \to \mathcal{F}\langle c\rangle$ and it is clear that $\ker \kappa_{\hat{y}} = \ker(\alpha \circ \kappa_{\hat{y}})$. Consider the image of $\hat{y}$ under the isomorphism and denote it by $\hat{z} := \alpha(\hat{y})$. Per construction, $\mathcal{F}\langle\hat{z}\rangle = \mathcal{F}\langle c\rangle$ and $\hat{y}, \hat{z}$ are generic points of the very same prime differential ideal. Therefore, $\hat{z}$ is a general solution of the AODE as well and yields another rational parametrization of $\mathcal{C}_F$. From Lemma 3.5 we obtain that $\mathcal{F}\langle\hat{z}\rangle = \mathcal{F}(\hat{z}_{(0)}, \hat{z}_{(1)})$. But this means that $\mathcal{F}(\hat{z}_{(0)}, \hat{z}_{(1)}) = \mathcal{F}(c)$, in other words, $(\hat{z}_{(0)}, \hat{z}_{(1)})$ satisfies the definition of a proper rational parametrization. □

Corollary 3.8. *If $F = 0$ is a first-order AODE such that $\deg_{Y_{(0)}} F > 2 \deg_{Y_{(1)}} F$, then there cannot exist a general solution in $\mathcal{F}\langle c\rangle$.*

Proof. Theorem 3.7 implies that any first-order AODE with a general solution in $\mathcal{F}\langle c\rangle$ possesses a general solution $\hat{z} \in \mathcal{F}\langle c\rangle$ which yields a proper rational parametrization of $\mathcal{C}_F$. By the degree conditions on proper parametrizations from Theorem 1.12, $\deg_c \hat{z}_{(0)} = \deg_{Y_{(1)}} F$ and $\deg_c \hat{z}_{(1)} = \deg_{Y_{(0)}} F$. In addition, the degree of the derivative of $\hat{z}$ is bounded by the quotient rule, viz. $\deg_c \hat{z}_{(1)} \leq 2 \deg_c \hat{z}_{(0)}$. Consequently, any AODE with a general solution in $\mathcal{F}\langle c\rangle$ must satisfy $\deg_{Y_{(0)}} F \leq 2 \deg_{Y_{(1)}} F$. □

Remark 3.9 (Quasi-linear AODEs). *A first-order AODE of the form $PY_{(1)} + Q = 0$, where $P, Q \in \mathcal{F}[Y_{(0)}]$, is called* quasi-linear. *According to Corollary 3.8, quasi-linear AODEs cannot possess a general solution in $\mathcal{F}\langle c\rangle$ if their degree in $Y_{(0)}$ exceeds two. Furthermore, if a quasi-linear AODE has a general solution $\hat{y} \in \mathcal{F}\langle c\rangle$, then we can choose*

$$\hat{y} = \frac{pc+q}{rc+s}, \text{ where } p,q,r,s \in \mathcal{F} \text{ such that } \begin{vmatrix} p & q \\ r & s \end{vmatrix} \neq 0.$$

So far we have established that particular general solutions of first-order AODEs give rise to (proper) rational parametrizations of the associated curve. It is natural to ask whether this process is reversible, i.e. if one can derive a general solution from a proper rational parametrization. From a field theoretic perspective, rational parametrizations are merely a particular kind of generic point of the AODE's associated curve. So, alternatively, me might ask which of these generic curve points can be extended to generic differential points of the general component.

Lemma 3.10. *Let $F = 0$ be a first-order AODE. If there exists an element $\hat{y} \in \mathcal{F}\langle c\rangle \setminus \mathcal{F}$ such that $(\hat{y}_{(0)}, \hat{y}_{(1)})$ is a generic point of $\mathcal{C}_F$, then $\hat{y}$ constitutes a general solution of the AODE.*

Proof. Consider the (non-differential) subalgebra $\mathcal{R} = \mathcal{F}[Y_{(0)}, Y_{(1)}] \subseteq \mathcal{F}\{Y\}$ and let

$$\kappa^{\mathcal{R}}_{\hat{y}} : \mathcal{R} \to \mathcal{F}\big(\hat{y}_{(0)}, \hat{y}_{(1)}\big) = \mathcal{F}\langle \hat{y}\rangle,\ G\big(Y_{(0)}, Y_{(1)}\big) \mapsto G\big(\hat{y}_{(0)}, \hat{y}_{(1)}\big)$$

be the evaluation homomorphism at the point $(\hat{y}_{(0)}, \hat{y}_{(1)})$. The identity $\mathcal{F}\big(\hat{y}_{(0)}, \hat{y}_{(1)}\big) = \mathcal{F}\langle \hat{y}\rangle$ is due to Lemma 3.5. If $(\hat{y}_{(0)}, \hat{y}_{(1)})$ is a generic point of the associated curve $\mathcal{C}_F$, then $\ker \kappa^{\mathcal{R}}_{\hat{y}} = \mathbf{I}(\mathcal{C}_F) = (F) \subseteq \mathcal{R}$. Clearly, $\kappa^{\mathcal{R}}_{\hat{y}}$ can be extended to the differential evaluation homomorphism $\kappa_{\hat{y}} : \mathcal{F}\{Y\} \to \mathcal{F}\langle \hat{y}\rangle$, in which case we see that $\kappa_{\hat{y}}\big|_{\mathcal{R}} = \kappa^{\mathcal{R}}_{\hat{y}}$ and $\ker \kappa_{\hat{y}} \cap \mathcal{R} = \ker \kappa^{\mathcal{R}}_{\hat{y}}$. It remains to show that the prime differential ideal $P \coloneqq \ker \kappa_{\hat{y}}$ is equal to the general component of F. By definition, this would make $\hat{y}$ a general solution of the AODE.

Since P is prime, P contains the radical differential ideal generated by any of its elements. Consequently, $F \in P$ implies that $\{F\} \subseteq P$ and P must divide an essential prime divisor of $\{F\}$. Recall that $\{F\} = (\{F\} : S_F) \cap \{F, S_F\}$, where $S_F = \partial F/\partial Y_{(1)} \in \mathcal{R}$. Now, $F \nmid S_F$, which implies that P cannot be a divisor of $\{F, S_F\}$ or of any singular component. Therefore, P must be divisor (a superset) of the general component $\{F\} : S_F$.

For the other direction—$P \subseteq (\{F\} : S_F)$—we make use of Proposition 3.3. Let $G \in P$ and denote by $R \coloneqq \operatorname{prem}(G, F)$ the differential pseudo-remainder of G wrt. F. By the proposition, we have to show that $R = 0$. Aiming for a contradiction, assume that $R \neq 0$. By construction, R can be either trivial or of order at most $\operatorname{ord} F = 1$. In addition, if $\operatorname{ord} R = \operatorname{ord} F$, then

$\deg_{Y_{(1)}} R < \deg_{Y_{(1)}} F$. We find that $R \in \mathcal{R}$ such that $F \nmid R$. According to Ritt [8, Ch. 1 (Reduction)] there exists a differential polynomial $H \in \mathcal{F}\{Y\}$ such that $HG \equiv R \bmod [F]$.[19] Consequently, $HG - R \in \{F\} \subseteq P$, in other words, $HG - R \in \ker \kappa_y$. It is clear that $HG \in \ker \kappa_y$, whereby $R \in \ker \kappa_y$ as well. But such a thing is impossible since $R \in \mathcal{R}$ and $\ker \kappa_y \cap \mathcal{R} = \ker \kappa_y^{\mathcal{R}}$ cannot contain an element which is not divisible by F. This forces $R = 0$ which concludes the proof. □

Theorem 3.11. *Let $F = 0$ be a first-order AODE such that $\mathcal{C}_F$ is rational and let $(p_{Y_{(0)}}, p_{Y_{(1)}})$ be a proper rational parametrization, where $p_{Y_{(0)}}, p_{Y_{(1)}} \in \mathcal{F}(c)$. There exists a general solution $\hat{y} \in \mathcal{F}\langle c\rangle$ if and only if one can find an $\mathcal{F}$-automorphism α of the field $\mathcal{F}(c)$ such that $\delta\alpha(p_{Y_{(0)}}) = \alpha(p_{Y_{(1)}})$. In the affirmative case, $\hat{y} = \alpha(p_{Y_{(0)}})$ is such a general solution of the AODE.*

Proof. The first direction follows readily from Theorem 3.7. Assume that the AODE has a general solution in $\mathcal{F}\langle c\rangle$. Item (iii) of the theorem asserts the existence of a general solution $\hat{z} \in \mathcal{F}\langle c\rangle$ with the property that $(\hat{z}_{(0)}, \hat{z}_{(1)})$ is a proper rational parametrization of $\mathcal{C}_F$. By Proposition 1.13, there exists an $\mathcal{F}$-automorphism $\alpha : \mathcal{F}(c) \to \mathcal{F}(c)$ such that $\alpha(p_{Y_{(0)}}) = \hat{z}_{(0)}$ and $\alpha(p_{Y_{(1)}}) = \hat{z}_{(1)}$. Obviously, $\delta\alpha(p_{Y_{(0)}}) = \alpha(p_{Y_{(1)}})$ in such a case.

For the other direction, assume we can find an automorphism α satisfying the requirements of the theorem. Recall that the transformation $(\alpha(p_{Y_{(0)}}), \alpha(p_{Y_{(1)}}))$ produces another proper rational parametrization of $\mathcal{C}_F$. Therefore, $\deg_c \alpha(p_{Y_{(0)}}) = \deg_{Y_{(1)}} F > 0$ by the degree conditions from Theorem 1.12 and, consequently, $\alpha(p_{Y_{(0)}}) \notin \mathcal{F}$. Since $\delta\alpha(p_{Y_{(0)}}) = \alpha(p_{Y_{(1)}})$, Lemma 3.10 asserts that $\alpha(p_{Y_{(0)}})$ is a general solution of the AODE. □

We find that the task of computing a general solution of a first-order AODE can be reduced to the search for a particular automorphism of a univariate rational function field, granted we are in possession of a proper rational parametrization of the associated curve. The objectives of deciding whether an algebraic curve is rational and the deduction of a proper rational parametrization are well-studied in the literature.[20] For the remainder of the section we analyze how the problem of finding the elusive automorphism can be turned into solving a system of differential equations over $\mathcal{F}$. To do so, we use the fact that these automorphisms are determined by linear rational functions.

As a preliminary step, recall how the derivative of an element in $\mathcal{F}(c)$ behaves when each occurrence of c is replaced by an element $e \in \mathcal{U}$. Initially, let $f \in \mathcal{F}[c]$. The derivative of f after substitution of e for the constant c is of the form

$$\delta f(e) = (\delta f)(e) + (\delta e) \cdot \left(\frac{\partial f}{\partial c}\right)(e).$$

It is not difficult to see that the identity can be extended to the quotient field $\mathcal{F}(c)$ if e does not annihilate the denominator.[21] For our purpose, e will be transcendental over $\mathcal{F}$, so this condition is always met.

[19] More precisely, H consists of non-negative powers of the separant and the so-called initial of F. The object $[F] \subseteq \mathcal{F}\{Y\}$ denotes the differential ideal generated by F.

[20] Cf. Sendra, Winkler and Pérez-Díaz [9, Ch. 4] and the references therein for further information.

[21] Basically, this is just the usual chain rule from calculus.

Proposition 3.12. *Using the objects and notation from Theorem 3.11, a necessary condition for the existence of the automorphism α is that*

$$\left(p_{Y_{(1)}} - \delta p_{Y_{(0)}}\right) \Big/ \frac{\partial p_{Y_{(0)}}}{\partial c} = u + vc + wc^2 \tag{3}$$

for some $u, v, w \in \mathcal{F}$. Should Equation (3) be satisfiable, then α can be deduced by solving either of the following differential systems for $p, q\,(, s) \in \mathcal{F}$:

$$\begin{gathered} \{\, \delta p = vp,\ \delta q = vq + u,\ w = 0,\ p \neq 0 \,\} \\ \textit{or} \\ \left\{\, \delta p = wp^2 + vp + u,\ \delta q = wpq + vq + us,\ \delta s = wps - wq,\ ps \neq q \,\right\}. \end{gathered} \tag{4}$$

If soluble, let $g = pc + q$ or $g = {}^{(pc+q)}/_{(c+s)}$, respectively. The desired $\mathcal{F}$-automorphism is given by $\alpha : \mathcal{F}(c) \to \mathcal{F}(c), G(c) \mapsto G(g)$.

Proof. Recall that the $\mathcal{F}$-automorphisms of $\mathcal{F}(c)$ are determined by Möbius transformations, i.e. they are given by linear rational functions $g \in \mathcal{F}(c)$ of the form

$$g = \frac{pc + q}{rc + s}, \text{ where } p, q, r, s \in \mathcal{F} \text{ such that } \begin{vmatrix} p & q \\ r & s \end{vmatrix} \neq 0.$$

To find an $\mathcal{F}$-automorphism α satisfying $\delta\alpha(p_{Y_{(0)}}) = \alpha(p_{Y_{(1)}})$ is equivalent to deducing a linear rational function of the antecedent form such that $\delta p_{Y_{(0)}}(g) = p_{Y_{(1)}}(g)$. Differentiation of the left-hand side of the latter equation, utilizing the aforementioned chain rule, shows that

$$\delta g = \left(p_{Y_{(1)}}(g) - \left(\delta p_{Y_{(0)}}\right)(g)\right) \Big/ \left(\frac{\partial p_{Y_{(0)}}}{\partial c}\right)(g) \tag{5}$$

after rearranging terms. Notice that the partial derivative of $p_{Y_{(0)}}$ cannot vanish; according to the degree conditions on proper rational parametrizations, $\deg_c p_{Y_{(0)}} > 0$ and ${}^{\partial p_{Y_{(0)}}}/_{\partial c} \neq 0$, thus. Furthermore, Proposition 2.6 shows that the derivative of a linear rational function satisfies

$$\delta g = \frac{\left|\begin{smallmatrix} p & \delta p \\ q & \delta q \end{smallmatrix}\right|}{\left|\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right|} + \frac{\left(\left|\begin{smallmatrix} q & \delta q \\ r & \delta r \end{smallmatrix}\right| - \left|\begin{smallmatrix} p & \delta p \\ s & \delta s \end{smallmatrix}\right|\right)}{\left|\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right|} g + \frac{\left|\begin{smallmatrix} r & \delta r \\ s & \delta s \end{smallmatrix}\right|}{\left|\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right|} g^2 \tag{6}$$

since $\left|\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right| \neq 0$. Comparing these two identities for δg, the left-hand side of Equation (3) must simplify to a polynomial in c of degree at most two, should g exist. Stated differently, Equation (5) must reduce to either a linear differential equation or a Riccati equation. The differential systems (4) follow from simple pattern matching. Notice that we can eliminate the unknown r by splitting g into the cases $r = 0$ and $r = 1$. In the former case, we can assume $s = 1$, w.l.o.g. Matching the coefficients on the right-hand side of Equation (6) against u, v, w yields the differential systems

$$\begin{gathered} \left\{\, up = \left|\begin{smallmatrix} p & \delta p \\ q & \delta q \end{smallmatrix}\right|,\ vp = \delta p,\ wp = 0,\ p \neq 0 \,\right\} \\ \textit{and} \\ \left\{\, u(ps - q) = \left|\begin{smallmatrix} p & \delta p \\ q & \delta q \end{smallmatrix}\right|,\ v(q - ps) = \delta q + \left|\begin{smallmatrix} p & \delta p \\ s & \delta s \end{smallmatrix}\right|,\ w(ps - q) = \delta s,\ ps \neq q \,\right\} \end{gathered} \tag{7}$$

for the cases $r = 0, s = 1$ and $r = 1$, respectively. These systems can be further simplified by substituting the derivatives of the unknowns into the other equations.[22] After rearranging terms, one obtains the differential systems (4). □

At last we see how to deduce a general solution of a first-order AODE from a special generic point—a proper rational parametrization—of the associated curve. For a better overview, the different steps and conditions of this procedure are summarized in Algorithm 1.

Algorithm 1: General solution of a first-order AODE in a simple constant extension

Input : First-order AODE $F = 0$ such that $F \in \mathcal{F}[Y_{(0)}, Y_{(1)}]$ is irreducible
Output : General solution $\hat{y} \in \mathcal{F}\langle c\rangle$ or string message

1 **if** *F is absolutely irreducible* **and** $\deg_{Y_{(0)}} F \leq 2 \deg_{Y_{(1)}} F$ **and** genus $\mathcal{C}_F = 0$ **then**
2 Compute $(p_{Y_{(0)}}, p_{Y_{(1)}}) \in \mathcal{F}(c) \times \mathcal{F}(c)$, a proper rational parametrization of $\mathcal{C}_F$.
3 **if** *such a parametrization does not exist* **then**
  `// Reached only if` $\mathcal{F}$ `is not an optimal parametrization field`
4 **goto** Step 10
5 Construct $G := \left(p_{Y_{(1)}} - \delta p_{Y_{(0)}}\right) \Big/ \frac{\partial p_{Y_{(0)}}}{\partial c}$.
6 **if** *$G = u + vc + wc^2$ for some $u, v, w \in \mathcal{F}$* **then**
  `// Find` g `either directly or by solving any of the`
  `// differential systems (4) from Proposition 3.12`
7 Determine $g = \frac{pc+q}{rc+s}$, where $p, q, r, s \in \mathcal{F}$ and $\left|\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right| \neq 0$, satisfying

$$\delta g = u + vg + wg^2.$$

8 **if** *such a linear rational function exists* **then**
9 **return** $\hat{y} = p_{Y_{(0)}}(g)$
10 **return** *"AODE does not possess a general solution in $\mathcal{F}\langle c\rangle$"*

4 Conclusion and outlook

It has been shown that, for first-order AODEs, the problem of finding a general solution in a simple constant differential extension reduces to the computation of a proper rational parametrization of the associated curve, followed by the deduction of a suitable linear rational function. The coefficients of this linear rational function can found by solving a system of (quasi-)linear differential equations over the AODE's differential field of definition.

A key step in this derivation was to prove the existence of special general solutions, which give rise to proper rational parametrizations of the associated curve. From this point onward, we could use the knowledge that any two proper rational parametrizations are related via

[22] Alternatively, fix an orderly ranking of the differential variables p, q, s and compute characteristic sets from the systems (7), cf. Kolchin [3, Ch. I, Sec. 10] for details.

Möbius transformations. Remark 2.5 suggests that we can also find these special solutions in differential extensions generated by the adjunction of two arbitrary constants, granted that the field of constants is algebraically closed. This would be a natural setting for the search for general solutions of second-order AODEs. In this case, Möbius transformations are replaced by birational transformations of the plane, i.e. Cremona transformations.

References

[1] Ruyong Feng and Xiao-shan Gao. 'Rational General Solutions of Algebraic Ordinary Differential Equations'. In: *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*. ISSAC '04. New York, NY, USA, 2004, pp. 155–162. DOI: 10.1145/1005285.1005309.

[2] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. 3rd ed. Ergebnisse Der Mathematik Und Ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Berlin Heidelberg: Springer-Verlag, 2008. ISBN: 978-3-540-77269-9. DOI: 10.1007/978-3-540-77270-5.

[3] Ellis R. Kolchin. *Differential Algebra and Algebraic Groups*. Pure and Applied Mathematics 54. Academic Press, 1973. ISBN: 978-0-12-417650-8.

[4] Johann J. Mitteramskogler and Franz Winkler. 'Symbolic Solutions of Algebraic ODEs—A Comparison of Methods'. In: *to appear in Publicationes Mathematicae Debrecen* 100 (2022).

[5] Patrick Morandi. *Field and Galois Theory*. Graduate Texts in Mathematics 167. New York: Springer-Verlag, 1996. ISBN: 978-0-387-94753-2. DOI: 10.1007/978-1-4612-4040-2.

[6] Châu L. X. Ngô and Franz Winkler. 'Rational General Solutions of First Order Non-Autonomous Parametrizable ODEs'. In: *Journal of Symbolic Computation* 45 (2010), pp. 1426–1441. DOI: 10.1016/j.jsc.2010.06.018.

[7] Gleb A. Pogudin. 'The Primitive Element Theorem for Differential Fields with Zero Derivation on the Ground Field'. In: *Journal of Pure and Applied Algebra* 219.9 (2015), pp. 4035–4041. DOI: 10.1016/j.jpaa.2015.02.004.

[8] Joseph F. Ritt. *Differential Algebra*. Colloquium Publications 33. American Mathematical Society, 1950. ISBN: 978-0-8218-4638-4.

[9] J. Rafael Sendra, Franz Winkler and Sonia Pérez-Díaz. *Rational Algebraic Curves: A Computer Algebra Approach*. Algorithms and Computation in Mathematics 22. Berlin Heidelberg New York: Springer-Verlag, 2008. ISBN: 978-3-540-73724-7. DOI: 10.1007/978-3-540-73725-4.

[10] Bartel L. van der Waerden. *Algebra I*. 8th ed. Heidelberger Taschenbücher Band 12. Berlin Heidelberg New York: Springer-Verlag, 1971. ISBN: 978-3-642-96044-4. DOI: 10.1007/978-3-642-96044-4.

[11] N. Thieu Vo, Georg Grasegger and Franz Winkler. 'Deciding the Existence of Rational General Solutions for First-Order Algebraic ODEs'. In: *Journal of Symbolic Computation* 87 (2018), pp. 127–139. DOI: 10.1016/j.jsc.2017.06.003.

[12] Franz Winkler. 'The Algebro-Geometric Method for Solving Algebraic Differential Equations—A Survey'. In: *Journal of Systems Science and Complexity* 32 (2019), pp. 256–270. DOI: 10.1007/s11424-019-8348-0.