# On the Computation of the Differential Galois Group

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Mathematiker
Daniel Rettstadt
aus Seesen

| | | |
|---|---|---|
| Berichter: | Universitätsprofessorin | Dr. Julia Hartmann |
| | Universitätsprofessor | Dr. Sebastian Walcher |

Tag der mündlichen Prüfung: 16.06.2014

# Contents

# Introduction

When studying solutions of a given linear differential equation

$$L(y) = \frac{d^n y(x)}{(dx)^n} + a_{n-1}(x)\frac{d^{n-1}y(x)}{(dx)^{n-1}} + \ldots + a_1(x)\frac{dy(x)}{dx} + a_0(x)y(x) = 0$$

with $a_i(x) \in \overline{\mathbb{Q}(x)}$ there are several important classes: Rational solutions (i.e. those which lie in $\mathbb{Q}(x)$), exponential solutions (i.e. those with rational logarithmic derivative) and Liouvillian solutions (i.e. those which are iterated algebraic combinations of exponentials, integrals and algebraic elements).
But in general the solutions of differential equations can not be explicitly calculated and do not belong to any of those mentioned classes. Differential Galois theory allows to derive further properties of the solutions of a given linear differential equation using the symmetry group of the solution space.
This thesis is concerned with the computation of these symmetry groups. In contrast to existing algorithms, which are not explicit and of theoretical nature, we can precisely state the necessary steps. Reducing these steps to classical problems in algebraic geometry or differential algebra we can show how most of the computations can be done and provide computer implementations to solve them.

Analogous to the classical Galois theory for polynomial equations, the starting point is a base field $\mathbb{F}$ and a differential equation $L(y) = 0$ of order $n$. The field is equipped with a derivation $\delta$, i.e., the tuple $(\mathbb{F}, \delta)$ is a differential field. The constants $\mathbb{F}_0$ of $\mathbb{F}$ are the kernel of the derivative $\delta$, which we require to be algebraically closed.
The Picard-Vessiot field is defined as a differential field extension $\mathbb{K}$ that has no new constants and is generated over $\mathbb{F}$ by a maximal $\mathbb{F}_0$-linearly independent set of solutions of $L(y) = 0$. It is unique up to isomorphism.
The differential Galois group $\mathscr{G}$ finally is the group of $\mathbb{F}$-automorphisms of $\mathbb{K}$, which commute with the derivation. After a choice of a basis of the solution space, the Galois group $\mathscr{G}$ can be embedded into the general linear group $\mathrm{GL}_n(\mathbb{F}_0)$. Moreover $\mathscr{G}$ has the structure of a linear algebraic group over $\mathbb{F}_0$.
As in classical Galois theory, there is a Galois correspondence of algebraic subgroups of $\mathscr{G}$ and differential subfields of $\mathbb{K}$.
An example how to derive information from the differential Galois group is the following well known result: All solutions of $L(y) = 0$ are Liouvillian if and only if $\mathscr{G}^\circ$ is solvable.

Kovacic gave in [Kov86] methods to compute the differential Galois group for differential equations of order two.
For a reductive differential Galois group $\mathscr{G}$, the corresponding Picard-Vessiot field can be described by the invariants of $\mathscr{G}$, as shown in [Com98]. After van Hoeij and Weil gave effective methods to compute these invariants in [vHW97], Compoint and Singer were able to give an

algorithm that computes the differential Galois group if it is reductive, see [CS99]. Given the differential equation it is easy to check whether the corresponding differential Galois group is reductive or not (see [Sin96]). Note that this approach can not be generalized as it requires that the invariants are finitely generated, which is in general only true for reductive groups. Hrushovski presented an algorithm in [Hru02] to compute the differential Galois group of a general linear differential equation.
By computing the differential Galois group $\mathscr{G}$, we mean computing the defining polynomials of the representation of $\mathscr{G}$ in $\mathrm{GL}_n(\mathbb{F}_0)$. At several steps Hrushovskis work does not give an computable algorithm, but mere existence statements.
The starting point of Hrushovskis algorithm is [Hru02, Corollary 3.7]:

**Theorem (Hrushovski).** *Given $n \in \mathbb{N}$ there exists a number $B(n)$ and a family $\mathfrak{F}$ of subgroups of $\mathrm{GL}_n(\mathbb{F}_0)$, whose defining ideals are generated by polynomials of degree less than or equal to $B(n)$, with the property: For every closed subgroup $\mathscr{G} \leq \mathrm{GL}_n(\mathbb{F}_0)$ there exists $\mathscr{F} \in \mathfrak{F}$ with*

$$\mathscr{F}^u \lhd \mathscr{G}^\circ \leq \mathscr{G} \leq \mathscr{F} \ .$$

*Here $\mathscr{F}^u$ is the subgroup of $\mathscr{F}$ generated by unipotent elements.*

A first main result is achieved by reconstructing the various parts of Hrushovski original proof with Gröbner bases. This way we obtain a different proof of the above theorem in the language of algebraic geometry. In particular we can compute a bound on the number $B(n)$ (see Corollary 2.37).
Then Hrushovskis applies this theorem to the representation of the differential Galois group $\mathscr{G}$ inside $\mathrm{GL}_n(\mathbb{F}_0)$: One obtains a subgroup $\mathscr{F} \in \mathrm{GL}_n(\mathbb{F}_0)$ bounding $\mathscr{G}$ from both sides (in the above sense), which we will call a Pre-Galois group.
Knowing the existence of Pre-Galois groups, the question arises how to compute such a group.
In [Hru02, Lemma 3.8] it is shown that one can compute a Pre-Galois group by taking the stabilizer of a certain family of subvarieties of $\mathbb{K}^{n\times n}$.
We give a different method to define a Pre-Galois group, which relies on the structure of the ring of differential operators:
In the non-commutative ring of differential operators $\mathbb{F}[\delta]$ every differential operator can be written as the product of irreducible differential operators. From such a given factorization, every other factorization can be obtained by a finite number of interchanges of adjacent irreducible factors. Interchanging two adjacent factors means they switch places in the factorization and both are replaced by similar operators without changing the product. Two factors are similar, if we can not distinguish them by the action of the differential Galois group.
The structure of the ring of differential operators has been investigated by Ore in [Ore32a] and [Ore32b].
After restating and proving Ores ideas in new terminology, we can develop an algorithm that decides whether two differential operators interchange. In particular we get the following result (Proposition 4.45):

**Proposition.** *Let $\mathbb{F}$ be a differential field such that rational solutions of differential operators in $\mathbb{F}[\delta]$ are computable. Given a linear differential operator $K \in \mathbb{F}[\delta]$. If no pair of irreducible factors of $K$ are similar, then we can compute all factorizations of $K$.*

In particular $\overline{\mathbb{Q}}(x)$ meets the requirements of this proposition.
Denote the solution space of $L(y) = 0$ in $\mathbb{K}$ by $V$. It is an $\mathbb{F}_0$-vector space of dimension $n$. For every element $w$ in the tensor algebra $T(V)$ of $V$, we can construct a differential operator

$K$, which has $w$ as a solution. If $k$ is the highest tensor product power of any summand of such a $w$, then we call $K$ a $k$-th power tensorial construction of $L$.

**Theorem.** *Given $L(y) = 0$ with differential Galois group $\mathscr{G}$. One can compute a $(n+1)B(n)$-th power tensorial construction $K$ of $L$ such that the stabilizer of the solution spaces of all right hand factors of $K$ is a Pre-Galois group for the representation of $\mathscr{G}$.*

The above theorem is another main result of this thesis. It shows that there is an explicit, algebraic description of a Pre-Galois group. This theorem together with the computability of $B(n)$ are the main reasons that a analog to Hrushovskis algorithm to compute a differential Galois group exists and can be formulated in the language of differential algebra and algebraic geomtery, avoiding model-theoretic arguments.
In the general case, the computation of all right hand factors is an open problem. We can solve this in the special case mentioned in the proposition above.
Once we have calculated a Pre-Galois group $\mathscr{H}$, we proceed in a similar fashion as Hrushovski: Take a generating set $\{\chi_1, \ldots, \chi_r\}$ of the character group of $\mathscr{H}^\circ$ and define a map $\chi\colon \mathscr{H}^\circ \to \mathbb{G}_m^r$ by $\chi(h) = (\chi_1(h), \ldots, \chi_r(h))$. If we restrict $\chi$ to $\mathscr{G}^\circ$, then its image is a torus $\mathscr{T}$. From [CS99] we can derive that this torus is the computable image of a map $\eta$. In Theorem 5.19 we show that the connected component of the pullback of $\eta$ equals $\mathscr{G}^\circ$.
From this pullback we construct a torsor over $\overline{\mathbb{F}}$. Note that such torsor has an $\overline{\mathbb{F}}$-rational point. If we can find such an $\overline{\mathbb{F}}$-rational point, we denote by $\Theta$ the (classical) Galois group over its field of definition. Note that the problem of computating $\overline{\mathbb{F}}$-rational points also occurs in Hrushovskis algorithm.
The differential Galois group $\mathscr{G}$ is given by the action of $\Theta$ on the defining equation of $\mathscr{G}^\circ$ (see Theorem 5.23).
We also give methods to compute generators of the character group of $\mathscr{H}^\circ$, again under the assumption of computability of a $\overline{\mathbb{F}}$-rational point of a certain torsor.
The presented algorithm is modular, meaning that the individual parts are seperated and should allow replacement by improvement or different methods.

In Chapter 1 notation and well-known results about Gröbner bases are presented. In Chapter 2 we develop bounds for various constructions from algebraic geometry. These bounds together with Gröbner bases techniques render the proof and computation of Hrushovskis bound $B(n)$ possible. Chapter 1 and 2 only deal with algebraic geometry and do not require any differential structure.
The third chapter gives a brief introduction to differential algebra and differential Galois theory. In the fourth chapter we develop algorithms, which help to compute all factors of a given linear differential operator. In particular we present an algorithm that decides whether two given differential operators swap and/or are similar.
In Chapter 5, Section 1 we compute the above-mentioned tensorial construction of $L$ and prove that the stabilizer of its solution space is in fact a Pre-Galois group. The computation of generators of the character group of $\mathscr{H}^\circ$ is presented in Chapter 5, Section 2.
Using these generators and the Pre-Galois group we compute the connected component $\mathscr{G}^\circ$ of the differential Galois group in Chapter 5 Section 3. In particular we show how to apply the methods of [CS99]. The last section of Chapter 5 then computes the differential Galois group by conjugation on the defining polynomials of $\mathscr{G}^\circ$.
Most of the implementations that were programmed during the progress of writing this thesis can be found in Chapter 6.
Subsequent to this introdcution we give a brief overview of the algorithm, which might help to understand the structure and briefly lists all required results.

## Acknowledgements

I am in great debt to my supervisor, Professor Julia Hartmann, who made this thesis possible. She introduced me to this topic, was always understanding and supportive. Her invaluable advice guided me through all stages of work.
Also J.Hartmann provided a friendly and inspiring atmosphere for our young research group Lehrstuhl für Mathematik (Algebra). I thank Michael, Stefan and most of all Annette for many fruitful discussions and for never growing tired to listen to my ideas.
I am thankful to Larry Smith for introducing me to Julia and being a very valuable mentor in my student years.
I thank Michael Singer for his hospitality and friendly discussion during my short research stay at the North Carolina State University.
I thank Ruyong Feng for rich email discussion and providing a different view on the topic.
During my research at the RWTH Aachen, I encountered many helpful, friendly and cooperative people; I want to express my gratitude to all of them. In particular I want to mention Viktor Levandovskyy and Albert Heinle for new ideas and many discussions.
All my life my parents were full-hearted supportive, while still overlooking my occasional grumpiness. I thank them for all they did for me.
Finally I thank Ann and Andy for always keeping my sanity up.

I am also very grateful that my research was partially funded by Deutsche Forschungs Gemeinschaft (DFG) under Schwerpunktprogramm Darstellungstheorie 1388.

# The Algorithm: Overview

This brief chapter is a summary of the algorithm proposed by this thesis. It might facilitate the orientation in this thesis and help to understand the value of the individual chapters and results.
Let $\mathbb{F}$ be an algebraic field extension of $\mathbb{Q}(t)$ and $\delta = \frac{d}{dt}$.
Furthermore $L(y) = 0$ is a linear differential equation with $L \in \mathbb{F}[\delta]$. We denote by $\mathbb{K}$ a Picard-Vessiot field obtained from $L$. The companion matrix $A$ of $L$ gives a matrix differential equation $\delta(Y) = AY$. A fundamental solution matrix $F_A$ for this equation gives a representation $\phi\colon \mathscr{G} \to \mathrm{GL}_n(\mathbb{C})$.
Under the assumption that we can find two rational points and compute all right hand factors of a certain differential operator $\mathbb{L}$, the following algorithm computes $\phi(\mathscr{G})$.

**1. Compute a bound $e = (n+1)B_5(n) \in \mathbb{N}$**

How this number is computed, is shown in the proof of Corollary 2.37.

**2. Define $\mathscr{H}$ as in Theorem 5.2**

By Theorem 5.2 we know that $\mathscr{H}$ is a Pre-Galois group for $\mathscr{G}$.

**3. Compute the defining ideal $\mathcal{I}(\mathscr{H})$ and its primary decomposition**

This step is done by first computing all right hand factors of $\mathbb{L} := \mathrm{LCLM}(L_n^{\circledS i} \mid i = 0 \ldots, e)$ up to similarity. In certain cases (if $\mathbb{L}$ has no pair of interchanging similar irreducible factors) the right hand factors of $\mathbb{L}$ can be computed with the methods presented in Section 4.4.3. Then we compute $\mathcal{I}(\mathscr{H})$ using Lemma 4.56.

**4. Find $g$ as in Proposition 5.6**

This is an open problem in general. We assumed that this can be done, see Assumption 5.8, 5.9.

**5. Compute generators $\chi_1, \ldots, \chi_l$ of the characters of $\mathscr{H}^\circ$**

How this can be computed is shown in Theorem 5.11. These characters define an exponential field extension $\mathbb{E}$ of $\overline{\mathbb{C}(t)}$ (see Section 5.3).
Then we can define a map $\eta\colon (\mathbb{C}^\times)^l \to \mathrm{Gal}(\mathbb{E}/\overline{\mathbb{C}(t)})$. Results of [CS99] show us in Theorem 5.19 that the image of $\mathscr{G}^\circ$ in $\mathrm{GL}_n(\mathbb{F}_0)$ is $H^\circ$.

**6. Compute $H^\circ$ as in Theorem 5.19**

Having computed generators for the character group of $\mathscr{H}^\circ$, we compute relations among them using results of [CS99]. These relations yield $H$. Gröbner basis techniques allow us to compute $H^\circ$ (see Theorem 1.25).

**7. Compute $\tilde{g}$ as in Proposition 5.21**

Here again we assumed that this computation can be done.
Since the entries of $\tilde{g}$ are in an algebraic extension $\mathbb{F}_2$ of $\mathbb{C}(t)$, we can define the (algebraic) Galois group $\Theta = \mathrm{Gal}(\mathbb{F}_2/\mathbb{C}(t))$.

**8. Conjugate the generators of $H^\circ$ by elements in $\Theta$ to obtain the image of $\mathscr{G}$ in $\mathrm{GL}_n(\mathbb{C})$**

Use common algorithms to compute (algebraic) Galois groups (see for example [Sta73]) to compute $\phi(\mathscr{G})$ in $\mathrm{GL}_n(\mathbb{C})$.

**Remark.** *This algorithm was designed in a way that it is easy to replace individual parts. So for example more efficient Gröbner basis constructions can lower the bound $B_5(n)$ without influencing other parts of the algorithm.*
*Other factorization algorithms of differential operators can easily replace the presented methods here.*
*Also we tried to be as explicit as possible, where rational points were needed and what information about them has to be known.*

# Chapter 1

# Gröbner bases

The goal of the first two chapters is the proof of the following theorem.

**Theorem 1.1.** *For every $n \in \mathbb{N}$ there is a computable number $B_5(n)$ such that: For every closed subgroup $\mathscr{G} \subseteq \mathrm{GL}_n(\mathbb{F}_0)$ there exists closed subgroup $\mathscr{M} \subseteq \mathrm{GL}_n(\mathbb{F}_0)$ with $\mathscr{M}^u \subseteq \mathscr{G}^\circ \subseteq \mathscr{G} \subseteq \mathscr{M}$ and the defining ideal of $\mathscr{M}$ is generated by polynomials of degree less than or equal to $B_5(n)$.*

Here $\mathscr{M}^u$ is the subgroup generated by unipotent elements.
The existence of such a bound first appeared in [Hru02, Corollary 3.7]. We will develop a new proof , which allows to compute the bound $B_5(n)$ explicitly (see Corollary 2.37). In contrast to Hrushovski's proof, which is in terms of model theory, we will give a constructive proof.

## 1.1 Definitions and Notations

This section is merely a brief summary of the necessary Gröbner basis techniques we will use later on. Most of its definitions are taken from [CLO07].
By $\mathbb{N}_0$ we will always mean $\mathbb{N} \cup \{0\}$ whereas $\mathbb{N}$ denotes the naturals numbers not containing 0. Let $\mathbb{F}_0$ be any field and denote by $\mathbb{F}_0[x]$ the polynomial ring $\mathbb{F}_0[x_1, \ldots, x_n]$ for some fixed $n \in \mathbb{N}$. For any $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{N}_0)^n$ we write

$$x^\alpha := \prod_{i=1}^{n} x_i^{\alpha_i} \ .$$

**Definition 1.2.** *Let $S$ be a set. A* total ordering *on $S$ is a relation $\leq$ such that the following properties hold for all $\alpha, \beta, \gamma \in S$:*

- *If $\alpha \leq \beta$ and $\beta \leq \alpha$ then $\alpha = \beta$.*
- *If $\alpha \leq \beta$ and $\beta \leq \gamma$ then $\alpha \leq \gamma$.*
- *$\alpha \leq \beta$ or $\beta \leq \alpha$.*

*The total ordering $\leq$ on $S$ is a* well-ordering *if and only if*

$$\forall\, T \subseteq S\ \exists\, \alpha \in T\ \forall\, \beta \in T\colon\ \alpha \leq \beta \ .$$

**Definition 1.3.** *Let $\leq$ denote a well-ordering on $(\mathbb{N}_0)^n$ with the additional property:*

$$\forall \alpha, \beta, \gamma \in (\mathbb{N}_0)^n : \alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma.$$

*This induces a total ordering on $\mathbb{F}_0[x_1, \ldots, x_n]$:*

$$x^\alpha \leq x^\beta :\Leftrightarrow \alpha \leq \beta \qquad \text{for } \alpha, \beta \in (\mathbb{N}_0)^n.$$

*A total ordering on $\mathbb{F}_0[x]$ arising this way from a total ordering on $(\mathbb{N}_0)^n$ will be called a* monomial ordering *on $\mathbb{F}_0[x]$.*
*For a fixed monomial ordering define the* multidegree multidegree$(f)$, leading monomial $\mathrm{LM}(f)$, *the* leading coefficient $\mathrm{LC}(f)$ *and the* leading term $\mathrm{LT}(f)$ *of $f = \sum_\alpha p_\alpha x^\alpha \in \mathbb{F}_0[x]$ with $p_\alpha \in \mathbb{F}_0$ as*

$$\begin{aligned} \text{multidegree}(f) &:= \max\{\alpha \in (\mathbb{N}_0)^n \mid p_\alpha \neq 0\}, \\ \mathrm{LM}(f) &:= x^{\text{multidegree}(f)}, \\ \mathrm{LC}(f) &:= p_{\text{multidegree}(f)}, \\ \mathrm{LT}(f) &:= \mathrm{LC}(f) \cdot \mathrm{LM}(f) \ . \end{aligned}$$

**Definition 1.4 (and Example).** *The* lexicographic order $\leq_{\text{lex}}$ *is the total ordering on $(\mathbb{N}_0)^n$ defined via $\beta \leq_{\text{lex}} \alpha$ if and only if the left-most nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is positive.*

**Definition 1.5 (and Example).** *The* graded lexicographic order $\leq_{\text{grlex}}$ *is the total ordering on $(\mathbb{N}_0)^n$ defined via*

$$\beta \leq_{\text{grlex}} \alpha \Leftrightarrow \sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i \text{ or } \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ and } \beta \leq_{\text{lex}} \alpha$$

*for any $\alpha = (\alpha_1, \ldots, \alpha_n),\ \beta = (\beta_1, \ldots, \beta_n) \in (\mathbb{N}_0)^n$. The multidegree with respect to $\leq_{\text{grlex}}$ of $f \in \mathbb{F}_0[x]$ is called* total degree of $f$ *and will always be denoted as* $\deg(f)$.

**Definition 1.6.** *The monomials in the variables $\{x_1, \ldots, x_n\}$ of total degree less than or equal to $d$ will be denoted by*

$$\mathrm{Mon}(n, d) := \left\{ x^\alpha \;\middle|\; \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n,\ \sum_{i=1}^n \alpha_i \leq d \right\}.$$

*Similarly we define the polynomials in the variables $\{x_1, \ldots, x_n\}$ of total degree less than or equal to $d$ by $\mathbb{F}_0[x]_{\leq d}$.*

**Theorem 1.7.** *[CLO07, Chap2. §3, Theorem 3] Given any monomial ordering $\leq$ on $(\mathbb{N}_0)^n$ and $G := \{f_1, \ldots, f_s\} \subseteq \mathbb{F}_0[x]$ with $f_{i+1} \leq f_i$ for $i = 1, \ldots, s-1$. Any $f \in \mathbb{F}_0[x]$ can be written as*

$$f = r + \sum_{i=1}^s a_i f_i$$

*with $a_i, r \in \mathbb{F}_0[x]$ for $i = 1, \ldots, n$ such that the* remainder $\mathrm{N}(f, G) := r$ *does not contain a monomial divisible by $\mathrm{LT}(f_i)$ for $i = 1, \ldots, n$. We also call $\mathrm{N}(f, G)$ the* normal form of $f$ with respect to $G$ .

The proof of this theorem relies on the *division algorithm*, which, using the notation of Theorem 1.7, goes as follows (this algorithm is taken from [CLO07, Chap2. §3, Proof of theorem 3]; note the typing error in line 9 there):

**Algorithm 1.8 (Division Algorithm).**
***Input:*** $f_s \leq f_{s-1} \ldots \leq f_1, f$
***Output:*** $a_1, \ldots, a_s, r$
***Instructions:***
$a_1 := 0, \ldots, a_s := 0, r := 0, p := f$
*While* $p \neq 0$ *do*
    $i := 1$
    divisionOccured := false
    *While* $i \leq s$ *and* divisionOccured = false *do*
        *If* $\mathrm{LT}(f_i)$ *divides* $\mathrm{LT}(p)$ *then*
            $a_i := a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$
            $p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i$
            divisionOccured := true
        *else*
            $i := i + 1$
    *If* divisionOccured = false *then*
        $r := r + \mathrm{LT}(p)$
        $p := p - \mathrm{LT}(p)$

**Example 1.9.** *Let $f = x_1^d$ be a polynomial in the polynomial ring $\mathbb{F}_0[x_1, x_2]$ (so $n = 2$) and consider the set $G = \{x_1 - x_2^m\}$ for fixed $m \in \mathbb{N}$. Then $\mathrm{N}(f, G) = x_2^{md}$, if one calculates the normal form with respect to the lexicographical order.*

**Remark 1.10.** *Since we will often have to bound the degree of polynomials, the behavior of some monomial orderings, as illustrated in the example, is rather unpleasant.*
*If $G$ is ordered with respect to the graded lexicographic order, then* $\deg(f) \geq N(f, G)$.

**Definition 1.11.** *Let $I$ be an ideal in $\mathbb{F}_0[x]$ and let $\leq$ be a monomial ordering. A subset $G := \{g_1, \ldots, g_r\} \subseteq \mathbb{F}_0[x]$ is called a* Gröbner basis *for $I$ if and only if*

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r) \rangle = \langle \mathrm{LT}(I) \rangle \ .$$

*Here $\langle M \rangle$ denotes the ideal generated by $M$ for any set $M \subseteq \mathbb{F}_0[x]$.*

Note that this implies $\langle g_1, \ldots, g_r \rangle = I$ (see [CLO07, Chapter 2, §5]). Gröbner bases are always with respect to a monomial ordering, which usually will be omitted.

**Remark 1.12.** *A constructive version of the proof of* Hilbert's Basis Theorem *shows that Gröbner bases exist (see for example [CLO07, Chapter 2, §5, Corollary 6]).*

The following bound of Dubé will turn out to be crucial for bounding the complexity of algorithms using Gröbner basis techniques:

**Theorem 1.13.** *[Dub90, Corollary 8.3] Let $I \subseteq \mathbb{F}_0[x]$ be any ideal generated by a finite set of polynomials of total degree less than or equal to $d$. For every monomial ordering, which satisfies $1 \leq x_i$ for $i = 1, \ldots, n$, there is a Gröbner basis for $I$ consisting of polynomials of total degree less than or equal to*

$$B_0(n, d) := 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}} \ .$$

## 1.2 Applications

In this section we present common techniques to compute constructions from algebraic geometry or to solve decision problems. Most subsections will contain two versions of the algorithms: The first version is usually the one found in most textbooks about Gröbner bases. The second version uses Dubé's bound (Theorem 1.13) to bound the degree of generators defining the occurring ideals.
Before we start we fix the following notation:

**Definition 1.14.** *Let $\mathbb{A}^n := \mathbb{A}^n(\mathbb{F}_0)$ denote the affine space over $\mathbb{F}_0$. We have the following functors:*

$$\begin{aligned}\mathcal{I}\colon \{U \text{ subset of } \mathbb{A}^n\} &\to \{I \text{ ideal in } \mathbb{F}_0[x]\}\\ U &\mapsto \mathcal{I}(U) := \{f \in \mathbb{F}_0[x] \mid f(u) = 0 \text{ for all } u \in U\}\\ \mathcal{V}\colon \{I \text{ ideal in } \mathbb{F}_0[x]\} &\to \{U \text{ subset of } \mathbb{A}^n\}\\ I &\mapsto \mathcal{V}(I) := \{v \in \mathbb{A}^n \mid f(v) = 0 \text{ for all } f \in I\}.\end{aligned}$$

*A subset $A \subseteq \mathbb{A}^n$ is called an* affine variety *if and only if $A = \mathcal{V}(I)$ for some Ideal $I$ in $\mathbb{F}_0[x]$.*[1]

### 1.2.1 Elimination

Elimination techniques are important as they serve to compute the radical of ideals, intersection of ideals or images of affine varieties.

**Definition 1.15.** *For any ideal $I \subseteq \mathbb{F}_0[x]$ and a subset $U \subseteq \{x_1, \ldots, x_n\}$ the ideal $I \cap \mathbb{F}_0[U]$ in $\mathbb{F}_0[U]$ is called the* elimination ideal *of $I$ with respect to $U$.*

The natural question arising is: 'How to compute elimination ideals?' With Gröbner bases this turns out to be very simple:

**Theorem 1.16.** *[BW93, Proposition 6.15]*
*Let $I$ be an ideal in $\mathbb{F}_0[x]$, $U \subseteq \{x_1, \ldots, x_n\}$ and $G$ a Gröbner basis for $I$ with respect to a monomial ordering $\leq$. If $\leq$ satisfies $u \leq \tilde{x}$ for every $\tilde{x} \in \{x_1, \ldots, x_n\} - U$ and $u \in U$ then $G \cap \mathbb{F}_0[U]$ is a Gröbner basis for $I \cap \mathbb{F}_0[U]$.*

### 1.2.2 Membership problem

The *(ideal) membership problem* is the following: Given an ideal $I = \langle f_1, \ldots, f_r\rangle \subseteq \mathbb{F}_0[x]$ and a polynomial $f \in \mathbb{F}_0[x]$, determine if $f \in I$.
The solution to this problem, with the aid of Gröbner bases, goes as follows:

**Theorem 1.17.** *[CLO07, Chap2. §6, Corollary 2] Let $G$ be a Gröbner basis for an ideal $I \subseteq \mathbb{F}_0[x]$. Then for $f \in \mathbb{F}_0[x]$ we have*

$$f \in I \Leftrightarrow \mathrm{N}(f, G) = 0\ .$$

Again let $I$ denote an ideal in the polynomial ring $\mathbb{F}_0[x]$. Given a number $d \in \mathbb{N}_0$ and a subset $\mathscr{A}$ of $\mathrm{Mon}(n, d)$. Let $h_1, \ldots, h_m$ be the distinct elements of $\mathscr{A}$.

[1] We neither require $A$ to be irreducible nor the ideal $I$ to be prime.

Associate to every $q = (q_1, \ldots, q_m) \in \mathbb{F}_0^m$ the polynomial

$$f_q(x_1, \ldots, x_n) \coloneqq \sum_{i=1}^{m} q_i h_i(x_1, \ldots, x_n) \ .$$

Consider the set

$$V_{\text{coeff}}(\mathscr{A}, I) \coloneqq \{q = (q_1, \ldots, q_m) \in \mathbb{F}_0^m \mid f_q(x_1, \ldots, x_n) \in I\} \, ,$$

it is the set of coefficients of certain polynomials of degree less than or equal to $d$, that lie in $I$.
By the Theorem 1.17 we have

$$V_{\text{coeff}}(\mathscr{A}, I) = \{q = (q_1, \ldots, q_m) \in \mathbb{F}_0^m \mid \mathrm{N}\,(f_q(x_1, \ldots, x_n), G) = 0\} \ .$$

**Corollary 1.18.** *For any $q \in \mathbb{F}_0^m$, any ideal $I \subseteq \mathbb{F}_0[x]$ and any $\mathscr{A} \subseteq \mathrm{Mon}(n, d)$ with $m = |\mathscr{A}|$ the set $V_{\text{coeff}}(\mathscr{A}, I)$ is an affine variety in $\mathbb{A}^m(\mathbb{F}_0)$. The corresponding defining ideal*

$$\mathcal{I}(V_{\text{coeff}}(\mathscr{A}, I)) =: I_{\text{coeff}}(\mathscr{A}, I) \subseteq \mathbb{F}_0[y_1, \ldots, y_m]$$

*is generated by a finite set of polynomials of degree 1.*

*Proof.* Let $\mathscr{A} = \{h_1, \ldots, h_m\}$ and $G = \{f_1, \ldots, f_s\}$ be a Gröbner basis for the ideal $I$. We will prove this corollary by applying Algorithm 1.8 to the polynomial

$$f_{(y_1,\ldots,y_m)}(x_1, \ldots, x_n) \coloneqq \sum_{i=1}^{m} y_i h_i \in \mathbb{F}_0[x_1, \ldots, x_n, y_1, \ldots, y_m]$$

to compute its normal form.
In the algorithm $p$ is initialized as $f_{(y_1,\ldots,y_m)}(x_1, \ldots, x_n)$, which is of total degree 1 in the variables $y_1, \ldots, y_m$. For $i \in \{1, \ldots, s\}$ the step

$$p \coloneqq p - \underbrace{\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}}_{\coloneqq k} f_i$$

alters $p$ by subtraction of the product of $k$ and $f_i$. Since $f_i \in G \subseteq \mathbb{F}_0[x_1, \ldots, x_n]$, its total degree in $y_1, \ldots, y_m$ is zero. The degree in $y_1, \ldots, y_m$ of $k$ is bounded by the degree in $y_1, \ldots, y_m$ of $p$, which is 1 by induction assumption.
Since $p$ is of degree 1 in $y_1, \ldots, y_m$ in every step, the normal form is of degree 1 in $y_1, \ldots, y_m$.□

**Example 1.19.** *Set $n = 2$ and $\mathscr{A} = \mathrm{Mon}(2, 3)$, thus we have*

$$\begin{aligned} f_{(q_1,\ldots,q_{10})}(x_1, x_2) =& q_1 x_1^3 + q_2 x_1^2 x_2 + q_3 x_1^2 + q_4 x_1 x_2^2 + q_5 x_1 x_2 \\ &+ q_6 x_1 + q_7 x_2^3 + q_8 x_2^2 + q_9 x_2 + q_{10} 1 \ . \end{aligned}$$

*Consider the ideal $I = \langle x_1^2 - x_2 \rangle \subseteq \mathbb{F}_0[x_1, x_2]$. Fixing the lexicographical order, meaning that*

$$x_1^3 \geq x_1^2 x_2 \geq x_1^2 \geq x_1 x_2^2 \geq x_1 x_2 \geq x_1 \geq x_2^3 \geq x_2^2 \geq x_2 \geq 1$$

*and using the Algorithm 1.8 we can compute $I_{\text{coeff}} \subseteq \mathbb{F}_0[y_1, \ldots, y_{10}]$:*

$$\begin{aligned} I_{\text{coeff}} =& \mathcal{I}\left(\left\{q = (q_1, \ldots, q_{10}) \;\middle|\; \mathrm{N}\left(f_q(x_1, x_2), \{x_1^2 - x_2\}\right) = 0\right\}\right) \\ =& \langle y_1 + y_5, \ y_2 + y_8, \ y_3 + y_9 \rangle \end{aligned}$$

*This means that elements in $I$ of degree less than or equal to 3 are of the form*

$$a(x_1^3 - x_1 x_2) + b(x_1^2 x_2 - x_2^2) + c(x_1^2 - x_2) \text{ for } a, b, c \in \mathbb{F}_0 \ .$$

### 1.2.3 Image of a morphism

**Theorem 1.20.** *[VGS+97, Proposition 2.1.3] Let $\varphi : V \to W$ be a morphism of algebraic varieties with corresponding ideals $\mathcal{I}(V) \subseteq \mathbb{F}_0[x_1, \ldots, x_n]$ and $\mathcal{I}(W) \subseteq \mathbb{F}_0[z_1, \ldots, z_m]$. Then*

$$\mathcal{I}\left(\overline{\varphi(V)}\right) = \langle \mathcal{I}(V) + \langle z_i - \varphi_i(x_1, \ldots, x_n) \mid i = 1, \ldots, m \rangle \rangle \cap \mathbb{F}_0[z_1, \ldots, z_m]$$

*with $\overline{\varphi(V)}$ the (Zariski) closure of $\varphi(V)$.*

**Corollary 1.21.** *Under the assumptions of Theorem 1.20, if $\mathcal{I}(V)$ is generated by a finitely many polynomials of total degree less than or equal to $d$, then the ideal $\overline{\mathcal{I}(\varphi(V))}$ has a Gröbner basis of degree less than or equal to $B_0(n+m, e)$ with*

$$e = \max\left\{\deg\left(\varphi_1(x_1, \ldots, x_n)\right), \ldots, \deg\left(\varphi_m(x_1, \ldots, x_n)\right), d\right\} \ .$$

*Proof.* Define $e$ as the highest degree in $x_1, \ldots, x_n$ of all occurring generators in

$$J := \langle \mathcal{I}(V) + \langle z_i - \varphi_i(x_1, \ldots, x_n) \mid i = 1, \ldots, m \rangle \rangle \ .$$

By Theorem 1.13 a Gröbner basis $G$ for $J$ is of degree less than or equal to $B_0(n+m, e)$. Since a Gröbner basis $G'$ for the elimination ideal $J \cap \mathbb{F}_0[z_1, \ldots, z_m]$ can be obtained from $G$ by omitting those elements, which do not lie in $\mathbb{F}_0[x_1, \ldots, x_n]$ (see Theorem 1.16), the same bound applies to $G'$. □

### 1.2.4 Intersection of ideals

**Theorem 1.22.** *[BW93, Proposition 6.19] Let $I_1, \ldots, I_r$ be ideals in $\mathbb{F}_0[x_1, \ldots, x_n]$. Define*

$$J := \left\langle y_1 I_1, \ldots, \ y_r I_r, \ 1 - \sum_{i=1}^{r} y_i \right\rangle \subseteq \mathbb{F}_0[x_1, \ldots, x_n, y_1, \ldots, y_r]$$

*then $\bigcap_{i=1}^{r} I_i = J \cap \mathbb{F}_0[x_1, \ldots, x_n]$.*

**Corollary 1.23.** *Under the assumptions of Theorem 1.22, let $I_i$ be generated by a finite set of polynomials of total degree less than or equal to $d_i$ for $i = 1, \ldots, r$ and $d = \max\{d_i \mid i = 1, \ldots, r\}$. The ideal $J \cap \mathbb{F}_0[x] = \cap_{i=1}^{r} I_i$ has a Gröbner basis of degree less than or equal to $B_0(n+r, d+1)$.*

*Proof.* The ideal $J \subseteq \mathbb{F}_0[y_1, \ldots, y_r, x_1, \ldots, x_n]$ is generated by polynomials of degree less than or equal to $d+1$. As in the proof of Theorem 1.20 a Gröbner basis for $J$ yields a Gröbner basis for $J \cap \mathbb{F}_0[x]$. □

### 1.2.5 Primary Decomposition of Ideals

The following theorem is well-known. For example it follows from [AM69, p.51-52] and [Har77, Chapter I, Corollary 1.6].

**Theorem 1.24.** *Let $\mathfrak{R}$ be a Noetherian ring. Any ideal $\mathfrak{i}$ in $\mathfrak{R}$ can be written as*

$$\mathfrak{i} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$$

*such that $\mathfrak{q}_1 \ldots, \mathfrak{q}_s$ are primary ideals in $\mathfrak{R}$, the* associated prime ideals *$\sqrt{\mathfrak{q}_k}$ are distinct and for every $k = 1, \ldots, s$ we have*

$$\bigcap_{\substack{j=1 \\ j \neq k}}^{s} \mathfrak{q}_j \neq \mathfrak{i} \ .$$

*We call such a decomposition of $\mathfrak{i}$ the* minimal primary decomposition.

There are several algorithms to compute primary decompositions. Most of them are implemented in common computer algebra systems, such as *Maple* or *Singular*. For an overview of these algorithms consult [DGP99].

**Remark 1.25.** *If* $\mathfrak{R} = \mathbb{F}_0[X]$ *then there are algorithms, using Gröbner bases, to compute a minimal primary decomposition for any ideal* $\mathfrak{i} \subseteq \mathfrak{R}$.

# Chapter 2

# Families of Bounded Type

In this chapter we will compute bounds for various objects occuring naturally in the language of algebraic varieties and algebraic groups. We will assume the field $\mathbb{F}_0$ to be algebraically closed and of characteristic 0.
The goal is to prove Theorem 1.1 and in particular to compute the bound $B_5(n)$.

## 2.1 Bound Definable Ideals and $\mathrm{GL}_n(\mathbb{F}_0)$

**Action of $\mathrm{GL}_n(\mathbb{F}_0)$ via multiplication**

We will fix the following left action of $\mathrm{GL}_n(\mathbb{F}_0)$ on $\mathbb{A}^{k\times n}$:

$$\begin{aligned} r\colon \mathrm{GL}_n(\mathbb{F}_0)\times \mathbb{A}^{k\times n} &\to \mathbb{A}^{k\times n}\\ (g,u) &\mapsto u\cdot g^{-1} \end{aligned}$$

where $u\cdot g^{-1}$ denotes the usual matrix multiplication of the $k\times n$ matrix $u$ with the $n\times n$ matrix $g^{-1}$. On the coordinate ring $R := \mathbb{F}_0[x_{1,1},\dots,x_{k,n}]$ we obtain another left action

$$\begin{aligned} \rho\colon \mathrm{GL}_n(\mathbb{F}_0)\times R &\to R\\ (g, f(X_{k,n})) &\mapsto f(X_{k,n}\cdot g) \end{aligned}$$

Here $X_{k,n}$ denotes the variables $x_{1,1},\dots,x_{k,n}$ conveniently arranged in the matrix

$$X_{k,n} = \begin{pmatrix} x_{1,1} & \dots & x_{1,n}\\ \vdots & \ddots & \vdots\\ x_{k,1} & \dots & x_{k,n} \end{pmatrix}$$

and $X_{k,n}\cdot g$ just denotes the usual matrix product. If $k=n$ we will often write just $X$ instead of $X_{n,n}$.

**Example 2.1.** *Let $n=2$ and $k=3$ and take $g=\begin{pmatrix}1&2\\1&0\end{pmatrix}\in \mathrm{GL}_2(\mathbb{Q})$. Then for any $f(x_{1,1},\dots,x_{3,2})$ we have:*

$$\rho\left(\begin{pmatrix}1&2\\1&0\end{pmatrix}, f\begin{pmatrix}x_{1,1}&x_{1,2}\\x_{2,1}&x_{2,2}\\x_{3,1}&x_{3,2}\end{pmatrix}\right) = f\begin{pmatrix}x_{1,1}+x_{1,2}&2x_{1,1}\\x_{2,1}+x_{2,2}&2x_{2,1}\\x_{3,1}+x_{3,2}&2x_{3,1}\end{pmatrix}.$$

For any $g \in \mathrm{GL}_n(\mathbb{F}_0)$ the two actions induce morphisms $r_g := r(g,-)$ and $\rho_g := \rho(g,-)$. The reason for these unusual actions comes from the representation of the differential Galois groups in some $\mathrm{GL}_n(\mathbb{F}_0)$ as discussed in Proposition 3.18 below.
These two actions $r$ and $\rho$ are compatible:

**Lemma 2.2.** *Let $U \subseteq \mathbb{A}^{k\times n}$ be an affine variety and $g \in \mathrm{GL}_n(\mathbb{F}_0)$. Then we have*

$$\rho_g \mathcal{I}(U) = \mathcal{I}(r_g U)$$

*Proof.*

$$\begin{aligned}
\rho_g \mathcal{I}(U) &= \rho_g \{ f(X_{k,n}) \in R \mid \forall u \in U\colon\ f(u) = 0 \} \\
&= \{ f(X_{k,n} \cdot g) \mid f(X_{k,n}) \in R, \forall u \in U\colon\ f(u) = 0 \} \\
&= \left\{ f(X_{k,n}) \in R \;\middle|\; \forall u \in U\colon\ f(u \cdot g^{-1}) = 0 \right\} \\
&= \left\{ f(X_{k,n}) \in R \;\middle|\; \forall u \in U \cdot g^{-1}\colon\ f(u) = 0 \right\} \\
&= \mathcal{I}(U g^{-1}) = \mathcal{I}(r_g U).
\end{aligned}$$

□

### Action of $\mathrm{GL}_n(\mathbb{F}_0)$ via conjugation

Occasionally we will also let $\mathrm{GL}_n(\mathbb{F}_0)$ act via conjugation. As above we have the two left actions:

$$\begin{aligned}
c\colon \mathrm{GL}_n(\mathbb{F}_0) \times \mathbb{A}^{n^2} &\to \mathbb{A}^{n^2} \\
(g, A) &\mapsto g A g^{-1} \\
\gamma\colon \mathrm{GL}_n(\mathbb{F}_0) \times \mathbb{F}_0[X] &\to \mathbb{F}_0[X] \\
(g, f(X)) &\mapsto f(g^{-1} X g)
\end{aligned}$$

For fixed $g \in \mathrm{GL}_n(\mathbb{F}_0)$ both actions induce maps $c_g := c(g,-)\colon \mathbb{A}^{n^2} \to \mathbb{A}^{n^2}$ and $\gamma_g := \gamma(g,-)\colon \mathbb{F}_0[X] \to \mathbb{F}_0[X]$. As above we have the following compatibility:

**Lemma 2.3.** *For any affine variety $U \subseteq \mathbb{A}^{n^2}$ and any $g \in \mathrm{GL}_n(\mathbb{F}_0)$ we have:*

$$\gamma_g \mathcal{I}(U) = \mathcal{I}(c_g U)$$

*Proof.* As the proof of Lemma 2.2. □

### Bound Definable Ideals

Often we will need to consider ideals of algebraic subgroups of $\mathrm{GL}_n(\mathbb{F}_0)$. Identify the coordinate ring of $\mathbb{A}^{n^2+1}$ with $\mathbb{F}_0[X,t]$ where $X := X_{n,n}$ and $t$ is an extra variable.

**Remark 2.4.** *All ideals occurring will always be understood to lie in free polynomial rings, unless otherwise stated. So for example if we write "$\mathcal{I}(\mathscr{G})$" for an algebraic subgroup $\mathscr{G}$ of $\mathrm{GL}_n(\mathbb{F}_0)$ we mean the defining ideal of $\mathscr{G}$ in the polynomial ring with $n^2+1$ variables $\mathbb{F}_0[X,t]$. This is in coherence with Definition 1.14 and necessary to have a well-defined notion of "degree of a polynomial" (see the following definition).*

The subvariety $\mathrm{GL}_n(\mathbb{F}_0)$ is then given via $\langle \det(X)t - 1 \rangle$. Sometimes we will need a second copy of $\mathbb{F}_0[X,t]$. We will denote this copy by $\mathbb{F}_0[Z,s]$, where $Z$ is a $n \times n$ matrix with indeterminantes $z_{1,1}, \ldots, z_{n,n}$ as entries.
To measure the complexity of occurring varieties the following definition will become helpful:

**Definition 2.5.** *Let $d$ be any natural number.*

*1a) An ideal $I \leq \mathbb{F}_0[X_{k,n}]$ is called* $d$-bound definable *if and only if $I$ is generated by a finite set of polynomials each of total degree less than or equal to $d$.*

*1b) An affine variety $U \subseteq \mathbb{A}^n$ is called $d$-bound definable if and only if $\mathcal{I}(U)$ is $d$-bound definable.*

*2a) An ideal $I \leq \mathbb{F}_0[X,t]$ is called* $d$-bound $\mathrm{GL}_n$-definable *if and only if there exists an ideal $I' \leq \mathbb{F}_0[X]$ such that $I = \langle I',\ \det(X)t-1\rangle \leq \mathbb{F}_0[X,t]$ and $I'$ is $d$-bound definable. We call $I'$ the* determinant-free form of $I$.

*2b) An affine variety $U \subseteq \mathrm{GL}_n(\mathbb{F}_0)$ is called $d$-bound $\mathrm{GL}_n$-definable if and only if $\mathcal{I}(U)$ is $d$-bound $\mathrm{GL}_n$-definable.*

**Proposition 2.6.** *Any $d$-bound definable affine variety $\mathscr{U} \subseteq \mathrm{GL}_n(\mathbb{F}_0)$ is $(n+1)d$-bound $\mathrm{GL}_n$-definable.*

*Proof.* Let $\mathcal{I}(\mathscr{U})$ be generated by $q_\alpha(X,t) \in \mathbb{F}_0[X,t]$ of degree less than or equal to $d$ for all $\alpha$ in some finite index set $\mathscr{A}$. Define $f(X,t) = \det(X)t - 1$ and note that it is a polynomial of degree $n+1$. Now for every $\alpha \in \mathscr{A}$ let $p_\alpha(X) \in \mathbb{F}_0[X]$ be the polynomial of degree $(n+1)d$ one obtains from $\det(X)^d q_\alpha(X,t)$ be replacing every occurrence of $\det(X)t$ by 1. Since

$$(\det(X)t)^k = (f(X,t)+1)^k = \sum_{j=0}^{k} \binom{k}{j} f(X,t)^{k-j}$$

this can be done by subtracting suitable $\mathbb{F}_0[X]$-multiplies of $f(X,t)$. The identity $\mathcal{I}(\mathscr{U}) = \langle p_\alpha(X),\ f(X,t) \mid \alpha \in \mathscr{A}\rangle$ follows. □

**Definition 2.7.** *Let $A \subseteq \mathbb{A}^n$ and $B \subseteq \mathbb{A}^m$ be two arbitrary affine varieties. A* morphism *$f\colon X \to Y$ is a mapping of the form*

$$f(\underbrace{a_1,\ldots,a_n}_{=a}) = (f_1(a),\ldots,f_m(a))$$

*with $f_i(a) \in \mathbb{F}_0[A] = \mathbb{F}_0[x_1,\ldots,x_n]/\mathcal{I}(A)$.*
*We say that $f$* is of degree *$d$ if and only if for $i = 1,\ldots,m$ there is $g_i \in \mathbb{F}_0[x_1,\ldots,x_n]$ of degree less than or equal to $d$ so that $g_i$ equals $f_i$ modulo $\mathcal{I}(A)$.*

## 2.2 Effective Version of a Theorem of Chevalley

For every closed normal subgroup $\mathscr{N}$ of an algebraic group $\mathscr{G} \leq \mathrm{GL}_n(\mathbb{F}_0)$ there is a rational representation with kernel equal to $\mathscr{N}$ (this is due to Chevalley). The goal of this section is to bound the degree and dimension of this representation.
We will achieve this by closely following the presentation in [Hum75] and computing bounds for all necessary steps, which lead to the proof of Chevalley's theorem.

This lemma is essentially a more technical restatement of [Hum75, Proposition 8.6.(a)]:

**Lemma 2.8.** *Let $\mathscr{G}$ be a closed subgroup of $\mathrm{GL}_n(\mathbb{F}_0)$. For any $f_1,\ldots,f_r \in \mathbb{F}_0[X]$ each of degree less or equal to $d \in \mathbb{N}$ there exists a finite-dimensional $\mathscr{G}$-stable subspace $W \subseteq \mathbb{F}_0[X]$ spanned by polynomials of degree less than or equal to $d$ with*

$$\mathrm{span}_{\mathbb{F}_0}\{f_1,\ldots,f_r\} \subseteq W \subseteq \mathbb{F}_0[X]\ .$$

*Furthermore the dimension of $W$ can be bounded:*

$$\dim_{\mathbb{F}_0}(W) \leq M_1(n^2, d) := \sum_{i=0}^{d} \binom{n^2+i-1}{i} = \sum_{i=0}^{d} \prod_{k=0}^{i} \frac{n^2+k-1}{k} \in \mathcal{O}\big((n^2)^d\big).$$

*Here $M_1(n,d)$ is the number of all monomials of degree less or equal to $d$ in $n^2$ variables.*

*Proof.* For $i = 1, \ldots, r$ we can rewrite

$$f_i(X \cdot Z) = \sum_{\alpha \in \mathscr{M}} p_{i,\alpha}(Z) X^\alpha$$

with $p_{i,\alpha}(Z) \in \mathbb{F}_0[Z]$ and $\mathscr{M}$ the set of all tuples $(a_1, \ldots, a_{n^2})$ in $\mathbb{N}_0^{n^2}$ with $\sum_{i=1}^{n^2} a_i \leq d$. Let $G$ be a Gröbner basis of the determinant-free form of $\mathcal{I}(\mathscr{G})$ in $\mathbb{F}_0[Z, s]$ with respect to some monomial ordering that satisfies $s > Z_{i,j}$ for all $i, j \in \{1, \ldots, n\}$.

$$W := \{X^\alpha \mid \alpha \in \mathscr{M}, \exists i \in \{1, \ldots, r\} \colon \ \mathrm{N}(p_{i,\alpha}(Z), G) \neq 0\}.$$

By construction $W$ is spanned by monomials of degree less than or equal to $d$.
For any $g \in \mathscr{G}$ and $X^\alpha \in W$ we can compare $\rho_g f(X \cdot Z) = \sum_\alpha p_{i,\alpha}(Z)(X \cdot g)^\alpha$ and $\rho_g f(X \cdot Z) = f(X \cdot g \cdot Z) = \sum_\alpha p_{i,\alpha}(g \cdot Z) X^\alpha$. Now substituting $Z$ with the identity matrix shows that we can rewrite $(X \cdot g)^\alpha$ as $\mathbb{F}_0$-linear combination of other elements in $W$. Hence $W$ is $\mathscr{G}$-stable. □

**Example 2.9.** *Take* $\mathscr{H} = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \mid \lambda \in \mathbb{F}_0 \right\} \leq \mathrm{GL}_2(\mathbb{F}_0)$. *The defining ideal of $\mathscr{H}$ is given by*

$$\langle f_1(X) = x_{1,2},\ f_2(X) = x_{2,1},\ f_3(X) = x_{1,1}x_{2,2} - 1 \rangle\ .$$

*Now we compute (as in the proof of Lemma 2.8) a finite-dimensional subspace $W \leq \mathbb{F}_0[X]$ containing $f_1, f_2$ and $f_3$, which is $\mathrm{GL}_2(\mathbb{F}_0)$-stable.*

$$X \cdot Z = \begin{pmatrix} x_{1,1}z_{1,1} + x_{1,2}z_{2,1} & x_{1,1}z_{1,2} + x_{1,2}z_{2,2} \\ x_{2,1}z_{1,1} + x_{2,2}z_{2,1} & x_{2,1}z_{1,2} + x_{2,2}z_{2,2} \end{pmatrix}$$

$$\begin{aligned} f_1(X \cdot Z) &= x_{1,1}z_{1,2} + x_{1,2}z_{2,2} \\ f_2(X \cdot Z) &= x_{2,1}z_{1,1} + x_{2,2}z_{2,1} \\ f_3(X \cdot Z) &= z_{1,1}z_{12}x_{1,1}x_{2,1} + z_{1,1}z_{2,2}x_{1,1}x_{2,2} + z_{2,1}z_{1,2}x_{1,2}x_{2,1} + z_{1,2}z_{2,2}x_{1,2}x_{2,2} - 1 \end{aligned}$$

*So $W = \mathrm{span}_{\mathbb{F}_0}(1,\ x_{1,1},\ x_{1,2},\ x_{2,1},\ x_{2,2},\ x_{1,1}x_{2,1},\ x_{1,1}x_{2,2},\ x_{1,2}x_{2,1},\ x_{1,2}x_{2,2})$ is $\mathrm{GL}_2(\mathbb{F}_0)$-stable and generated by $9 \leq 15 = M_1(2,2)$ elements.*

**Example 2.10.** *Let $\mathscr{H}$ be the group of upper triangle matrices with ones on the diagonal. Thus $\mathcal{I}(\mathscr{H}) = \langle x_{i,i} - 1,\ x_{i,j} \mid i = 1, \ldots, n, j < i \rangle$. Again we want to find a $\mathrm{GL}_n(\mathbb{F}_0)$-stable subspace of $\mathbb{F}_0[X]$ containing the chosen generators of $\mathcal{I}(\mathscr{H})$. For any $i, j \in \{1, \ldots, n\}$ we have*

$$(x_{i,j} - 1)(X \cdot Z) = \sum_{k=1}^{n} x_{i,k} z_{k,j}\ .$$

*Therefore $W$ is the $\mathbb{F}_0$-spann of $\{1,\ x_{i,j} \mid\ i, j \in \{1, \ldots, n\}\}$.*

This is a restatement of [Hum75, Lemma 11.1] adjusted to our settings. Its proof is a slight variation of the proof stated there.

**Lemma 2.11.** *Let $g \in \mathrm{GL}_n(\mathbb{F}_0)$, $M$ an $m$-dimensional subspace of $\mathbb{F}_0[X]$ and set $L = \bigwedge^m M$. Then we have $(\wedge^m g)L = L$ if and only if $\rho_g M = M$.*
*Here $(\wedge^m \rho_g)(l_1 \wedge \ldots \wedge l_m) = (\rho_g l_1 \wedge \ldots \wedge \rho_g l_m)$.*

**Theorem 2.12.** *[Hum75, Chapter 11.2, Theorem] Let $\mathscr{H}$ and $\mathscr{G}$ be closed subgroups of $\mathrm{GL}_n(\mathbb{F}_0)$ with $\mathscr{H} \subseteq \mathscr{G}$ and $\mathscr{H}$ be $d$-bound $\mathrm{GL}_n$-definable. Then there exists an $\mathbb{F}_0$-vector space $V$, a 1-dimensional subspace $L \subseteq V$ and a rational representation $\varphi : \mathscr{G} \to \mathrm{GL}(V)$ such that:*

$$\mathscr{H} = \{ g \in \mathscr{G} \mid \varphi(g)(L) = L \}.$$

*Furthermore the dimension of $V$ can be bound by $M_2(n,d) := \binom{M_1(n^2,d)}{\lfloor \frac{M_1(n^2,d)}{2} \rfloor}$ and $\varphi(g)_{i,j}$ is a polynomial of degree less than or equal to $d \cdot M_2(n,d)$ for all $i,j \in \{1,\ldots,\dim_{\mathbb{F}}(V)\}$ and $g \in \mathscr{G}$.*

*Proof.* Let $I$ be the determinant-free form of $\mathcal{I}(\mathscr{H})$ and suppose $I$ is generated by $\{f_1,\ldots,f_r\}$ in $\mathbb{F}_0[X]$ with $\deg(f_i) \leq d$ for $i = 1,\ldots,r$. Find a linear subspace $W \subseteq \mathbb{F}_0[X]$ according to Lemma 2.8 such that $W$ is $\mathscr{G}$-stable, spanned by polynomials of degree less than or equal to $d$ and

$$\mathrm{span}_{\mathbb{F}_0}\{f_1,\ldots,f_r\} \subseteq W .$$

Set $M := W \cap I$ then $M$ is $\mathscr{H}$-stable and generates $I$.
If for any $g \in \mathscr{G}$ we have $\rho_g M = M$, then

$$\begin{aligned} \rho_g I &= \rho_g\big(M \cdot \mathbb{F}_0[X]\big) \\ &= \rho_g M \cdot \rho_g\big(\mathbb{F}_0[X]\big) \\ &= M \cdot \mathbb{F}_0[X] \\ &= I . \end{aligned}$$

With [Hum75, Chapter 8.5, Lemma] we conclude $g \in \mathscr{H}$.
This shows $\mathscr{H} = \{ g \in \mathscr{G} \mid \rho_g M = M \}$. Now define

$$\begin{aligned} m &:= \dim_{\mathbb{F}} M, \\ L &:= \bigwedge^m M, \\ V &:= \bigwedge^m W, \\ \varphi &:= \bigwedge^m \rho : \mathscr{G} \to \mathrm{GL}(V) \\ &\quad g \mapsto \big((w_1 \wedge \ldots \wedge w_m) \mapsto (\rho_g w_1 \wedge \ldots \wedge \rho_g w_m)\big), \end{aligned}$$

then $L$ is 1-dimensional and the characterization of $\mathscr{H}$ follows from $\rho_g M = M$ and Lemma 2.11. The bound on the dimension of $V$ follows from the bound in Lemma 2.8 and the fact that for a fixed number $a$ the value of $\binom{2a}{b}$ is maximal if $a = b$. The bound on the degree of $\varphi$ comes from

$$\begin{aligned} &\varphi(g)(w_1 \wedge w_2 \wedge \ldots \wedge w_m)(x_{1,1},\ldots,x_{n,n}) \\ &\qquad = w_1((x_{1,1},\ldots,x_{n,n}) \cdot g) \wedge \ldots \wedge w_m((x_{1,1},\ldots,x_{n,n}) \cdot g) \end{aligned}$$

for $w_1, \dots, w_m$ some $\mathbb{F}_0$-linear combination of the generators of $W$, which by construction have degree less than or equal to $d$. □

**Definition 2.13.** *The* character group $X(\mathscr{G})$ *of* $\mathscr{G}$ *is defined as the group of all morphisms of algebraic groups* $\chi\colon \mathscr{G} \to \mathbb{F}_0^\times$. *The elements* $\chi$ *of* $X(\mathscr{G})$ *are called* characters of $\mathscr{G}$.

**Theorem 2.14.** *[Hum75, Chapter 11.5, Theorem] Let* $\mathscr{N} \leq \mathscr{G}$ *be closed subgroups of* $\mathrm{GL}_n(\mathbb{F}_0)$ *such that* $\mathscr{N}$ *is* $d$*-bound* $\mathrm{GL}_n$*-definable and normal in* $\mathscr{G}$. *Then there is a* $\mathbb{F}_0$*-vector space* $W_0$ *and a rational representation* $\psi : \mathscr{G} \to \mathrm{GL}(W_0)$ *with* $\ker(\psi) = \mathscr{N}$. *Furthermore* $\dim_{\mathbb{F}_0}(W_0)$ *is bound by* $M_2(n,d)^2$ *and* $\psi(X,t)_{i,j}$ *is a polynomial in* $\mathbb{F}_0[X,t]$ *of degree less than or equal to*

$$(n+1)\cdot d \cdot M_2(n,d) \text{ for all } i,j \in \{1,\dots,\dim_{\mathbb{F}_0}(W_0)\}\ .$$

*Proof.* By Theorem 2.12 there is a representation $\varphi : \mathscr{G} \to \mathrm{GL}(V)$ and a 1-dimensional subspace $L \subseteq V$ such that $\mathscr{N} = \{g \in \mathscr{G} \mid \varphi(g)L = L\}$. The action of $\mathscr{N}$ via $\varphi$ on $L$ is scalar multiplication and therefore yields a character $\chi_0 \in X(\mathscr{N})$ with $\varphi(n)(l) = \chi_0(n)l$ for all $l \in L$.
For any character define $V_\chi \coloneqq \{v \in V \mid \varphi(n)v = \chi(n)v \text{ for all } n \in \mathscr{N}\}$ and observe that

$$V \supseteq \bigoplus_{\chi \in X(\mathscr{N})} V_\chi \supseteq V_{\chi_0} \supseteq L$$

(the sum is direct, see e.g. [Hum75, Chapter 11.4, Lemma].) Let $\chi \in X(\mathscr{N}), v \in V_\chi, g \in \mathscr{G}$ and $n \in \mathscr{N}$, then the calculation

$$\begin{aligned}\varphi(n)\big(\varphi(g)(v)\big) = \varphi(gg^{-1}ng)(v) &= \varphi(g)\big(\varphi(\underbrace{g^{-1}ng}_{\in\mathscr{N}})v\big)\\ &= \varphi(g)\big(\chi(g^{-1}ng)v\big) = \chi(g^{-1}ng)\varphi(g)(v)\end{aligned}$$

shows that $\varphi(\mathscr{G})$ permutes the set $\{V_\chi \mid \chi \in X(\mathscr{N})\}$. By restriction $\varphi : \mathscr{G} \to \mathrm{GL}(\bigoplus V_\chi)$ we can without loss of generality assume that $V = \bigoplus_{\chi\in X(\mathscr{N})} V_\chi$. If we define

$$W_0 \coloneqq \{f \in \mathrm{End}_{\mathbb{F}_0}(V) \mid f(V_\chi) \subseteq V_\chi \text{ for all } \chi \in X(\mathscr{N})\}$$

then the desired map is given as

$$\begin{aligned}\psi : \mathscr{G} &\to \mathrm{GL}(W_0)\\ g &\mapsto \Big(f \mapsto \varphi(g)f\varphi(g)^{-1}\Big).\end{aligned}$$

For arbitrary $v \in V$ find $\chi \in X(\mathscr{N})$ with $v \in V_\chi$ and let $n \in \mathscr{N}$ then the calculation

$$\begin{aligned}\big(\psi(n)(f)\big)(v) &= \big(\varphi(n)\circ f\circ\varphi(n)^{-1}\big)(v)\\ &= (\varphi(n)\circ f)\,(\chi(n)^{-1}v)\\ &= \chi(n)^{-1}\cdot\varphi(n)(f(v))\\ (\text{ since } f(V_\chi)\subseteq V_\chi\ ) &= \chi(n)^{-1}\chi(n)f(v)\\ &= f(v)\end{aligned}$$

shows that the kernel of $\psi$ is $\mathscr{N}$. Since $\dim_{\mathbb{F}}(V) \leq M_2(n^2,d)$ and $W_0 \subseteq \mathrm{End}_{\mathbb{F}}(V)$ the first bound follows.
The inverse $g^{-1}$ is a polynomial of degree $n$ in the entries of $g$ and the inverse of its determinant. We plug this into $\varphi$, a polynomial of degree $d \cdot M_2(n,d)$ and obtain an expression of degree $n \cdot d \cdot M_2(n,d)$. Adding the degree of $\varphi$ gives the degree of $\psi$. □

## 2.3 Bound definable Families

Bound definable families are the components, which allow us to prove Theorem 1.1 and are bounded in some sense.
Hrushovski used the term "uniformly definable family" to describe in model-theoretic terms the components he required for the proof of his model-theoretic version of Theorem 1.1.
We will show in this and the following sections that most of Hrushovski's uniformly definable families have a compuatble bound in our sense.
Whenever we formulate a result that has a model-theoretic analog in [Hru02], we will give a reference.

**Definition 2.15.** *Let $d \in \mathbb{N}$. A set $\mathfrak{F}$ of affine varieties in $\mathbb{A}^{n^2+1}(\mathbb{F}_0)$ (or of ideals in $\mathbb{F}_0[X,t]$) is $d$-bound $\mathrm{GL}_n$-definable if and only if every element $\mathfrak{F}$ is a $d$-bound $\mathrm{GL}_n$-definable variety (or ideal).*

The following lemma has an analog in [Hru02, Lemma 3.1.a)] and [Hru02, Example 3.2.c-3)].

**Lemma 2.16.** *Let $\mathfrak{F}$ denote a set of subvarieties of $\mathbb{A}^{n^2+1}$.*

*(1) The set of maximal tori in $\mathrm{GL}_n(\mathbb{F}_0)$ is 1-bound $\mathrm{GL}_n$-definable in $\mathbb{A}^{n^2+1}$.*

*(2) Let $\mathfrak{F}$ be $d$-bound $\mathrm{GL}_n$-definable and denote the set of all intersections of elements of $\mathfrak{F}$ by $\mathfrak{F}_\cap$. Then $\mathfrak{F}_\cap$ is $d$-bound definable.*

*Proof.* (1) Every maximal torus is conjugated to the group of diagonal matrices

$$\mathrm{Diag}(n) := \left\{ \begin{pmatrix} \lambda_{1,1} & & & \\ & \lambda_{2,2} & & \\ & & \ddots & \\ & & & \lambda_{n,n} \end{pmatrix} \;\middle|\; \prod_{i=1}^{n} \lambda_{i,i} \neq 0 \right\} .$$

Since $\mathcal{I}(\mathrm{Diag}(n)) = \langle t \cdot \prod_{i=1}^{n} x_{i,i} - 1, x_{i,j} \mid \ i,j \in \{1,\dots,n\} \text{ with } i \neq j \rangle \subseteq \mathbb{F}_0[X,t]$ and conjugation is just linear replacement of variables, the claim follows.

(2) Take any subset $\mathfrak{F}_{\mathscr{A}} := \{V_\alpha \mid \alpha \in \mathscr{A}\}$ of $\mathfrak{F}$. For every $\alpha \in \mathscr{A}$ fix a generating set $S_\alpha \subseteq \mathbb{F}_0[X]$ such that $S_\alpha$ is $d$-bound $\mathrm{GL}_n$-definable and

$$\langle S_\alpha,\ \det(X)t - 1 \rangle = \mathcal{I}(V_\alpha) \text{ for all } \alpha \in \mathscr{A} .$$

Let $M$ denote the dimension of all polynomials in $\mathbb{F}_0[X]$ of degree less than or equal to $d$. Note that the union on the right-hand side of

$$\mathcal{I}\left( \bigcap_{\alpha \in \mathscr{A}} V_\alpha \right) = \langle \bigcup_{\alpha \in \mathscr{A}} S_\alpha,\ \det(X)t - 1 \rangle$$

is a finite union of at most $M$ sets $S_{\alpha(1)}, \dots, S_{\alpha(M)}$ with $\alpha(1), \dots, \alpha(M) \in \mathscr{A}$. This proves the statement. □

**Lemma 2.17.** *Let $\mathfrak{F}$ be a $d$-bound definable family of affine varieties in $\mathbb{A}^n$ and let $\tau : \mathbb{A}^m \to \mathbb{A}^n$ be a morphism of algebraic varieties of degree less than or equal to $e$. The set of preimages $\tau^{-1}(\mathfrak{F})$ is $(d \cdot e)$-bound definable.*

*Proof.* Take any element $\mathscr{F} \in \mathfrak{F}$ and let its ideal $\mathcal{I}(V)$ be generated by $S \subseteq \mathbb{F}[X]$.

$$\tau^{-1}(\mathscr{F}) = \{w \in \mathbb{A}^m \mid f(\tau(w)) = 0 \text{ for all } f \in S\}. \qquad \square$$

**Definition 2.18.** *Define the family*

$$\mathfrak{F}_{imt}(\mathrm{GL}_n(\mathbb{F}_0)) := \{\textit{intersection of maximal tori of } \mathrm{GL}_n(\mathbb{F}_0)\} .$$

Compare the following lemma to [Hru02, Example 3.2 c-3)].

**Lemma 2.19.** *The family $\mathfrak{F}_{imt}$ is 1-bound $\mathrm{GL}_n$-definable and any $\mathscr{M} \in \mathfrak{F}_{imt}(\mathrm{GL}_n(\mathbb{F}_0))$ is connected.*

*Proof.* From Lemma 2.16 (a) and (b) we already know, that the family $\mathscr{F}_{imt}(\mathrm{GL}_n(\mathbb{F}))$ is 1-bound $\mathrm{GL}_n$-definable.
Let $\mathscr{D}$ be $\mathrm{Diag}(n)$, the group of diagonal matrices in $\mathrm{GL}_n(\mathbb{F}_0)$ (as in the proof of Lemma 2.16) and define the linear subspace

$$W := \left\{ \begin{pmatrix} \lambda_{1,1} & & & \\ & \lambda_{2.2} & & \\ & & \ddots & \\ & & & \lambda_{n,n} \end{pmatrix} \middle| \lambda_1, \ldots, \lambda_n \in \mathbb{F}_0 \right\} \subseteq \mathrm{Mat}_n(\mathbb{F}_0) .$$

Then we have $\mathscr{D} = W \cap \mathrm{GL}_n(\mathbb{F}_0)$. Now let $\tilde{\mathscr{D}}$ be any other maximal torus. Thus there is $g \in \mathrm{GL}_n(\mathbb{F}_0)$ such that $\tilde{\mathscr{D}} = g^{-1}\mathscr{D}g$.

$$\tilde{\mathscr{D}} \cap \mathscr{D} = \underbrace{W \cap g^{-1}Wg}_{\text{subspace}} \cap \mathrm{GL}_n(\mathbb{F}_0) \subseteq \mathbb{A}^{n^2}(\mathbb{F}_0)$$

This shows, that the intersection of maximal tori is the intersection of a linear subspace with a Zariski-open set and thus ([Har77, Chapter I, Example 1.1.3]) is irreducible. $\square$

## 2.4 Unipotently generated Groups

In this section we will show that unipotently generated subgroups are bound definable. In Hrushovski's article his analog is stated in the remark following Example 3.2.

**Definition 2.20.** *Let $\mathscr{G}$ be an algebraic group. An element $u \in \mathscr{G}$ is* unipotent *if and only if there exists an integer $n$ such that*

$$(u-1)^n = 0.$$

*The* unipotently generated subgroup $\mathscr{G}^u$ *of $\mathscr{G}$ is defined as*

$$\mathscr{G}^u := \bigcap_{\chi \in X(\mathscr{G})} \ker(\chi) = \langle u \in \mathscr{G} \mid u \textit{ unipotent} \rangle .$$

**Proposition 2.21.** *If $\mathscr{G}$ is an algebraic group, then $\mathscr{G}^\circ/\mathscr{G}^u$ is a torus.*

*Proof.* By [Hum75, Lemma A] $X(\mathscr{G})$ is a finitely generated abelian group, say $X(\mathscr{G}) = \langle \chi_1, \ldots, \chi_m \rangle$. Since $\mathscr{G}^\circ$ is connected, $X(\mathscr{G})$ is torsion-free ([Hum75, Lemma B]). Now consider the map

$$\begin{aligned} \chi \colon \mathscr{G}^\circ &\to (\mathbb{F}_0^\times)^m \ . \\ g &\mapsto (\chi_1(g), \ldots, \chi_m(g)) \end{aligned}$$

It maps onto a torus and its kernel is $\mathscr{G}^u$. □

This section will deal with the proof of the following theorem and its corollary.

**Theorem 2.22.** *If $\mathscr{G}$ is a closed subgroup of $\mathrm{GL}_n(\mathbb{F}_0)$, $n > 1$ and $\mathrm{char}(\mathbb{F}_0) = 0$ then $\mathscr{G}^u$ is $B_1(n)$-bound definable with*

$$B_1(n) := B_0\left(n^2, 2n^2 \cdot (n^2 - 1)\right) \ .$$

**Corollary 2.23.** *If $\mathfrak{F}$ is a set of closed subgroups of $\mathrm{GL}_n(\mathbb{F}_0)$, then*

$$\mathfrak{F}^u := \{\mathscr{F}^u \mid \mathscr{F} \in \mathfrak{F}\}$$

*is $B_1(n)$-bound definable in $\mathbb{A}^{n^2}$.*

To prove the theorem we will state a well-known theorem about algebraic groups (see for example [TY05, 21.3.1 Theorem], [Hum75, 7.5 Proposition] or [Bor91, Chapter I, §2, 2.2 Proposition and Remark]):

**Theorem 2.24.** *Let $(X_i)_{i \in I}$ be a family of irreducible $\mathbb{F}_0$-varieties, $\mathscr{G} \subseteq \mathrm{GL}_n(\mathbb{F}_0)$ be an algebraic group and for $i \in I$, $f_i : X_i \to \mathscr{G}$ be an morphism of algebraic varieties. Assume further, that the unit element $e \in \mathscr{G}$ lies in $f(X_i)$ for every $i \in I$.*
*Define $\mathscr{H}$ to be the subgroup of $\mathscr{G}$ generated by $\{f(X_i) \mid i \in I\}$. Then $\mathscr{H}$ is connected and there exists $N \in \mathbb{N}$, $i_1, \ldots, i_N \in I$ and $\epsilon_1, \ldots, \epsilon_N \in \{-1, 1\}$ such that:*

$$\mathscr{H} = f_{i_1}(X_{i_1})^{\epsilon_1} \cdots f_{i_N}(X_{i_N})^{\epsilon_N}$$

*Furthermore $N$ can be bounded by $2 \cdot \dim(G)$.*

*Proof of Theorem 2.22:.* For any unipotent element $u \in \mathscr{G}$ define the map

$$\begin{aligned} \psi_u : \left(\mathbb{F}_0, +\right) &\to \langle u \rangle \\ b &\mapsto u^b := \exp(b \cdot \log(u)) \end{aligned}$$

with $\exp(A) := \sum_{k \geq 0} \frac{1}{k!} A^k$ and $\log(A) := \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} (A - \mathrm{Id})^k$ for $A \in \mathrm{GL}_n(\mathbb{F}_0)$. Furthermore Id denotes the identity matrix. By [OV90, Chap.3 §2.2°] $\psi_u$ is an isomorphism of algebraic groups if $\mathbb{F}_0$ is of characteristic zero.
By Theorem 2.24 there is a finite number of unipotent elements $u(1), \ldots, u(r) \in \mathscr{G}$ such that

$$\mathscr{G}^u = \psi_{u(1)}(\mathbb{F}_0) \cdot \ldots \cdot \psi_{u(r)}(\mathbb{F}_0)$$

and $r \leq 2 \dim(\mathscr{G}) \leq 2 \dim(\mathrm{SL}_n(\mathbb{F}_0)) = 2(n^2 - 1)$.
Since $\mathscr{G}^u$ is closed in $\mathbb{A}^{n^2}$, we can use Theorem 1.20 to calculate $\mathscr{G}^u$ as the image of the morphism

$$\begin{aligned} \psi : \mathbb{F}_0^r &\to \mathscr{G}^u \\ (b_1, \ldots, b_r) &\mapsto \psi_{u(1)}(b_1) \cdot \ldots \cdot \psi_{u(r)}(b_r) \ . \end{aligned}$$

Note that $\mathcal{I}(\mathbb{F}_0^r) = \langle 0 \rangle$ and $\psi$ is the product of at most $2(n^2 - 1)$ factors, each of degree less than or equal to $n^2$. Now apply Corollary 1.21 with $e = d = 2n^2 \cdot (n^2 - 1)$ and $n^2$ indeterminantes. □

The proof of the following theorem was provided by Ruyong Feng in a private communication. Although we do not require the following theorem until much later in Theorem 5.11 to compute the characters of an approximation on the differential Galois group, it is best formulated and proven in the current context.

**Theorem 2.25.** *Let $\mathscr{H} \leq \mathrm{GL}_n(\mathbb{F}_0)$ be any closed subgroup. Consider its character group $X(\mathscr{H})$ as subset in $\mathbb{F}_0[X,t]$, then $X(\mathscr{X})$ can be generated by polynomials in $\mathbb{F}_0[X,t]$ of degree less than or equal to*

$$(n+1) \cdot B_1(n) \cdot M_2(n, B_1(n)) \ .$$

*Proof.* Let $\tau\colon \mathscr{H} \to \mathrm{GL}_m(\mathbb{F}_0)$ be the map of Theorem 2.14 with kernel equal to $\mathscr{H}^u$. The degree is bounded by $(n+1) \cdot B_1(n) \cdot M_2(n, B_1(n))$ (use Theorem 2.22 and Theorem 2.14). By Proposition 2.21 $\tau(\mathscr{H}^\circ)$ is a torus, so it is conjugate to a subgroup of $(\mathbb{F}_0^\times)^m$. Thus $X(\tau(\mathscr{H}^\circ))$ is generated by linear polynomials $\langle p_1, \ldots, p_m \rangle$.
Now consider the group homomorphism

$$\begin{aligned} \tilde{\tau}\colon X(\tau(\mathscr{H}^\circ)) &\to X(\mathscr{H}^\circ) \ . \\ \chi &\mapsto \chi \circ \tau \end{aligned}$$

We show that $\tilde{\tau}$ is surjective: Let $\chi \in X(\mathscr{H}^\circ)$ be any character. On any coset $h\mathscr{H}^u$ (with $h \in \mathscr{H}^\circ$) $\chi$ is constant. Thus there exists $g \in \mathbb{F}_0[\tau(\mathscr{H}^\circ)]$ with $g \circ \tau = \chi$. Note that $g$ is a character: Take any $a, b \in \tau(\mathscr{H}^\circ)$ and take preimages $\tilde{a}, \tilde{b} \in \mathscr{H}^\circ$. Then we have

$$g(ab) = g(\tau(\tilde{a})\tau(\tilde{b})) = g(\tau(\tilde{a}\tilde{b})) = \chi(\tilde{a}\tilde{b}) = \chi(\tilde{a})\chi(\tilde{b}) = g(a)g(b) \ .$$

By surjectivity $p_1 \circ \tau, \ldots, p_m \circ \tau$ must generate $X(\mathscr{H}^\circ)$. □

## 2.5 Stabilizers and Normalizers

For a group $G$ acting on a set $X$ let

$$\mathrm{Stab}_G(x) \coloneqq \{ g \in G \mid gx = x \}$$

denote the *stabilizer* of $x \in X$ in $G$.

**Definition 2.26.** *Let $V$ be a $n$-dimensional $\mathbb{F}_0$-vector space. For $k, d \in \mathbb{N}$ define*

$$\mathfrak{N}_d(V^k) \coloneqq \left\{ W \subseteq V^k \mid W \text{ is } d\text{-bound definable} \right\}$$

**Theorem 2.27.** *Let $\mathscr{H}$ be an $e$-bound $\mathrm{GL}_n$-definable closed subgroup of $\mathrm{GL}_n(\mathbb{F}_0)$ and $U \in \mathscr{N}_d(V^k)$, then $\mathrm{Stab}_{\mathscr{H}}(U) \subseteq \mathbb{F}_0[X,t]$ can be computed and is $\max\{e,\ d\}$-bound definable.*

The following corollary has an analog in [Hru02, Lemma 3.8.a].

**Corollary 2.28.** *For every $k \in \mathbb{N}$ the family*

$$\mathfrak{F}_{V^n,k,d} \coloneqq \left\{ \mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_0)}(U) \mid U \in \mathfrak{N}_d(V^k) \right\}$$

*is $d$-bound $\mathrm{GL}_n$-definable.*

*Proof of the theorem.* Fix an arbitrary $U \in \mathfrak{N}_d(V^k)$ and denote a set of generators of the defining ideal $I := \mathcal{I}(U)$ by $\{f_1, \ldots, f_r\}$ each of degree less than or equal to $d$. For any $g = (g_{i,j})_{1 \le i,j \le n} \in \mathrm{GL}_n(\mathbb{F}_0)$ there is according to Lemma 2.2 the following equivalence:

$$r_g U \subseteq U \Leftrightarrow \rho_g f_i \in I \text{ for } i = 1, \ldots, r \ .$$

Let $\mathscr{A} = \{h_1, \ldots, h_m\}$ be the set of all monomials of degree less than or equal to $d$ in the $nk$ variables $x_{1,1}, \ldots, x_{n,k}$ with respect to any order. We can rewrite

$$\rho_Z f_i(X_{k,n}) = \sum_{j=1}^{m} p_{i,j}(Z) h_j$$

with $p_{i,j}(Z) \in \mathbb{F}_0[Z]$ of degree less than or equal to $d$ for $i = 1, \ldots, r$ and $j = 1, \ldots, m$. Define the set

$$\mathscr{S} = \{g \in \mathrm{GL}_n(\mathbb{F}_0) \mid \rho_g f_i(X_{k,n}) \in I \text{ for } i = 1, \ldots, r\} \ .$$

If we replace the occurring $p_{i,j}(Z)$ by new variables $y_{i,j}$ for $1 \le i \le r$ and $1 \le j \le m$ then Corollary 1.18 tells us that $\mathscr{S}$ is a variety generated by polynomials of degree 1 in $y_{i,j}$. Resubstituting the polynomials $p_{i,j}(Z)$, which are of degree $d$, for $y_{i,j}$, we see that the defining ideal of $\mathscr{S}$ in $\mathbb{F}_0[Z]$ is $d$-bound definable.
Now we have bounded the variety

$$\mathscr{S} = \{g \in \mathrm{GL}_n \mid r_g U \subseteq U\} \ .$$

But in fact this already is the stabilizer, since for any $g \in \mathrm{GL}_n(\mathbb{F}_0)$ we have $r_g U \subseteq U \Rightarrow r_g U = U$. This is due to the fact that the map

$$\begin{aligned} \rho_g : \mathrm{span}_{\mathbb{F}}(f_1, \ldots, f_r) &\to \mathrm{span}_{\mathbb{F}}(f_1, \ldots, f_r) \\ f_i &\mapsto \rho_g(f_i) \end{aligned}$$

is an injective map of finite dimensional vector spaces and thus surjective. □

**Example 2.29.** *Let the variety $U$ be given by the ideal*

$$I = \langle \underbrace{x_{1,1}^2 - x_{1,2}}_{f_1}, \ \underbrace{x_{1,1}^2 + 4x_{1,1}x_{1,2} + 4x_{1,2}^3}_{f_2} \rangle \subseteq \mathbb{F}_0[x_{1,1}, \ x_{1,2}] \ .$$

*We want to compute its stabilizer in $\mathrm{GL}_2(\mathbb{F}_0)$. Since $I$ is generated by polynomials of degree 2, the set of monomials $\mathscr{A}$ equals $\{1, \ x_{1,1}, \ x_{1,2}, \ x_{1,1}^2, \ x_{1,1}x_{1,2}, \ x_{1,2}^2\}$.*
*The following computations are in $\mathbb{F}_0[x_{1,1}, \ x_{1,2}] \otimes \mathbb{F}_0[Z]$ with $Z = \begin{pmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{pmatrix}$ and $G$ a*

*Gröbner basis of $I$:*

$$\begin{aligned}
\rho_Z f_1 =& z_{1,1}^2 x_{1,1}^2 + 2z_{1,1}z_{2,1}x_{1,1}x_{1,2} + z_{2,1}^2 x_{1,2}^2 - x_{1,1}z_{1,1} - x_{1,2}z_{2,1},\\
\rho_Z f_2 =& (2z_{1,1}z_{2,1} + 4z_{1,1}z_{2,2} + 4z_{2,1}z_{1,2} + 8z_{1,2}z_{2,2})x_{1,1}x_{1,2}\\
&+ (z_{1,1}^2 + 4z_{1,1}z_{1,2} + 4z_{1,2}^2)x_{1,1}^2 + (z_{2,1}^2 + 4z_{2,1}z_{2,2} + 4z_{2,2}^2)x_{1,2}^2,\\
\mathrm{N}(\rho_Z f_1, G) =& x_{1,2}^2 \underbrace{(z_{2,1} - 8z_{1,1}z_{2,1})}_{p_1(Z)} + x_{1,2}\underbrace{(z_{1,1} - \frac{1}{2}z_{1,1}z_{2,1} - z_{2,2})}_{p_2(Z)} - x_{1,1}\underbrace{z_{1,2}}_{p_3(Z)},\\
\mathrm{N}(\rho_Z f_2, G) =& x_{1,2}^2 p_4(Z) + x_{1,2}p_5(Z),\\
&\textit{with}\\
p_4(Z) =& 16z_{2,2}^2 + 4z_{2,1}z_{2,2} + z + 2, 1^2 - 32z_{1,2}z_{2,2} - 16z_{1,2}z_{2,1}\\
&- 16z_{1,1}z_{2,2} - 8z_{1,1}z_{2,1},\\
p_5(Z) =& z_{1,1}^2 + 4z_{1,1}z_{1,2} - \frac{1}{2}z_{1,1}z_{2,1} - z_{1,1}z_{2,2} + 16z_{1,2}^2 - z_{1,2}z_{2,1} - 2z_{2,2}.
\end{aligned}$$

*Then* $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_0)}(I)$ *is given as the vanishing set of the ideal* $\langle p_1(Z), \ldots, p_5(Z)\rangle \subseteq \mathbb{F}_0[Z]$ *(and the requirement to have non-zero determinant).*

For a subset $M$ of a group $G$ let

$$N_G(M) \coloneqq \left\{ g \in G \;\middle|\; gMg^{-1} = M \right\}$$

denote the *normalizer* of $M$ in $G$.
Hrushovki proves an analog of the following theorem in [Hru02, Example 3.2.b)].

**Theorem 2.30.** *Let $\mathscr{H}$ be an $e$-bound definable closed subgroup of $\mathrm{GL}_n(\mathbb{F}_0)$ and $\mathscr{M} \subseteq \mathrm{GL}_n(\mathbb{F}_0)$ a $d$-bound $\mathrm{GL}_n$-definable closed subset . Then $N_{\mathscr{H}}(\mathscr{M}) \in \mathbb{F}[X,t]$ is $\max\{e, d(n+1)\}$-bound definable and thus $\max\{e, d(n+1)^2\}$-bound $\mathrm{GL}_n$-definable.*

*Proof.* The proof goes exactly as the proof of Theorem 2.27. One just has to change some ingredients: Let the $I'$ be the determinant-free form of $\mathcal{I}(M)$, which is generated by some $f_1, \ldots, f_r \in \mathbb{F}_0[X]$. Let $h_1, \ldots, h_m$ denote all monomials in the variables in $X$ of degree less than or equal to $d$. Now for every $i = 1, \ldots, r$ we have

$$\gamma_Z f_i(X) = \sum_{j=1}^{m} p_{i,j}(Z,s)h_j \in \mathbb{F}_0[Z,X,s]$$

with $p_{i,j}(Z,s) \in \mathbb{F}_0[Z,s]$. Here we used the fact that we can rewrite the inverse of a matrix as the product of the inverse of the determinant with a matrix with entries of degree $n-1$ (this is known as Cramer's rule from linear algebra). Thus the degree of the occurring $p_{i,j}(Z,s)$ is of degree $d \cdot (n+1)$. □

**Corollary 2.31.** *Let $\mathscr{M}$ be an arbitrary intersection of maximal tori in $\mathrm{GL}_n(\mathbb{F}_0)$. The normalizer $N_{\mathrm{GL}_n(\mathbb{F}_0)}(\mathscr{M})$ is $(n+1)$-bound definable and $(n+1)^2$-bound $\mathrm{GL}_n$-definable.*

**Example 2.32.** *Consider the diagonal torus $\mathscr{T} = \mathrm{Diag}(7)$ in $\mathrm{GL}_7(\mathbb{F}_0)$. Every other maximal torus $\mathscr{T}_1$ is conjugate to $\mathscr{T}$ via some matrix $Y \in \mathrm{GL}_7(\mathbb{F}_0)$.*

*If we choose* $Y = \begin{pmatrix} 1 & 1 & 1 & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & 1 & 1 & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & \end{pmatrix}$, *then the intersection $\mathscr{M} = \mathscr{T} \cap c_Y(\mathscr{T})$ is*

$$\mathscr{M} := \left\{ \begin{pmatrix} \lambda_1 & & & & & & \\ & \lambda_1 & & & & & \\ & & \lambda_1 & & & & \\ & & & \lambda_2 & & & \\ & & & & \lambda_3 & & \\ & & & & & \lambda_3 & \\ & & & & & & \lambda_3 \end{pmatrix} \;\middle|\; \lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_0 \backslash \{0\} \right\}. \text{ The normalizer of } \mathscr{M} \text{ is given by}$$

$$\left\{ \begin{pmatrix} \boxed{A_1} & & \\ & a & \\ & & \boxed{A_3} \end{pmatrix} \;\middle|\; a \in \mathbb{F}_0 \backslash \{0\},\ A_1, A_3 \in \mathrm{GL}_3(\mathbb{F}_0) \right\}$$

$$\cup \left\{ \begin{pmatrix} & & \boxed{B_1} \\ & b & \\ \boxed{B_3} & & \end{pmatrix} \;\middle|\; b \in \mathbb{F}_0 \backslash \{0\},\ B_1, B_3 \in \mathrm{GL}_3(\mathbb{F}_0) \right\}.$$

*The defining ideal* $\mathcal{I}\big(N_{\mathrm{GL}_7(\mathbb{F}_0)}(\mathscr{M})\big)$ *is generated by* $\det(X)t - 1$ *and the following set of polynomials:*

$$\begin{aligned}
x_{i,j} \det \begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,1} & x_{2,2} & x_{2,3} \\ x_{3,1} & x_{3,2} & x_{3,3} \end{pmatrix} &\text{ for } 1 \le i \le 3,\ 5 \le j \le 7, \\
x_{i,j} \det \begin{pmatrix} x_{5,5} & x_{5,6} & x_{5,7} \\ x_{6,5} & x_{6,6} & x_{6,7} \\ x_{7,5} & x_{7,6} & x_{7,7} \end{pmatrix} &\text{ for } 5 \le i \le 7,\ 1 \le j \le 3, \\
x_{i,j} \det \begin{pmatrix} x_{1,5} & x_{1,6} & x_{1,7} \\ x_{2,5} & x_{2,6} & x_{2,7} \\ x_{3,5} & x_{3,6} & x_{3,7} \end{pmatrix} &\text{ for } 1 \le i \le 3,\ 1 \le j \le 3, \\
x_{i,j} \det \begin{pmatrix} x_{5,1} & x_{5,2} & x_{5,3} \\ x_{6,1} & x_{6,2} & x_{6,3} \\ x_{7,1} & x_{7,2} & x_{7,3} \end{pmatrix} &\text{ for } 5 \le i \le 7,\ 5 \le j \le 7.
\end{aligned}$$

*Thus* $N_{\mathrm{GL}_7(\mathbb{F}_0)}(\mathscr{M})$ *is* 8*-bound definable* ($8 = n + 1$).

**Remark 2.33.** *We will apply Corollary 2.31 in the proof of the important Lemma 2.35. In fact one can understand much more about the nature of intersections of maximal tori and their normalizers: The normalizer of the intersection of maximal tori consist of "generalized block permutation matrices"*[1]*, as seen in Example 2.32. Using this description one arrives at the same result as in Corollary 2.31.*

## 2.6 Hrushovskis bound definable family

Having provided all the necessary tools and ingredients, we are able to restate and proof the existence statements of Hrushovskis article [Hru02] in the language of algebraic geometry. The following result goes back to Jordan and the bound is due to Schur. It is restated in the following form in [vdPS03, Theorem 4.17]:

**Theorem 2.34.** *There is a function* $J : \mathbb{N} \to \mathbb{N}$ *having the following property: For every finite subgroup* $\mathscr{A}$ *of* $\mathrm{GL}_n(\mathbb{F}_0)$ *there is an abelian normal subgroup* $\mathscr{N}$ *of* $\mathscr{A}$ *with*

$$[\mathscr{A} : \mathscr{N}] \le J(n) \le (\sqrt{8n} + 1)^{2n^2} - (\sqrt{8n} - 1)^{2n^2}\ .$$

[1] These are block matrices consisting of submatrices such that there is exactly one invertible submatrix in each row and column, all other submatrices are zero.

The following lemma is the analog of [Hru02, Lemma 3.6a/d] in the language of bound definable families.

**Lemma 2.35.** *Define the two functions* $B_3, B_4 \colon \mathbb{N} \to \mathbb{N}$

$$B_3(n) = (n+1)^3 \cdot M_2(n, (n+1)^2)$$
$$B_4(n) = B_3\Big(M_2(n, B_1(n))^2\Big) \cdot B_1(n) \cdot (n+1) \cdot M_2(n, B_1(n)) \ .$$

*There is a* $B_4(n)$*-bound definable family* $\mathfrak{F}$ *of closed subgroups of* $\mathrm{GL}_n(\mathbb{F}_0)$ *and an integer* $I(n)$ *with the following property:*
*For all closed subgroups* $\mathscr{G}$ *of* $\mathrm{GL}_n(\mathbb{F}_0)$ *there exists an element* $\mathscr{F} \in \mathfrak{F}$ *such that*

*(1)* $\mathscr{G}^\circ$ *is a subgroup of* $\mathscr{F}$*,*

*(2)* $\mathscr{G} \subseteq N_{\mathrm{GL}_n(\mathbb{F}_0)}(\mathscr{F})$*,*

*(3)* $[\mathscr{G} : \mathscr{G} \cap \mathscr{F}] = [\mathscr{G}\mathscr{F} : \mathscr{F}] \leq I(n) := J\Big(M_2\big(P(n),\ (P(n)+1)^2\ \big)^2\ \Big)$ *with* $P(n) = M_2(n, B_1(n))$*,*

*(4)* $\mathscr{F}^u \subseteq \mathscr{G}^\circ$*.*

*Proof.* This proof will be subdivided into three parts: First we show the claim for finite groups, then for groups whose connected component is a torus and finally for arbitrary groups.
Let $\mathscr{G}$ be a finite subgroup of $\mathrm{GL}_n(\mathbb{F}_0)$. By Theorem 2.34 there is an abelian normal subgroup $\mathscr{A}$ of $\mathscr{G}$ with $[\mathscr{G} : \mathscr{A}] \leq J(n)$. Being a finite abelian subgroup of $\mathrm{GL}_n(\mathbb{F}_0)$, $\mathscr{A}$ is diagonalizable and therefore lies in a maximal torus. Define the group

$$\mathscr{M} := \bigcap \mathscr{T} \in \mathfrak{F}_{imt}(\mathrm{GL}_n(\mathbb{F}_0))$$

where the intersection runs over all maximal tori $\mathscr{T}$ in $\mathrm{GL}_n(\mathbb{F}_0)$, which contain $\mathscr{A}$. By Lemma 2.19 we have $\mathscr{M} = \mathscr{M}^\circ$. Furthermore $\mathscr{M}$ satisfies the conditions (1)-(4):

(1) $\mathscr{G}^\circ = \{1\} \subseteq \mathscr{M}$.

(2) $\mathscr{G}$ normalizes $\mathscr{M}$: For every $g \in \mathscr{G}$ we have $g\mathscr{M}g^{-1} = \bigcap g\mathscr{T}g^{-1} = \mathscr{M}$ (since $g\mathscr{T}g^{-1} \supseteq g\mathscr{A}g^{-1} = \mathscr{A}$ by normality of $\mathscr{A}$ in $\mathscr{G}$).

(3) Since $\mathscr{A}$ is contained in $\mathscr{M}$ we have $[\mathscr{G} : \mathscr{G} \cap \mathscr{M}] = [\mathscr{G} : \mathscr{A}] \cdot [\mathscr{A} : \mathscr{G} \cap \mathscr{M}] \leq [\mathscr{G} : \mathscr{A}] \leq J(n)$.

(4) Tori do not contain non-trivial unipotent elements.

So for the finite case the family $\mathfrak{F}_0(n) := (\mathfrak{F}_{imt}(\mathrm{GL}_n(\mathbb{F}_0)))^\circ$ suffices and this family is 1-bound $\mathrm{GL}_n$-definable (use Lemma 2.19).

Now assume that $\mathscr{G}^\circ$ is a torus and define

$$\mathscr{M} := \bigcap \mathscr{T} \in \mathfrak{F}_{imt}(\mathrm{GL}_n(\mathbb{F}_0))$$

where the intersection runs over all maximal tori $\mathscr{T}$ in $\mathrm{GL}_n(\mathbb{F}_0)$, which contain $\mathscr{G}^\circ$. We have $\mathscr{M} = \mathscr{M}^\circ$ and $\mathscr{G} \subseteq N_{\mathrm{GL}_n(\mathbb{F}_0)}(\mathscr{M})$ ( since for any $g \in \mathscr{G}$ we have $g\mathscr{G}^\circ g^{-1} = \mathscr{G}^\circ$). Also define $\mathscr{N} := N_{\mathrm{GL}_n(\mathbb{F}_0)}(\mathscr{M}^\circ)$. By Theorem 2.14 there is a rational representation

$\tau : \mathscr{N} \to \mathrm{GL}_{m(n)}(\mathbb{F}_0)$ with kernel $\mathscr{M}^\circ$ and $m(n)$ some natural number bound by $M := M_2(n, (n+1)^2)^2$ (apply Theorem 2.14 and Corollary 2.31).Furthermore the degree of $\tau$ is bound by

$$B_3(n) := (n+1)^3 \cdot M_2(n, (n+1)^2) \ .$$

Since $\mathscr{G}^\circ \subseteq \mathscr{M}^\circ$ and the index of $\mathscr{G}^\circ$ in $\mathscr{G}$ is finite we see that $\tau(\mathscr{G})$ is a finite subgroup of $\mathrm{GL}_M(\mathbb{F}_0)$. Since we already proved the claim for finite groups, there is $\mathscr{F} \in \mathfrak{F}_0(M)$ with properties (1)-(4) with respect to $\tau(\mathscr{G})$. Now check that the pullback $\tau^{-1}(\mathscr{F})$ has the desired properties (as preimage of a closed set under a continuous map, it is closed):

(1) Since $\mathbb{F}_0$ is algebraically closed, morphisms commute with taking connected components (see [Hum75, Chapter II, 7.4, Proposition B (c)]) we have
$\tau(\mathscr{G})^\circ = \tau(\mathscr{G}^\circ) \leq \mathscr{F} \Rightarrow \mathscr{G}^\circ \leq \tau^{-1}(\mathscr{F})$.

(2) Let $g \in \mathscr{G}$ be arbitrary and write it as a product $g = hg_i$ for some representatives of the irreducible components of $\mathscr{G}$ denoted by $g_i$ and some $h \in \mathscr{G}^\circ$. Then for any $f \in \tau^{-1}(\mathscr{F})$ we observe that $\tau(g_i f g_i^{-1}) = \tau(g_i)\tau(f)\tau(g_i)^{-1} \in \mathscr{F}$ since $\tau(\mathscr{G}) \subseteq N_{\mathrm{GL}_M}(\mathscr{F})$ by assumption. Therefore $g_i f g_i^{-1} \in \tau^{-1}(\mathscr{F})$ and conjugation with an element $h \in \mathscr{G}^\circ \subseteq \ker(\tau) \subseteq \tau^{-1}(\mathscr{F})$ leaves $\tau^{-1}(\mathscr{F})$ invariant.

(3)
$$\begin{aligned}
[\mathscr{G} : \mathscr{G} \cap \tau^{-1}(\mathscr{F})] &= [\mathscr{G} : \mathscr{N}] \cdot [\mathscr{G} \cap \tau^{-1}(\mathscr{F}) : \mathscr{N}]^{-1} \\
&= |\tau(\mathscr{G})| \cdot |\tau\big(\mathscr{G} \cap \tau^{-1}(\mathscr{F})\big)|^{-1} \\
&= [\tau(\mathscr{G}) : \tau\big(\mathscr{G} \cap \tau^{-1}(\mathscr{F})\big)] \\
&= [\tau(\mathscr{G}) : \tau(\mathscr{G}) \cap \mathscr{F}] \leq J(M).
\end{aligned}$$
For the last equality see the Proposition 2.36 below and note that $\mathscr{N} \subseteq \tau^{-1}(\mathscr{F})$.

(4) We use the argument that a torus does not contain unipotent elements several times: If $u \in \tau^{-1}(\mathscr{F})$ is unipotent, then $\tau(u) \in \mathscr{F}$ is also unipotent. Since $\mathscr{F}$ is the intersection of tori $\tau(u) = 1$. So $u \in \ker(\tau) = \mathscr{M}^\circ \subseteq \mathscr{M} \subseteq \mathscr{T}$ for any torus $\mathscr{T}$ occurring in the definition of $\mathscr{M}$. Therefore $u = 1$.

So in this case the family

$$\mathfrak{F}_1(n) := \Big\{ \tau_{\mathscr{M}^\circ}^{-1}(\mathscr{F}) \ \Big| \ \mathscr{M} \in \mathfrak{F}_{imt}(\mathrm{GL}_n(\mathbb{F}_0)), \mathscr{F} \in \mathfrak{F}_0(M) \\ \tau_{\mathscr{M}^\circ} : N_{\mathrm{GL}_n(\mathbb{F}_0)}(\mathscr{M}^\circ) \to \mathrm{GL}_M(\mathbb{F}_0) \text{ with } \ker(\tau) = \mathscr{M}^\circ \Big\}$$

suffices and is $B_3(n)$-bound definable.

Now let $\mathscr{G}$ be arbitrary. Define $\mathscr{U} := (\mathscr{G}^\circ)^u$ and $\mathscr{N} := N_{\mathrm{GL}_n(\mathbb{F}_0)}(\mathscr{U})$. Since for any $u \in \mathscr{U}$ and $g \in \mathscr{G}$ the element $gug^{-1}$ is unipotent, we have $\mathscr{G} \leq \mathscr{N}$. Again use Theorem 2.14 to find a rational representation $\tau : \mathscr{N} \to \mathrm{GL}_{p(n)}(\mathbb{F}_0)$ with $\ker(\tau) = \mathscr{U}$ and $p(n) \leq P$ with $P := M_2(n, B_1(n))^2$ and degree of $\tau$ bounded by

$$B_1(n) \cdot (n+1) \cdot M_2(n, B_1(n)) \ .$$

Since $\tau(\mathscr{G})^\circ = \mathscr{G}^\circ/(\mathscr{G}^\circ)^u$ is a torus we can apply the claim for $\tau(\mathscr{G})$: There exists $\mathscr{F} \in \mathfrak{F}_1(P)$ with properties (1)-(4) with respect to $\tau(\mathscr{G})$. Then $\tau^{-1}(\mathscr{F})$ satisfies the properties (1)-(3) exactly as in the previous case with

$$[\mathscr{G} \cdot \tau^{-1}(\mathscr{F}) : \tau^{-1}(\mathscr{F})] \leq J(M_2(P, (P+1)^2)^2) \ .$$

For any unipotent element $u \in \tau^{-1}(\mathscr{F})$ we have $\tau(u) \in \mathscr{F}$ and is unipotent, thus $\tau(u) \in \tau(\mathscr{G}) = \mathscr{G}/\mathscr{G}^u$ and $\tau(u) = 1$. Since the kernel of $\tau$ is $\mathscr{G}^u$, property (4) is satisfied.
For an arbitrary $\mathscr{G}$ set $P := M_2(n, B_1(n))$ and let $\mathfrak{GL}_n$ be the family of all closed subgroups of $\mathrm{GL}_n(\mathbb{F}_0)$. Then the family

$$\mathfrak{F}_2(n) := \left\{ \tau_{\mathscr{U}}^{-1}(\mathscr{F}) \;\middle|\; \mathscr{F} \in \mathfrak{F}_1(P), \mathscr{U} \in \mathfrak{GL}_n^u, \right. \\ \left. \tau_{\mathscr{U}} : N_{\mathrm{GL}_n(\mathbb{F}_0)}(\mathscr{U}) \to \mathrm{GL}_P(\mathbb{F}_0) \text{ with kernel } \mathscr{U} \right\}$$

is $B_4(n)$-bound definable with

$$B_4(n) := \underbrace{B_3\left(M_2(n, B_1(n))^2\right)}_{\text{bound on } \mathfrak{F}_1(P)} \cdot \underbrace{B_1(n) \cdot (n+1) \cdot M_2(n, B_1(n))}_{\deg(\tau)}$$

and satisfies all requirements. □

**Proposition 2.36.** *Let $f\colon G \to H$ be a group homomorphism with kernel $N$ and $A, B$ be two subgroups of $G$. Then $f(A \cap B \cdot N) = f(A) \cap f(B)$.*

*Proof.* We have $f(A \cap B \cdot N) \subseteq f(A) \cap f(B \cdot N) = f(A) \cap f(B)$.
Now let $x \in f(A) \cap f(B)$ and take $a \in A$, $b \in B$ with $x = f(a) = f(b)$. Then $1 = f(a)f(b)^{-1} = f(ab^{-1})$, so $ab^{-1} \in N$. Take $n \in N$ with $a = b \cdot n$ then $a \in A \cap B \cdot N$ and maps to $x$. □

Now we are able to prove the statement of Theorem 1.1. This corresponds to [Hru02, Corollary 3.7].

**Corollary 2.37.** *There is a $B_5(n)$-bound definable family $\mathfrak{F}$ of closed subgroups of $\mathrm{GL}_n(\mathbb{F}_0)$ with the following property:*
*For all closed subgroups $\mathscr{G}$ of $\mathrm{GL}_n(\mathbb{F}_0)$ there exists $\mathscr{M} \in \mathfrak{F}$ such that*

$$\mathscr{M}^u \lhd \mathscr{G}^\circ \leq \mathscr{G} \leq \mathscr{M} \ .$$

*Proof.* Let $\mathfrak{F}'$ be the $B_4(n)$-bound definable family of Lemma 2.35 and define

$$\mathfrak{F} := \{ \mathscr{M} \leq \mathrm{GL}_n(\mathbb{F}_0) \mid \exists\, \mathscr{F} \in \mathfrak{F}' : \ [\mathscr{M} : \mathscr{F}] \leq I(n) \} \ .$$

Take $\mathscr{M} \in \mathfrak{F}$ and pick $m_1, m_2, \ldots, m_{I(n)} \in \mathscr{M}$ such that $\mathscr{M} = \bigcup_{i=1}^{I(n)} \mathscr{F} \cdot m_i$ for some $\mathscr{F} \in \mathfrak{F}'$. Furthermore let $S \subseteq \mathbb{F}[X, s]$ be a finite subset of polynomials of degree less or equal to $B_4(n)$ such that $\mathcal{F} = \langle f \mid f \in S \rangle$. We have

$$\mathcal{I}(M) = \bigcap_{i=1}^{I(n)} \mathcal{I}(Fm_i) \ .$$

Use Theorem 1.22 to find generators for $\mathcal{I}(M)$. Doing this one first calculates a Gröbner basis of polynomials of degree $B_4(n) + 1$ in $n^2 + 1 + I(n)$ indeterminantes. Thus, using Theorem 1.13, that Gröbner basis is of degree

$$B_5(n) := B_0(n^2 + 1 + I(n), B_4(n) + 1) \ .$$

Now let $\mathscr{G}$ be a closed subgroup of $\mathrm{GL}_n(\mathbb{F}_0)$ and pick $\mathscr{F} \in \mathfrak{F}'$ satisfying the four properties of Lemma 2.35. Then $\mathscr{M} := \mathscr{F}\mathscr{G} \in \mathfrak{F}$ satisfies all the requirements.

Normality of $\mathscr{M}^u$ in $\mathscr{G}^\circ$ follows from an easy observation: Any $m \in \mathscr{M}^u$ is a product of unipotent elements $u_1, \ldots, u_r \in \mathscr{M}$. Let $g \in \mathscr{G}^\circ$ be arbitrary, then

$$gmg^{-1} = \prod_{i=1}^{r} gu_ig^{-1}$$

and every factor $gu_ig^{-1}$ is unipotent and hence is in $\mathscr{M}^u$. □

# Chapter 3

# Differential Algebra

In this chapter we give a brief introduction to differential algebra and fix further notation. All of these results are well known and most of them can be found in [vdPS03].
In contrast to many other sources about differential algebra, our main focus lies on linear differential operators. The reason for this will became apparent in Chapter 5.

## 3.1 Differential Equations

**Definition 3.1.** - *For any commutative ring* $\mathfrak{R}$ *a* derivation (on $\mathfrak{R}$) *is a map* $\delta\colon \mathfrak{R} \to \mathfrak{R}$ *satisfying for all* $a, b \in \mathfrak{R}$

$$\delta(a+b) = \delta(a) + \delta(b)$$
$$\delta(ab) = \delta(a)b + a\delta(b).$$

- *A* differential ring *is a tuple* $(\mathfrak{R}, \delta)$ *consisting of a commutative ring* $\mathfrak{R}$ *together with a derivation* $\delta\colon \mathfrak{R} \to \mathfrak{R}$. *Define the* constants *of* $(\mathfrak{R}, \delta)$ *as* $\mathfrak{R}_0 := \mathrm{Ker}(\delta)$.

- *Let* $(\mathfrak{R}, \delta)$ *be a differential ring. A* differential ideal $\mathfrak{i}$ *is an ideal* $\mathfrak{i}$ *in* $\mathfrak{R}$ *satisfying* $\delta(a) \in \mathfrak{i}$ *for all* $a \in \mathfrak{i}$.

- *A differential ring is* simple *if it contains no non-trivial differential ideals.*

- *A* differential field *is a tuple* $(\mathbb{F}, \delta)$ *consisting of a field* $\mathbb{F}$ *together with a derivation* $\delta\colon \mathbb{F} \to \mathbb{F}$. *Define the* constants *of* $(\mathbb{F}, \delta)$ *as* $\mathbb{F}_0 := \mathrm{Ker}(\delta)$.

- *Let* $(\mathfrak{R}_1, \delta_1)$, $(\mathfrak{R}_2, \delta_2)$ *be two differential rings. We say that* $(\mathfrak{R}_1, \delta_1)$ *is an extension of* $(\mathfrak{R}_2, \delta_2)$ *if and only if* $\mathfrak{R}_1 \supseteq \mathfrak{R}_2$ *and* $\delta_1|_{\mathfrak{R}_2} = \delta_2$. *We denote this by* $(\mathfrak{R}_2, \delta_2) \geq (\mathfrak{R}_1, \delta_1)$.

Most of the time we will require the constants $\mathbb{F}_0$ to be algebraically closed of characteristic 0. Sometimes we will even require $\mathbb{F}$ to be (a finite algebraic extension of) $\mathbb{C}(t)$ and $\delta = \frac{d}{dt}$.
In the case of extensions of differential rings, we often will not distinguish the occurring derivations and simply denote both of them by $\delta$.

**Definition 3.2.** *Let* $(\mathbb{F}, \delta)$ *be a differential field with constants* $\mathbb{F}_0$ *and* $(\mathfrak{R}, \delta)$ *a differential ring extending* $(\mathbb{F}, \delta)$. *For any vector or matrix* $v$ *we define* $\delta(v)$ *as the vector or matrix received by applying* $\delta$ *to every component.*

- *Let* $A \in \mathbb{F}^{n\times n}$ *and* $Y = (y_1, \ldots, y_n)^T$ *indeterminants. Then we call a matrix equation of the form* $\delta(Y) = AY$ *a* matrix differential equation (of dimension $n$).

- *For a given matrix differential equation* $\delta(Y) = AY$ *of dimension* $n$ *we define its* solution space (in $\mathfrak{R}$) *as* $\mathrm{Soln}_{\mathfrak{R}}(A) := \{v \in \mathfrak{R}^n \mid \delta(v) = Av\}$.
- *For a given matrix differential equation* $\delta(Y) = AY$ *of dimension* $n$ *a matrix* $F$ *in* $GL_n(\mathfrak{R})$ *with* $\delta(F) = AF$ *is called* fundamental matrix (for $\delta(Y) = AY$).
- *Two matrix differential equations given by the matrices* $A, B \in \mathbb{F}^{n\times n}$ *are* equivalent *if and only if there exists* $C \in \mathrm{GL}_n(\mathbb{F})$ *with*

$$B = C^{-1}AC - C^{-1}\delta(C) \ .$$

**Proposition 3.3.** *Let* $(\mathbb{F}, \delta)$ *be a differential field and* $(\mathfrak{R}, \delta)$ *a differential ring extension. Let* $A, B \in \mathbb{F}^{n\times n}$ *and* $C \in \mathrm{GL}_n(\mathbb{F})$ *such that* $B = C^{-1}AC - C^{-1}\delta(C)$. *Furthermore assume that there exists a fundamental matrix* $F \in \mathrm{GL}_n(\mathfrak{R})$ *for* $A$. *Then we have*

- *The solution space* $\mathrm{Soln}_{\mathfrak{R}}(A)$ *is a* $\mathbb{F}_0$*-vector space of dimension* $n$.
- *The set of all fundamental matrices for* $\delta(Y) = AY$ *is* $F \cdot \mathrm{GL}_n(\mathbb{F}_0)$.
- *The matrix* $C^{-1}F$ *is a fundamental matrix for* $B$.

*Proof.* These statements are clear after reading [vdPS03, Section 1.2] and in particular [vdPS03, Lemma 1.8].
Only the calculation proving the last statement can not be found and is proven here. At first we compute $\delta(C^{-1})$:

$$\begin{aligned} 0 = \delta(C^{-1}C) &= \delta(C^{-1})C + C^{-1}\delta(C) \\ \Rightarrow \delta(C^{-1}) &= C^{-1}\delta(C)C^{-1} \ . \end{aligned}$$

Now we can easily show the last claim:

$$\begin{aligned} BC^{-1}F &= C^{-1}AF - C^{-1}\delta(C)C^{-1}F \\ &= C^{-1}\delta(F) - \delta(C^{-1})F \\ &= \delta(C^{-1}F) \ . \end{aligned}$$

□

**Definition 3.4.** *For any differential field* $(\mathbb{F}, \delta)$ *denote by* $\mathbb{F}[\delta]$ *the non-commutative ring of polynomials in* $\delta$ *with coefficients in* $\mathbb{F}$. *Thus every element of* $\mathbb{F}[\delta]$ *is of the form*

$$L = a_n\delta^n + a_{n-1}\delta^{n-1} + \ldots + a_1\delta + a_0 \text{ with } a_0, \ldots, a_n \in \mathbb{F} \ . \tag{3.1}$$

*The multiplication in* $\mathbb{F}[\delta]$ *is induced by*

$$\delta \cdot a = \delta(a) + a \cdot \delta \text{ for all } a \in \mathbb{F} \ .$$

*The elements of* $\mathbb{F}[\delta]$ *are called* (ordinary) linear differential operators . *If* $L$ *is as in 3.1 we define the* order of $L$ *as* $\mathrm{ord}(L) = \max\{n \in \mathbb{N} \mid a_n \neq 0\}$ *and we call* $L$ monic *if* $a_{\mathrm{ord}(L)} = 1$. *For any* $L \in \mathbb{F}[\delta]$ *as in 3.1 we obtain a* linear differential equation *of the form*

$$L(y) = a_n\delta^n(y) + a_{n-1}\delta^{n-1}(y) + \ldots + a_1\delta(y) + a_0y = 0$$

*whereas* $y$ *is a variable.*
*For any differential ring extension* $(\mathfrak{R}, \delta)$ *of* $(\mathbb{F}, \delta)$ *and* $L \in \mathbb{F}[\delta]$ *we define the* solution space (of $L(y) = 0$ in $\mathfrak{R}$) *by*

$$\mathrm{Soln}_{\mathfrak{R}}(L) := \mathrm{Soln}_{\mathfrak{R}}\big(L(y) = 0\big) := \{v \in \mathfrak{R} \mid L(v) = 0\} \ .$$

Later on in Chapter 4 we will further investigate the properties of the ring $\mathbb{F}[\delta]$. Factorizations in this ring will turn out to be crucial to compute an first approximation on the differential Galois group.

**Definition 3.5.** *Let $L \in \mathbb{F}[\delta]$ be of order $n$ and $(\mathfrak{R}, \delta)$ any differential ring extension of $(\mathbb{F}, \delta)$. Any set $\{y_1, \ldots, y_n\} \subseteq \mathfrak{R}$ that is linearly independent over $\mathbb{F}_0$ and satisfies $L(y_1) = 0$, $\ldots, L(y_n) = 0$ is called a* fundamental set of solutions *for the linear differential equation $L(y) = 0$.*
*Any fundamental set of solutions is a basis of* $\mathrm{Soln}_{\mathfrak{R}}(L)$.

**Definition 3.6.** *Let $\delta(Y) = AY$ be a matrix differential equation with $A \in \mathbb{F}^{n\times n}$ and $v_0 \in \mathbb{F}^n$ a vector. Define for $i = 0, \ldots, n$ the elements $v_i = Av_{i-1} + v'_{i-1} \in \mathbb{F}^n$.*
*We call $v_0$ a* cyclic vector (for $A$) *if and only if* $\det(v_0, \ldots, v_{n-1}) \neq 0$.

The following lemma shows that problems and properties about matrix differential equations can be translated to differential operators and back.

**Lemma 3.7.** *[vdPS03, p. 8][vdPS03, Proposition 2.9] Let $(\mathbb{F}, \delta)$ be a differential field. For any monic linear differential operator $L \in \mathbb{F}[\delta]$ of order $n$ as in Equation 3.1 (thus $a_n = 1$) we can assign a matrix differential equation $\delta(Y) = A_L Y$. Here $A_L$ is the* companion matrix *defined as*

$$A_L = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & \ldots & \ldots & -a_{n-1} \end{pmatrix} .$$

*This induces for any differential ring extension $(\mathfrak{R}, \delta) \geq (\mathbb{F}, \delta)$ an isomorphism of the solution spaces as follows:*

$$\begin{aligned} \mathrm{Soln}_{\mathfrak{R}}(L) &\to \mathrm{Soln}_{\mathfrak{R}}(A_L) \\ v &\mapsto \big(v, \delta(v), \ldots, \delta^{n-1}(v)\big)^T \end{aligned}$$

*On the other hand, let $v_0$ be a cyclic vector for any matrix differential equation given by $A \in \mathbb{F}^{n\times n}$. Furthermore define $C = (v_0, \ldots, v_n) \in \mathbb{F}^{n\times n}$ with $v_i$ as in Definition 3.6. Then $A$ is similar to a matrix $B \in \mathbb{F}^{n\times n}$, which is the companion matrix of some linear differential operator $L \in \mathbb{F}[\delta]$. In particular we have*

$$B = C^{-1}AC - C^{-1}\delta(C) .$$

**Lemma 3.8.** *[Kat87] Let $(\mathbb{F}, \delta)$ be a differential field. If $\delta$ is not trivial (in particular there is an element $a \in \mathbb{F}$ with $\delta(a) = 1$), then cyclic vectors for any matrix differential equation exist and can be computed.*

## 3.2 Picard-Vessiot Extensions

In this section we fix a differential field $(\mathbb{F}, \delta)$ of characteristic zero and assume $\mathbb{F}_0 = \ker(\delta)$ to be algebraically closed.

**Definition 3.9.** *Given a matrix differential equation $\delta(Y) = AY$ with $A \in \mathbb{F}^{n\times n}$, we call a differential ring extension $(\mathfrak{K}, \delta) \geq (\mathbb{F}, \delta)$ a* Picard-Vessiot ring over $\mathbb{F}$ for $\delta(Y) = AY$ *if and only if the following requirements are satisfied:*

- *The differential ring $\mathfrak{K}$ is simple.*
- *There exists a fundamental matrix $F \in \mathrm{GL}_n(\mathfrak{K})$ for $\delta(Y) = AY$.*
- *As a ring $\mathfrak{K}$ is generated by $\mathbb{F}$, the entries of the fundamental matrix $F$ and $\det(F)^{-1}$.*

To see what the similar notion for linear differential equations would be, we need to define another concept:

**Definition 3.10.** *For any differential ring $(\mathfrak{R}, \delta)$ and $y_1, \ldots, y_n \in \mathfrak{R}$ define the* Wronskian matrix *of $y_1, \ldots, y_n$ as*

$$\mathrm{Wr}(y_1, \ldots, y_n) = \begin{pmatrix} y_1, & y_2 & \ldots & y_n \\ \delta(y_1) & \delta(y_2) & \ldots & \delta(y_n) \\ \vdots & \vdots & \ldots & \vdots \\ \delta^{n-1}(y_1) & \delta^{n-1}(y_2) & \ldots & \delta^{n-1}(y_n) \end{pmatrix}$$

**Lemma 3.11.** *[vdPS03, Lemma 1.12] For any $y_1, \ldots, y_n \in \mathbb{F}$ we have: The set $\{y_1, \ldots, y_n\}$ is $\mathbb{F}_0$-linearly independent if and only if $\mathrm{Wr}(y_1, \ldots, y_n) \neq 0$.*

**Definition 3.12.** *Given a linear differential operator $L \in \mathbb{F}[\delta]$ of order $n$, we call a differential ring extension $(\mathfrak{K}, \delta) \geq (\mathbb{F}, \delta)$ a* Picard-Vessiot ring over $\mathbb{F}$ for $L(y) = 0$ *if and only if the following requirements are satisfied:*

- *The differential ring $\mathfrak{K}$ is simple.*
- *There exists a $\mathbb{F}_0$-linearly independent subset $\{y_1, \ldots, y_n\} \subseteq \mathfrak{K}$ with $L(y_i) = 0$ for $i = 1, \ldots, n$.*
- *As a ring $\mathfrak{K}$ is generated by $\mathbb{F}$, $\det(\mathrm{Wr}(y_1, \ldots, y_n))^{-1}$ and $\delta^j(y_i)$ for $i = 1, \ldots, n$ and $j = 0, \ldots, n-1$.*

**Remark 3.13.** *The Picard-Vessiot extension of a linear differential operator $L$ is exactly the Picard-Vessiot extension obtained from the definition of Picard-Vessiot extension for the matrix differential equation $\delta(Y) = A_L Y$ where $A_L$ is the companion matrix of $L$.*
*Conversely, given a matrix $A \in \mathbb{F}^{n \times n}$, then $A$ is similar to a matrix $B$, which is the companion matrix of a linear differential operator $L$. Since the Picard-Vessiot rings of $\delta(Y) = AY$ and $\delta(Y) = BY$ coincide, the Picard-Vessiot rings corresponding to $\delta(Y) = AY$ and $L(y) = 0$ are isomorphic.*
*For this reason we will not distinguish Picard-Vessiot rings for matrix differential equations from Picard-Vessiot rings for linear differential equations.*
*Moreover we will just say "$\mathbb{K}$ is a Picard-Vessiot field" if $\mathbb{K}$ is the Picard-Vessiot field of some linear differential operator or matrix differential equation.*

**Theorem 3.14.** *[vdPS03, Lemma 1.17, Proposition 1.12] Given a linear differential equation $L(y) = 0$ with $L \in \mathbb{F}[\delta]$, then Picard-Vessiot rings for $L(y) = 0$ exists, have no zero divisors and are unique up to isomorphism. The constants of any such Picard-Vessiot ring equal $\mathbb{F}_0$.*

**Definition 3.15.** *Let $(\mathfrak{K}, \delta)$ be a Picard-Vessiot ring over $\mathbb{F}$ for a linear differential equation $L(y) = 0$ with $L \in \mathbb{F}[\delta]$. The field of fractions of $\mathfrak{K}$ will be called a* Picard-Vessiot field *for $L(y) = 0$.*

One can show that the constants of $\mathbb{K}$, which are defined as the kernel of $\delta \colon \mathbb{K} \to \mathbb{K}$, equal $\mathbb{F}_0$ (see [vdPS03, Proposition 1.22]).

## 3.3 The Differential Galois Group

Again fix a differential field $(\mathbb{F}, \delta)$ of characteristic zero and assume $\mathbb{F}_0 = \ker(\delta)$ to be algebraically closed.

**Definition 3.16.** *Let $L(y) = 0$ be a linear differential equation with $L \in \mathbb{F}[\delta]$ and $\mathbb{K}$ a Picard-Vessiot field. We define the differential Galois group* $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *of $L(y) = 0$ via*

$$\mathrm{Gal}(\mathbb{K}/\mathbb{F}) := \{\sigma \colon \mathbb{K} \to \mathbb{K} \mid \sigma \text{ is an } \mathbb{F}\text{-algebra automorphism and } \sigma \circ \delta = \delta \circ \sigma\} \ .$$

**Theorem 3.17.** *[vdPS03, Proposition 1.34] Let $L \in \mathbb{F}[\delta]$ and $\mathbb{K}$ a Picard-Vessiot field for $L(y) = 0$ over $\mathbb{F}$. Furthermore let $\mathscr{G}$ be the differential Galois group* $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *and define the two sets*

$$\mathfrak{S} := \{\mathscr{H} \mid \mathscr{H} \text{ is a closed subgroup of } \mathscr{G}\}$$
$$\mathfrak{T} := \{\mathbb{M} \mid \mathbb{F} \subseteq \mathbb{M},\ \mathbb{M} \text{ is a differential subfield of } \mathbb{K}\} \ .$$

*We obtain two maps*

$$\alpha \colon \mathfrak{S} \to \mathfrak{T},\ \mathscr{H} \mapsto \mathbb{K}^{\mathscr{H}}$$
$$\text{and } \beta \colon \mathfrak{T} \to \mathfrak{S},\ \mathbb{M} \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{M})$$

*whereas $\mathbb{K}^{\mathscr{H}} := \{a \in \mathbb{K} \mid \forall \sigma \in \mathscr{H} \colon \sigma(a) = a\}$ and*
$\mathrm{Gal}(\mathbb{K}/\mathbb{M}) := \{\sigma \in \mathscr{G} \mid \forall a \in \mathbb{M} \colon \sigma(a) = a\}$ *for $\mathscr{H} \in \mathfrak{S}$ and $\mathbb{M} \in \mathfrak{T}$. Let $\mathscr{G}^\circ$ be the identity component of $\mathscr{G}$. Then the following statements hold:*

- *The maps $\alpha$ and $\beta$ are inverse to each other.*
- *If $\mathscr{H}$ is a closed normal subgroup of $\mathscr{G}$, then $\mathbb{K}^{\mathscr{H}}$ is a Picard-Vessiot field of $\mathbb{F}$ with Galois group equal to $\mathscr{G}/\mathscr{H}$.*
- *The field $\mathbb{K}^{\mathscr{G}^\circ}$ is a finite Galois extension with Galois group $\mathscr{G}/\mathscr{G}^\circ$.*

**Proposition 3.18.** *Let $A \in \mathbb{F}^{n \times n}$ and $\mathbb{K}$ a Picard-Vessiot field for $\delta(Y) = AY$ over $\mathbb{F}$. Fix a fundamental matrix $F \in \mathrm{GL}_n(\mathbb{F}_0)$. There exists a faithful linear representation $\varphi \colon \mathrm{Gal}(\mathbb{K}/\mathbb{F}) \to \mathrm{GL}_n(\mathbb{F}_0)$ given via $\sigma \mapsto F^{-1}\sigma(F)$.*

*Proof.* For any $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ the computation

$$\delta(\sigma(F)) = \sigma(\delta(F)) = \sigma(AF) = A\sigma(F)$$

shows what $\sigma(F)$ is fundamental solution matrix for $\delta(Y) = AY$. By Proposition 3.3 we have $\sigma(F) = F \cdot C$ for some $C \in \mathrm{GL}_n(\mathbb{F}_0)$ and hence $F^{-1}\sigma(F) \in \mathrm{GL}_n(\mathbb{F}_0)$.
If $\varphi(\sigma)$ is the identity matrix for some $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ then $\sigma(F) = F$. Since $\mathbb{K}$ is generated by the entries of $F$ and the inverse of its determinant, we see that $\sigma$ fixes every element of $\mathbb{K}$ and thus is the identity map. Hence $\varphi$ is injective.
The following calculation for arbitrary $\sigma, \tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ shows that $\varphi$ is a group homomorphism:

$$\begin{aligned}\varphi(\sigma\tau) &= F^{-1}\sigma\tau(F) \\ &= F^{-1}\sigma(F\varphi(\tau)) \\ &= F^{-1}\sigma(F)\varphi(\tau) \\ &= F^{-1}F\varphi(\sigma)\varphi(\tau) \ .\end{aligned}$$

□

There is an alternative description of the differential Galois group

**Proposition 3.19.** *[Beu00] Let $A \in \mathbb{F}^{n\times n}$, $\mathbb{K}$ a Picard-Vessiot field for $\delta(Y) = AY$ over $\mathbb{F}$ and $\varphi(\mathscr{G})$ be the image of the differential Galois group* $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *in* $\mathrm{GL}_n(\mathbb{F}_0)$*. Let $F$ be a fundamental matrix for $\delta(Y) = AY$.*
*Recall from Section 2.1 that $\mathscr{G}$ acts on the polynomial ring $\mathbb{F}_0[X_{n,n}]$ in $n^2$ variables via $\rho$. We use a similar action on $\mathbb{F}[X,t]$:*

$$\begin{aligned}\rho\colon \mathscr{G}\times\mathbb{F}[X,t] &\mapsto \mathbb{F}[X,t]\\ (g, f(X,t)) &\mapsto f(X\cdot g,\ \det(g)^{-1}\cdot t)\end{aligned}$$

*Set $P := \{p \in \mathbb{F}[X,t] \mid p(F) = 0\}$, then $\varphi(\mathscr{G}) = \left\{C \in \mathrm{GL}_n(\mathbb{F}) \;\middle|\; P^C = P\right\}$ with $P^C = \{\rho(C,p) \mid p \in P\}$.*

## 3.4 Exponential Field extensions

Fix a differential field $(\mathbb{F},\delta)$ and a Picard-Vessiot extension $(\mathbb{K},\delta)$ of the former.

**Definition 3.20.** *Fix a differential operator $L \in \mathbb{F}[\delta]$. An element $a \in \mathbb{F}$ with $L(a) = 0$ is called* rational solution of $L$.
*An element $e \in \mathbb{K}$ is called an* exponential element over $\mathbb{F}$ *if and only if $\delta(e)\cdot e^{-1} \in \mathbb{F}$. An exponential element $e$ is called an* exponential solution of $L$ *if and only if $L(e) = 0$.*
*Let $(\mathbb{E},\delta)$ be a differential field extension of $(\mathbb{F},\delta)$. We say that $(\mathbb{E},\delta)$ is an* exponential field extension *if and only if $\mathbb{E}$ is generated by a finite number of elements $e_1,\dots,e_k \in \mathbb{K}$, which are exponential elements over $\mathbb{F}$.*

**Lemma 3.21.** *Let $\mathscr{G}$ be a subgroup of* $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *and $e \in \mathbb{K}$. The fraction $\frac{\delta(e)}{e}$ is $\mathscr{G}$-invariant if and only if $\sigma \mapsto \sigma(e)e^{-1}$ is a character of $\mathscr{G}$.*

*Proof.* The calculation, for any $\sigma \in \mathscr{G}$ proves the equivalence:

$$\begin{aligned}\delta\left(\frac{\sigma(e)}{e}\right) &= \frac{\delta(\sigma(e))e - \delta(e)\sigma(e)}{e^2}\\ &= \frac{\delta(\sigma(e))}{\sigma(e)}\frac{\sigma(e)}{e} - \frac{\delta(e)}{e}\frac{\sigma(e)}{e}\\ &= \frac{\sigma(e)}{e}\left(\sigma\left(\frac{\delta(e)}{e}\right) - \frac{\delta(e)}{e}\right)\ .\end{aligned}$$

□

**Remark 3.22.** *Lemma 3.21 is a generalization of [vdPS03, Lemma 4.8]. Note that $\frac{\delta e}{e}$ is* $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$*-invariant if and only if $e$ is exponential over $\mathbb{F}$.*

The following results can be found in [Abr89, Section 1] (or [vdPS03, Chapter 4.1] and [CW04a, Section 2.1]).

**Theorem 3.23.** *Given $L \in \mathbb{C}(x)[\delta]$ with $\delta = \frac{d}{dx}$, one can compute all rational solutions of $L$.*
*Furthermore one can compute all exponential solutions $e$ of $L$ such that $\frac{\delta(e)}{e}$ lies in the algebraic closure of $\mathbb{C}(x)$.*

Algorithms to compute rational and exponential solutions (over algebraic extensions of $\mathbb{Q}(x)$) are implemented in many common computer algebra systems. The author does not know about an implementation of the second part, the computation of exponential solutions over $\overline{\mathbb{Q}(x)}$.

# Chapter 4

# Linear Differential Equations

In this chapter fix an arbitrary differential field $(\mathbb{F}, \delta)$ of characteristic zero.
Recall the Definition 3.4: Multiplication in $\mathbb{F}[\delta]$ is induced via

$$\delta \cdot a = \delta(a) + a \cdot \delta \text{ for all } a \in \mathbb{F} .$$

Furthermore note that $\mathbb{F}[\delta]$ has no nontrivial zero divisors, since for any $K, L \in \mathbb{F}[\delta]$ we have

$$\operatorname{ord}(K \cdot L) = \operatorname{ord}(K) + \operatorname{ord}(L) .$$

In this chapter we further investigate the ring structure of $\mathbb{F}[\delta]$.
Irreducible factorizations of differential operators can be computed and are unique up to a certain equivalence relation on $\mathbb{F}[\delta]$. Furthermore, given a fixed factorization in irreducible factors, every other factorization is obtained by a process called transposition.
The main goal of this chapter is to give a method to decide and compute whether a transposition of two irreducible factors is possible.
This allows us to compute all right hand factors for a certain large class of differential operators.
Many of the mentioned computations and algorithms are already implemented in common computer algebra systems (CAS). In Section 6.1 we give a list of implementations in the CAS *Maple*.

## 4.1 Division and least common multiplies

### 4.1.1 (Right-hand) division

**Proposition 4.1.** *The ring $\mathbb{F}[\delta]$ is a right Euclidean ring with respect to* ord. *That is, given $L_1, L_2 \in \mathbb{F}[\delta]$ with $\operatorname{ord}(L_1) \geq \operatorname{ord}(L_2)$ there exists unique $Q, R \in \mathbb{F}[\delta]$ with $L_1 = QL_2 + R$ and $\operatorname{ord}(R) < \operatorname{ord}(L_2)$.*

*Proof.* Assume we are given two elements in $\mathbb{F}[\delta]$ denoted by

$$L_1 = \sum_{i=0}^{n_1} a_i \delta^i \text{ and } L_2 = \sum_{j=0}^{n_2} b_j \delta^j$$

with $n_1 > n_2$ and $a_i, b_j$ for $i = 0, \ldots, n_1$ and $j = 0, \ldots, n_2$. Now

$$L_3 \coloneqq L_1 - a_0 \delta^{n-m} ({b_0}^{-1}) \delta^{n_1 - n_2} L_2 \in \mathbb{F}[\delta]$$

is of lower degree as $L_1$. Proceeding with $L_3$ and $L_2$ in the same fashion we obtain, after $n_1 - n_2 + 1$ steps, a representation

$$L_1 = QL_2 + R$$

with $Q, R \in \mathbb{F}[\delta]$, $\operatorname{ord}(R) < \operatorname{ord}(L_2)$ and $\operatorname{ord}(Q) = n_1 - n_2$. □

**Remark 4.2.** *The computations in the proposition above can also be found in [Poo60, Chapter III, §9]. It is noteworthy that a left-hand division also exists and can be proven in a similar fashion (see for example [Ore33]). Since we will almost entirely rely only on right-hand division, we will drop the prefix 'right-hand'.*

**Definition 4.3.** *For $L_1, L_2 \in \mathbb{F}[\delta]$ we say, that $L_2$* divides *$L_1$* (from the right) *if and only if*

$$\exists Q \in \mathbb{F}[\delta] : L_1 = QL_2 \ .$$

*In this case we write $L_1 L_2^{-1} := Q$.*
*A differential operator $L \in \mathbb{F}[\delta]$ of order $n$ is* irreducible *or* prime *if and only if every differential operator $K \in \mathbb{F}[\delta]$ dividing $L$ has order $n$ or $0$.*

**Definition 4.4.** *Let $L_1, L_2 \in \mathbb{F}[\delta]$ be two monic linear differential operators. We say $L_1$ and $L_2$ are* relatively prime *if and only if there is no linear differential operator of positive order dividing both on the right.*

The following three lemmata show how divisibility relates to differential equations. They are well-known and variants of these can be found in [Sin96].

**Lemma 4.5.** *Let $L_1, L_2 \in \mathbb{F}[\delta]$ and let $\mathbb{K}$ be some Picard-Vessiot field containing a fundamental set of solutions for $L_1$ and $L_2$. If $\operatorname{Soln}_{\mathbb{K}}(L_2) \subseteq \operatorname{Soln}_{\mathbb{K}}(L_1)$, then $L_2$ divides $L_1$ from the right.*

*Proof.* Divide $L_1$ by $L_2$:

$$L_1 = QL_2 + R \qquad \text{with } Q, R \in \mathbb{F}[\delta] \text{ and } \operatorname{ord}(R) < \operatorname{ord}(L_2) \ .$$

This equation shows that every solution of $L_2$ is a solution of $R$. But $R$ has at most $\operatorname{ord}(L_2)-1$ $\mathbb{F}_0$-linearly independent solutions, thus $R = 0$. □

**Remark 4.6.** *Later we will see that there always is a Picard-Vessiot field that contains the solution spaces of any finite number of given differential operators. We define a respective operator in the next section.*

**Lemma 4.7.** *Let $L \in \mathbb{F}[\delta]$ be a linear differential operator with solution space $V$ in its Picard-Vessiot field $\mathbb{K}$. Furthermore let $\mathscr{G}$ be the differential Galois group of $\mathbb{K}$ over $\mathbb{F}$. If $W$ is a finite dimensional $\mathbb{F}_0$-vector space with $W \subseteq \mathbb{K}$, then $\mathscr{G}W \subseteq W$ if and only if there exists $K \in \mathbb{F}[\delta]$ with $\operatorname{Soln}_{\mathbb{K}}(K) = W$.*

*Proof.* $\underline{\Rightarrow}$**:** Pick a basis $w_1, \ldots, w_k$ of $W$ and define the differential operator

$$K(y) := \frac{\operatorname{Wr}(y, w_1, \ldots, w_k)}{\operatorname{Wr}(w_1, \ldots, w_k)} \ .$$

Then we have $W = \mathrm{Soln}_{\mathbb{K}}(K)$, thus there is only left to show, that $K \in \mathbb{F}[\delta]$: Rewrite $K(y) = \sum_{i=0}^{k} a_i \delta^i(y)$ then each $a_i$ is of the form

$$a_i = \frac{(-1)^{k+1+i}}{\mathrm{Wr}(w_1, \dots, w_k)} \det\left(\delta^\alpha(w_\beta)\right)_{\substack{0 \le \alpha \le k \\ 1 \le \beta \le k \\ \alpha \neq i}} \qquad \text{for } i = 0, \dots, k \ .$$

Since $\mathbb{K}^{\mathscr{G}} = \mathbb{F}$ it suffices to show that $g(a_i) = a_i$ for $i = 0, \dots, k$ and all $g \in \mathscr{G}$.
In the proof of Corollary 2.28 we saw that every $g \in \mathscr{G}$ maps a basis of $W$ to a basis of $W$. So there exists a matrix $B \in \mathrm{GL}_k(\mathbb{F}_0)$ with $g(w_i) = \big((w_1, \dots, w_k)B\big)_i = \sum_{j=1}^{k} B_{i,j} w_j$ for $i = 1, \dots k$. Note that also $B\delta^\alpha(w_\beta) = \sum_{j=1}^{k} B_{\beta,j} \delta^\alpha w_j$ for each $0 \le \alpha \le k$ and $1 \le \beta \le k$ and therefore

$$\begin{aligned}
g(a_i) =& \frac{(-1)^{k+1+i}}{\mathrm{Wr}(gw_1, \dots, gw_k)} \det\left(g\delta^\alpha(w_\beta)\right)_{\alpha \neq i} \\
=& \frac{(-1)^{k+1+i}}{\mathrm{Wr}(\sum_{j=1}^{k} B_{1,j} w_j, \dots, \sum_{j=1}^{k} B_{k,j} w_j)} \det\left(\sum_{j=1}^{k} B_{\beta,j} \delta^\alpha(w_j)\right)_{\alpha \neq i} \\
=& \frac{(-1)^{k+1+i}}{\det(B)\,\mathrm{Wr}(w_1, \dots, w_k)} \det\left(\delta^\alpha(w_\beta)\right)_{\alpha \neq i} \det(B) \\
=& a_i \qquad \text{for } i = 1, \dots k \ .
\end{aligned}$$

$\underline{\Leftarrow}$**:** Let $w \in W$ and $g \in \mathscr{G}$ be arbitrary. If we rewrite $K(y) = \sum_{i=0}^{k} a_i \delta^i(y)$ with $a_i \in \mathbb{F}$ for $i = 1, \dots, k$, then

$$\begin{aligned}
K(gw) =& \sum_{i=0}^{k} a_i \delta^i(gw) \\
=& \sum_{i=0}^{k} a_i g(\delta^i(w)) \\
=& g\left(\sum_{i=0}^{k} a_i \delta^i(w)\right) \\
=& g(K(w)) = g(0)
\end{aligned}$$

since $K(w) = 0$ and therefore $gw \in W$. □

**Lemma 4.8.** *Let $L \in \mathbb{F}[\delta]$ with Picard-Vessiot field $\mathbb{K}$ and $\mathscr{G}$ be the differential Galois Group, then the following are equivalent:*

*1) $L$ is irreducible.*

*2) $\mathscr{G}$ acts irreducibly on* $\mathrm{Soln}_{\mathbb{K}}(L)$.

*Proof.* $\underline{1 \Rightarrow 2:}$ Assume that there exists a $\mathscr{G}$-invariant subspace $W \subseteq \mathrm{Soln}_{\mathbb{K}}(L)$. Pick $L'$ according to Lemma 4.5 such that $\mathrm{Soln}(L') = W$. Then by Lemma 4.5 $L'$ is a factor of $L$, contradicting our assumption.
$\underline{2 \Rightarrow 1:}$ If $L'$ divides $L$ from the right, we have by Lemma 4.5 that $\mathrm{Soln}_K(L')$ is a $\mathscr{G}$-invariant subspaces of $\mathrm{Soln}(L)$. By irreducibility we have $L' = L$ or $L' \in \mathbb{F}$. □

### 4.1.2 Least Common Left Multiplies

The Euclidean algorithm allows to construct greatest common right divisor and least common left multiplies of linear differential operators. It seems more natural to start with the former although the later will turn out to be more useful.

**Definition 4.9.** *As $\mathbb{F}[\delta]$ is a right Euclidean ring, we have a Euclidean algorithm. Given $L_1, L_2 \in \mathbb{F}[\delta]$, we denote the result of the Euclidean algorithm by* $\mathrm{GCRD}(L_1, L_2)$ *and call it the* greatest common right divisor of $L_1$ and $L_2$. *We assume* $\mathrm{GCRD}(L_1, L_2)$ *to be monic. To compute* $\mathrm{GCRD}(L_1, L_2)$ *explicitly (with* $\mathrm{ord}(L_1) \geq \mathrm{ord}(L_2)$*) one computes a chain of divisions as follows:*

$$L_1 = Q_1 L_2 + L_3 \qquad \text{with } \mathrm{ord}(L_3) < \mathrm{ord}(L_2), \tag{4.1}$$
$$L_2 = Q_2 L_3 + L_4 \qquad \text{with } \mathrm{ord}(L_4) < \mathrm{ord}(L_3), \tag{4.2}$$
$$\ldots\ldots, \tag{4.3}$$
$$L_{r-2} = Q_{r-2} L_{r-1} + L_r \quad \text{with } \mathrm{ord}(L_r) < \mathrm{ord}(L_{r-1}), \tag{4.4}$$
$$L_{r-1} = Q_{r-1} L_r. \tag{4.5}$$

*This chain of divisions stops as soon as no remainder occurs. Normalize $L_r$ if it is not monic. Then the greatest common right divisor of $L_1$ and $L_2$ is $L_r$.*

**Proposition 4.10.** *Given $L_1, L_2, K \in \mathbb{F}[\delta]$, the differential operator $K$ is the greatest common right divisor of $L_1$ and $L_2$ if and only if the following three properties are satisfied:*

*1) $K$ is monic,*

*2) $K$ divides $L_1$ and $L_2$ from the right and*

*3) $K$ is maximal with this property (meaning: if $\tilde{K} \in \mathbb{F}[\delta]$ satisfies 1) and 2), then* $\mathrm{ord}(K) \geq \mathrm{ord}(\tilde{K})$*).*

**Proposition 4.11.** *[Sin96, Corollary 2.4] For $L_1, L_2 \in \mathbb{F}[\delta]$ the following are equivalent:*

*1 $L_1$ and $L_2$ are relatively prime.*

*2 There exists $R, S \in \mathbb{F}[\delta] : \; RL_1 + SL_2 = 1$.*

*3 $L_1$ and $L_2$ have no common nonzero solution in any differential ring extension $(\mathfrak{R}, \delta)$ of $(\mathbb{F}, \delta)$.*

We define the least common left multiple analogously to Proposition 4.10.

**Definition 4.12.** *Given $L_1, L_2 \in \mathbb{F}[\delta]$, we call an element $M \in \mathbb{F}[\delta]$ the* least common left multiple of $L_1$ and $L_2$ *and denote it by* $\mathrm{LCLM}(L_1, L_2)$ *if and only if the following three properties are satisfied:*

*1) $M$ is monic,*

*2) $L_1$ and $L_2$ divide $M$ from the right and*

*3) $M$ is minimal with this property (meaning: if $\tilde{M}$ satisfies 1) and 2), then* $\mathrm{ord}(\tilde{M}) \geq \mathrm{ord}(M)$*).*

The existence of the least common left multiple comes from the following theorem:

**Theorem 4.13.** *[Ore33, Theorem 8] Given $L_1, L_2 \in \mathbb{F}[\delta]$, apply the Euclidean algorithm to $L_1, L_2$ and define the $L_3, \ldots, L_r$ as in equations 4.1, then*

$$\mathrm{LCLM}(L_1, L_2) = aL_{r-1}L_r^{-1}L_{r-2}L_{r-1}^{-1}\cdots L_2 L_3^{-1} L_1$$

*for some $a \in \mathbb{F}$.*

The following immediate consequence will often turn out to be useful to show maximality of a potential candidate for a greatest common right divisor (or minimality in the case of least common left multiple).

**Corollary 4.14.** *Given $L_1, L_2 \in \mathbb{F}[\delta]$ the following identity holds:*

$$\mathrm{ord}(L_1) + \mathrm{ord}(L_2) = \mathrm{ord}(\mathrm{GCRD}(L_1, L_2)) + \mathrm{ord}(\mathrm{LCLM}(L_1, L_2)) \ .$$

**Proposition 4.15.** *Given $L, L_1, L_2 \in \mathbb{F}[\delta]$, then the two following statements hold:*

*1) The least common left multiple* $\mathrm{LCLM}(L_1, L_2)$ *is unique.*

*2) If $L_1$ and $L_2$ divide $L$ from the right, then* $\mathrm{LCLM}(L_1, L_2)$ *divides $L$ from the right.*

*Proof.* 1) Assume $M_1$ and $M_2$ both elements in $\mathbb{F}[\delta]$ satisfy properties 1)-3) of Definition 4.12. That is, there exists $Q_1, Q_2, P_1, P_2 \in \mathbb{F}[\delta]$ such that

$$\begin{aligned} M_1 &= Q_1 L_1 = P_1 L_2, \\ M_2 &= Q_2 L_1 = P_2 L_2, \\ \Rightarrow (M_1 - M_2) &= (Q_1 - Q_2)A = (P_1 - P_2)B. \end{aligned}$$

Note that $a(M_1 - M_2)$ is monic for some $a \in \mathbb{F}_0$ and thus satisfies properties 1) and 2) of Definition 4.12. But $\mathrm{ord}(a(M_1 - M_2)) < \mathrm{ord}(M_1)$ together with the minimality of $M_1$ yields $M_1 = M_2$.

2) Define $M := \mathrm{LCLM}(L_1, L_2) = Q_1 L_1 = Q_2 L_2$. Divide $L$ from the right by $M$ and let $R$ be a putative remainder:

$$\begin{aligned} L &= P_1 M + R \\ &= P_1 Q_1 L_1 + R \\ &= P_1 Q_2 L_2 + R. \end{aligned}$$

This shows, that $L_1$ and $L_2$ divide $R$ from the right-hand side and $\mathrm{ord}(R) < \mathrm{ord}(M)$. $aR$ is monic for some $a \in F$ and thus satisfies properties 1) and 2) of Definition 4.12. By minimality of $M$, we have $R = 0$. □

The following corollary follows easily from Proposition 4.15 and it can also be found in [Ore32a, p.229 in the proof of Satz 6].

**Corollary 4.16.** *Given $L_1, L_2, L_3 \in \mathbb{F}[\delta]$ then the following two identities hold:*

*1)* $\mathrm{LCLM}(L_1,\ L_2)L_3 = \mathrm{LCLM}(L_1 L_3,\ L_2 L_3)$,

*2)* $\mathrm{LCLM}(L_1,\ L_2 L_3) = \mathrm{LCLM}(\mathrm{LCLM}(L_1, L_3),\ L_2 L_3)$.

*Proof.* In both parts of the proof denote the left-hand side of the equations by $M$ and the right-hand side by $N$.

1) First we show that $N$ divides $M$. Using part 2 of Proposition 4.15 it is enough to show that $L_1L_3$ and $L_2L_3$ divide $M$ from the right, which is trivial.

   Instead of showing that $M$ divides $N$, we show that $ML_3^{-1}$ divides $NL_3^{-1}$. There exists $N_1, N_2 \in \mathbb{F}[\delta]$ such that $N = \mathrm{LCLM}(L_1L_3, L_2L_3) = N_1L_1L_3 = N_2L_2L_3$ and the claim follows.

2) Define $O \coloneqq \mathrm{LCLM}(L_1, L_3)$. Again we show that $M$ divides $N$: Therefore it suffices to show that $L_1$ and $L_2L_3$ divide $N$, which is trivial. To show that $N$ divides $M$ we have to prove that $O$ and $L_2L_3$ divide $M$. This follows from the fact that $L_1, L_3$ and $L_2L_3$ divide $M$. □

## 4.2 Similarity of linear differential operators

In this section we equip the ring of differential operators with an equivalence relation, which is called *similarity*.
Many of the results mentioned here can already be found in [Ore32a]. We present new proofs and use a different notation. In Theorem 4.19 we will prove the symmetry of similarity. This can be found in [Ore32a, Satz 7]. The transitivity is proven in Proposition 4.21 and corresponds to [Ore32a, Satz 6].

**Definition 4.17.** *For monic $L_1, L_2 \in \mathbb{F}[\delta]$ and $B \in \mathbb{F}[\delta]$ and relatively prime to $L_1$, we say that $L_2$ is* the transform of $L_1$ by $B$ *or* $L_1$ is similar to $L_2$ (via $B$) *if and only if*

$$\mathrm{LCLM}(B, L_1) = L_2B \ .$$

*We write $L_1 \sim_B L_2$ or just $L_1 \sim L_2$ if this is the case*

Before stating further properties of similarity of differential operators, we explain the name and show the most important fact about similar differential operators:

**Theorem 4.18.** *[Sin96, Corollary 2.6] Given monic $L_1, L_2, B \in \mathbb{F}[\delta]$ with $L_1 \sim_B L_2$, let $\mathbb{K}$ be a Picard-Vessiot extension over $\mathbb{F}$ containing a Picard-Vessiot extensions of $L_1(y) = 0$ and of $L_2(y) = 0$ over $\mathbb{F}$ (for example let $\mathbb{K}$ be a Picard-Vessiot extension of $\mathrm{LCLM}(L_1, L_2)(y) = 0$ over $\mathbb{F}$). Furthermore let $\mathscr{G}$ be the differential Galois group of $\mathbb{K}$ over $\mathbb{F}$.*
*Then $B$ induces a $\mathscr{G}$-isomorphism from $\mathrm{Soln}_{\mathbb{K}}(L_1)$ to $\mathrm{Soln}_{\mathbb{K}}(L_2)$.*

We will now show that the notion of similarity of differential operators yields an equivalence relation on $\mathbb{F}[\delta]$. The reflexivity is obvious. In the next theorem we prove that similarity is symmetric (cf. [Ore32a, Satz 7]).

**Theorem 4.19.** *Let $L_1, L_2, B \in \mathbb{F}[\delta]$ be monic. If $L_1 \sim_B L_2$, then there exists $B_1 \in \mathbb{F}[\delta]$ such that $L_2 \sim_{B_1} L_1$.*

*Proof.* By Proposition 4.11 we know there exists $S, B_1 \in \mathbb{F}[\delta]$ such that $B_1B + (-S)L_1 = 1$. Take $X \in \mathbb{F}[\delta]$ with $\mathrm{LCLM}(B_1B, L_1) = X(SL_1 + 1)$ and note that this expression is divisible from the right by $L_1$. Hence $X = \tilde{X}L_1$ and by minimality we get $\tilde{X} = 1$ and $X = L_1$. So we obtain the following equation:

$$\mathrm{LCLM}(B_1B, L_1) = L_1(SL_1 + 1) = L_1B_1B$$

The next computation becomes easy after using Corollary 4.16:

$$\begin{aligned} L_1B_1B = \mathrm{LCLM}(B_1B, L_1) &= \mathrm{LCLM}(\mathrm{LCLM}(L_1, B)B_1B) \\ &= \mathrm{LCLM}(L_2B, B_1B) \\ &= \mathrm{LCLM}(L_2, B_1)B \end{aligned}$$

Thus we have $L_1B_1 = \mathrm{LCLM}(L_2, B_1)$. Since $L_1$ and $L_2$ have the same order, using Corollary 4.14 we see that $L_2$ and $B_1$ are prime. □

The following proposition can also be found along the lines of Ore's article. The first statement can be found at [Ore32a, bottom of p.228]. The second statement is [Ore32a, Satz 4].

**Proposition 4.20.** *Let $L_1, L_2, B$ be monic differential operators in $\mathbb{F}[\delta]$*

1) *If $L_1$ is similar to $L_2$ via $B$, then $\mathrm{ord}(L_1) = \mathrm{ord}(L_2)$.*

2) *If $L_1 \sim_B L_2$, then there exists $R \in \mathbb{F}[\delta]$ such that $\mathrm{ord}(R) < \mathrm{ord}(L_1)$ and $L_1 \sim_R L_2$.*

3) *The differential operators $L_1$ and $L_2$ are similar via $B$ if and only if $L_1$ and $B$ are relatively prime, $\mathrm{ord}(L_2) = \mathrm{ord}(L_1)$ and $L_2B = \tilde{B}L_1$ for some $\tilde{B} \in \mathbb{F}[\delta]$.*

*Proof.* 1): There exists $\tilde{B} \in \mathbb{F}[\delta]$ with

$$\mathrm{LCLM}(B, L_1) = L_2B = \tilde{B}L_1. \tag{4.6}$$

Using Corollary 4.14 and $\mathrm{GCRD}(B, L_1) = 1$ we get the first and using Equation 4.6 we get the second equality of the following chain:

$$\begin{aligned} \mathrm{ord}(\mathrm{LCLM}(B, L_1)) = \mathrm{ord}(B) + \mathrm{ord}(L_1) &= \mathrm{ord}(\tilde{B}) + \mathrm{ord}(L_1) \\ &= \mathrm{ord}(L_2) + \mathrm{ord}(B)\ . \end{aligned}$$

The first line shows $\mathrm{ord}(B) = \mathrm{ord}(\tilde{B})$ and then the second line shows $\mathrm{ord}(L_1) = \mathrm{ord}(L_2)$.
2): Assume $\mathrm{ord}(B) \geq \mathrm{ord}(L_1)$ and divide $B$ from the right by $L_1$: $B = QL_1 + R$ with $\mathrm{ord}(R) < \mathrm{ord}(L_1)$. If $L_2B = \tilde{B}L_1$ for $\tilde{B} \in \mathbb{F}[\delta]$ then

$$L_2R = (\tilde{B} - L_2Q)L_1$$

is divisible from the right by $R$ and $L_1$. Since any common factor of $L_1$ and $R$ would yield a common factor of $L_1$ and $B$, $L_1$ and $R$ are relatively prime.
It is only left to show that $L_2R = \mathrm{LCLM}(L_1, R)$. By Proposition 4.15, this follows if the order of $L_2R$ is minimal. Since $\mathrm{GCRD}(L_1, R) = 1$, the order of the least common left multiple of $L_1$ and $R$ is $\mathrm{ord}(L_1) + \mathrm{ord}(R)$ (use Corollary 4.14), which is equal to $\mathrm{ord}(L_2) + \mathrm{ord}(R)$ by 1).
3): The only if part is trivial. For the if part we only have to check that $L_2B$ has the right order (using Corollary 4.14):

$$\mathrm{ord}(L_2) + \mathrm{ord}(B) = \mathrm{ord}(L_1) + \mathrm{ord}(B) = \mathrm{ord}(\mathrm{LCLM}(L_1, B))\ .$$ □

Now we can prove that similarity of differential operators is transitive (cf. [Ore32a, Satz 6]).

**Proposition 4.21.** *Let $L_1, L_2, L_3, B, C \in \mathbb{F}[\delta]$ with $L_1 \sim_B L_2$ and $L_2 \sim_C L_3$, then $L_1 \sim_{CB} L_3$.*

*Proof.* There exists $B, C \in \mathbb{F}[\delta]$ such that

$$L_2 B = \mathrm{LCLM}(B, L_1)$$
$$L_3 C = \mathrm{LCLM}(C, L_2)$$

and $\mathrm{GCRD}(L_1, B) = \mathrm{GCRD}(L_2, C) = 1$.

$$\begin{aligned} L_3 CB &= \mathrm{LCLM}(C, L_2)B \\ &= \mathrm{LCLM}(CB, BL_2) \text{ due to Corollary 4.16} \\ &= \mathrm{LCLM}(CB, \mathrm{LCLM}(B, L_1)) \\ &= \mathrm{LCLM}(L_1, CB) \text{ again due to Corollary 4.16.} \end{aligned}$$

It remains to check that $\mathrm{GCRD}(L_1, CB) = 1 \in \mathbb{F}$. Using Corollary 4.14 we get the following equality:

$$\begin{aligned} \mathrm{ord}(L_1 CB) &= \mathrm{ord}(\mathrm{LCLM}(L_1, CB)) + \mathrm{ord}(\mathrm{GCRD}(L_1, CB)) \\ &= \mathrm{ord}(L_3) + \mathrm{ord}(C) + \mathrm{ord}(B) + \mathrm{ord}(\mathrm{GCRD}(L_1, CB)). \end{aligned}$$

By Proposition 4.20 the order of $L_1$ equals the order of $L_2$, which in turn is equal to $L_3$. Thus the order of $\mathrm{GCRD}(L_1, CB)$ must be zero. □

## 4.3 Factors and Interchangeability

In this section we will define the transposition of two differential operators. It is a well known fact that factorizations of differential operators into irreducible factors are unique up to transposition.
In the last theorem of this section we will proof that two differential operators transpose if and only if a certain equation of differential operators can be solved. That will be the starting point for an important algorithm that computes the transposition of differential operators, if it exists.

**Proposition 4.22.** *Every linear differential operator can be written as a product of irreducible linear differential operators.*

*Proof.* Let $L$ be a linear differential operator of order $n$. If $n = 0$, then $L$ cannot be factored in a non-trivial way.
If $L$ is irreducible, we are done. Otherwise $L$ can be written as product of two linear differential operators of lower order, which can be factored by induction. □

There are algorithms that compute a factorization of a linear differential operator with coefficients in $\mathbb{F}_0(x)$ for a field $\mathbb{F}_0$ into irreducible factors. The first such algorithm was introduced by [Bek94], see also [vdPS03, Chapter 4.2]. In [vH97] one can find a different method that is also implemented in the CAS *Maple*.

Unfortunately the factorization of a linear differential operator is not unique. In general there are infinitely many different factorizations of a given linear differential operator, as the following example shows:

**Example 4.23.** *Let* $(\mathbb{F},\delta)=(\overline{\mathbb{Q}}(x),\frac{d}{dx})$*, then for any* $a,b\in\overline{\mathbb{Q}}$ *we have:*

$$\begin{aligned}\delta^2 &= \delta^2+\frac{a}{a\cdot x+b}\delta-\frac{a}{a\cdot x+b}\delta+\frac{a^2}{(a\cdot x+b)^2}-\frac{a^2}{(a\cdot x+b)^2}\\ &= \delta^2+\frac{a}{a\cdot x+b}\delta-\delta\frac{a}{a\cdot x+b}-\frac{a^2}{(a\cdot x+b)^2}\\ &= \left(\delta+\frac{a}{a\cdot x+b}\right)\left(\delta-\frac{a}{a\cdot x+b}\right)\end{aligned}$$

The following theorem is well-known and can for example be found in [Ore33, Chapter II, Theorem 1], [Tsa96, Theorem 1] or [Sin96, Proposition 2.11]. It also holds in the more general context of left and right principal ideal domains (see [Duc09, Theorem 2.17]).

**Theorem 4.24.** *Let* $L\in\mathbb{F}[\delta]$ *be a monic differential operator. Assume there are two factorizations*

$$L=Q_1\cdots Q_s \qquad \text{and} \qquad L=P_1\cdots P_r\ ,$$

*with* $Q_1,\ldots,Q_s,P_1,\ldots,P_r\in\mathbb{F}[\delta]$ *monic irreducible. Then* $r=s$ *and there is a permutation* $\pi$ *such that* $Q_i$ *and* $P_{\pi(i)}$ *are similar for all* $i=1,\ldots,r$*.*

**Definition 4.25.** *Given* $L_1,L_2,K_1,K_2\in\mathbb{F}[\delta]$ *such that*

$$\begin{aligned}L_1&\sim K_1\\ L_2&\sim K_2\\ L_1L_2&=K_2K_1\end{aligned}$$

*then we call* $K_2K_1$ *a* transposition of $L_1L_2$ *and we say* $L_1$ and $L_2$ interchange *or* swap*.*

With the notion of interchangeability we can refine Theorem 4.24 as follows:

**Corollary 4.26.** *Every factorization of a linear differential operator into irreducible factors can be obtained from a fixed factorization by a finite number of transpositions of the irreducible factors.*

We will give a method to check whether two differential operators swap. This theorem with a hint to its proof can be found in [Tsa96, p. 229 upper part of left column]. It will be the starting point for the *swap*-algorithm of the next section.

**Theorem 4.27.** *Given monic and irreducible* $L_1,L_2\in\mathbb{F}[\delta]$ *with* $L_1$ *and* $L_2$ *not similar and monic* $B\in\mathbb{F}[\delta]$ *then the following are equivalent:*

*a) There exists monic differential operators* $K_1,K_2\in\mathbb{F}[\delta]$ *with* $K_2K_1$ *is the transposition of* $L_1L_2$ *and* $L_1\sim_B K_1$*.*

*b) There exists* $C\in\mathbb{F}[\delta]$ *such that* $L_2B+CL_1=1$*.*

*Proof.* a) implies b): Let $\mathbb{K}$ be a Picard-Vessiot field over $(\mathbb{F},\delta)$ for $L_1(y)=0$ and $\mathscr{G}$ its Galois group. This part of the proof will be subdivided into three steps:

1) Show that $L_1\sim_{L_2B}L_1$.

2) Identify $L_2B$ with an element of the $\mathscr{G}$-equivariant isomorphisms of $\mathrm{Soln}_{\mathbb{K}}(L_1)$.

3) The $\mathscr{G}$-equivariant isomorphisms of $\mathrm{Soln}_{\mathbb{K}}(L_1)$ are just $\mathbb{F}_0$-multiplies of the identity.

1): There exists $\tilde{B} \in \mathbb{F}[\delta]$ such that $K_1 B = \tilde{B} L_1$ and we have

$$M := L_1 L_2 B = K_2 K_1 B = K_2 \tilde{B} L_1 \ .$$

Obviously $M$ is divisible by $L_1$ and $L_2 B$ from the right. In fact $M$ is minimal with this property:
Since $L_1$ is irreducible we have $\mathrm{GCRD}(L_1, L_2 B) \in \{1, L_1\}$. Assume
$\mathrm{GCRD}(L_1, L_2 B) = L_1$, then we have $\tilde{M} := L_2 B = Q L_1$ for some $Q \in \mathbb{F}[\delta]$. Take a differential operator $X \in \mathbb{F}[\delta]$ of minimal order with $XB = YL_1$ for some $Y \in \mathbb{F}[\delta]$ and divide $L_2$ by $X$: $L_2 = AX + R$ with $A, R \in \mathbb{F}[\delta]$ and $\mathrm{ord}(R) < \mathrm{ord}(X)$. Then $R$ satisfies $RB = (Q - Y)L_1$ and is of smaller order than $X$, thus by minimality we get $R = 0$. This means, that $L_2$ is divisible $X$. By irreducibility of $L_2$ we get $L_2 = X$. We have seen that $\tilde{M}$ is the least common left multiple of $B$ and $L_1$. This in turn implies that $L_1$ and $L_2$ are similar, contradicting our assumption. So $\mathrm{GCRD}(L_1, L_2 B) = 1$ and thus $M$ is minimal (by Corollary 4.14). We have shown that $L_1 \sim_{L_2 B} L_1$.
2): In the proof of Proposition 4.20 we have seen that $L_1 \sim_{L_2 B} L_1$ implies $L_1 \sim_S L_1$, where $S$ is the remainder of $L_2 B$ divided by $L_1$. Then $S$ belongs to the following set:

$$\mathcal{E}(L_1)^* := \left\{ R \in \mathbb{F}[\delta] \mid \mathrm{ord}(R) < \mathrm{ord}(L_1) \text{ and } L_1 R \text{ is divisible by } L_1 \right\}$$

Set $V := \mathrm{Soln}_{\mathbb{K}}(L_1)$, we will now show that

$$\begin{aligned} \Psi \colon \mathcal{E}(L_1)^* &\to \mathrm{Iso}_{\mathscr{G}}(V) \\ R &\mapsto (v \mapsto Rv) \end{aligned}$$

is bijection of the following sets. Here $\mathrm{Iso}_{\mathscr{G}}(V)$ is the set of $\mathscr{G}$-equivariant automorphisms on $V$. First we check, that $\Psi$ is well-defined: Let $n = \mathrm{ord}(L_1)$, $R = \sum_{i=0}^{n-1} a_i \delta^i \in \mathcal{E}(L_1)^*$ and $v \in V$. Then we have $L_1 R(v) = Q L_1(v) = 0$ for some $Q \in \mathbb{F}[\delta]$ (since $L_1 R$ is divisible by $L_1$ from the right) and so $R(v) \in V$. Furthermore for $g \in \mathscr{G}$ we have

$$g\Psi(R)(v) = g \sum_{i=0}^{n-1} a_i \delta^i(v) = \sum_{i=0}^{n-1} a_i D^i(g(v)) = \Psi(R)(g(v))$$

(since $a_i \in \mathbb{F}$ it is fixed under the Galois-action). Furthermore we have to show that $\Psi(R)$ is an isomorphism: If $\Psi(R)(v) = R(v) = 0$ then $R$ and $L_1$ would have a common solution, thus $v = 0$ (use the irreducibility of $L_1$ and Proposition 4.11).
We will now show that $\Psi$ is bijective: Given $R_1, R_2 \in \mathcal{E}(L_1)$ such that $\Psi(R_1)(v) = \Psi(R_2)(v)$ for all $v \in V$. Define the difference $R = R_1 - R_2$ and note that its order is less than or equal to the order of $L_1$. Thus $\mathrm{Soln}(L_1) \subseteq \mathrm{Soln}(R)$ together with $\mathrm{ord}(R) < \mathrm{ord}(L_1)$ and irreducibility of $L_1$ forces $R = 0$, which shows the injectivity of $\Psi$ (use Lemma 4.5).
Take any $\psi \in \mathrm{Iso}_{\mathscr{G}}(V)$ and let $\{v_1, \ldots, v_n\}$ be a basis of $V$. Define the matrix

$$A := \mathrm{Wr}(\psi(v_1), \ldots, \psi(v_n)) \cdot \mathrm{Wr}(v_1, \ldots, v_n)^{-1}.$$

The entries of $A$ are $\mathscr{G}$-invariant and thus lie in $\mathbb{F}$. If $(a_{n-1}, \ldots, a_0)$ is the first row of $A$, then define $R := \sum_{i=0}^{n-1} a_i \delta^i \in \mathbb{F}[\delta]$. By construction is $\Psi(R)(v_i)$ the first entry of the following vector:

$$\begin{aligned} A \cdot (v_i, \delta(v_i), \ldots, &\delta^{n-1}(v_i))^T \\ &= \mathrm{Wr}(\psi(v_1), \ldots, \psi(v_n)) \cdot \mathrm{Wr}(v_1, \ldots, v_n)^{-1} (v_i, \delta(v_i) \ldots, \delta^{n-1}(v_i))^T \\ &= \mathrm{Wr}(\psi(v_1), \ldots, \psi(v_n)) (\underbrace{0, \ldots, 0}_{i-1}, 1, 0 \ldots, 0)^T \\ &= \left(\psi(v_i), \delta(\psi(v_i)), \ldots, \delta^{n-1}(\psi(v_i))\right)^T \ . \end{aligned}$$

This shows the surjectivity of $\psi$.

3): Take $\psi \in \mathrm{Iso}_{\mathscr{G}}(V)$ and let $\lambda$ be an eigenvalue (since the constants are assumed to be algebraically closed, eigenvalues exist) and $E(\lambda)$ its eigenspace. Since $\psi$ is $\mathscr{G}$-equivariant, $E(\lambda)$ is a $\mathscr{G}$-invariant subspaces of $V$. Since $E(\lambda) \neq \{0\}$ and $\mathscr{G}$ acts irreducibly on $V$ (see Lemma 4.8), we have $E(\lambda) = V$.

Putting the pieces together: We saw that the remainder of $L_2B$ divided by $L_1$ is an element in $\mathcal{E}(L_1)^* = \{f \cdot \mathrm{Id} \mid f \in \mathbb{F}_0\}$. So we can adjust $B$ by an element $f_0 \in \mathbb{F}_0$ in a way that $L_2B$ leaves a remainder of 1 when divided by $L_1$ from the right. (Note that the preimage of the identity under $\Psi$ is 1).

b) implies a): Let $B, C \in \mathbb{F}[\delta]$ be given such that $L_2B + CL_1 = 1$.
Assume that $\mathrm{ord}(B) \geq \mathrm{ord}(L_1)$ and divide $B$ by $L_1$:

$$B = QL_1 + R \text{ for some } Q, R \in \mathbb{F}[\delta] \text{ and } \mathrm{ord}(R) < \mathrm{ord}(L_1).$$

Since

$$\begin{aligned} 1 &= L_2B + CL_1 \\ &= L_2R + (L_2Q + C)L_1, \end{aligned}$$

we can without loss of generality assume that the order of $B$ is strictly smaller than the order of $L_1$. By irreducibility of $L_1$ we also get $\mathrm{GCRD}(L_1, B) = 1$. Now compute the least common left multiple $M$ of $L_1$ and $B$. There exists $K_1, Q_1 \in \mathbb{F}[\delta]$ with

$$M = K_1B = Q_1L_1$$

and $\mathrm{ord}(K_1) = \mathrm{ord}(L_1)$ (since $\mathrm{GCRD}(L_1, B) = 1$). By Proposition 4.20 we get $L_1 \sim_B K_1$. Next we show that $L_1L_2$ is divisible by $K_1$. Using Lemma 4.5, we only need to show that every solution of $K_1$ is a solution of $L_1L_2$. Let $v$ be an arbitrary element of $\mathrm{Soln}(K_1)$. By Theorem 4.18 there exists $w \in \mathrm{Soln}(L_1)$ such that $B(w) = v$.

$$\begin{aligned} L_1L_2(v) &= L_1L_2B(w) \\ &= L_1(w - CL_1w) \\ &= 0 \end{aligned}$$

Now we can divide $L_1L_2$ from the left by $K_1$: $L_1L_2 = K_2K_1$.
To finish this proof, it is sufficient for $L_2 \sim K_2$ to show that $\mathrm{GCRD}(L_2, K_1) = 1$. Assume that $\mathrm{GCRD}(L_2, K_1)$ is not trivial. Since $K_1$ and $L_2$ are irreducible, we get $L_2 = K_1$. By transitivity of $\sim$ the differential operator $L_1$ would be similar to $L_2$, which was excluded by assumption. □

The second step of part a) of the previous proof relies heavily on [Sin96, Lemma 2.5]. Part 2) and 3) can be found in [vdPS03, Proposition 2.13.(2)].

**Lemma 4.28.** *If $L_1$ and $L_2$ are irreducible, not similar and there exists $B, C \in \mathbb{F}[\delta]$ such that*

$$L_2B + CL_1 = 1 \text{ and } \mathrm{ord}(B) < \mathrm{ord}(L_1),$$

*then $B$ and $C$ are unique with respect to this property.*

*Proof.* Assume we have $B_1, B_2, C_1, C_2$, such that

$$L_2B_1 + C_1L_1 = L_2B_2 + C_2L_1 = 1$$

and thus

$$L_2(B_1 - B_2) = (C_2 - C_1)L_1 = 0 \ .$$

Assume, that $B_1 - B_2$ and $L_1$ have a common factor. By the irreducibility of $L_1$, we have $B_1 - B_2 = QL_1$. But this would imply $\text{ord}(B_1 - B_2) \geq \text{ord}(L_1)$, hence a contradiction. So $B_1 - B_2$ and $L_1$ are relatively prime. We will need this information twice.

Let $\text{LCLM}(B_1 - B_2, L_1) = X(B_1 - B_2) = YL_1$ for some monic $X, Y \in \mathbb{F}[\delta]$ and by Proposition 4.15 it divides $L_2(B_1 - B_2)$:

$$\exists \text{ monic } Q \in \mathbb{F}[\delta] : L_2(B_1 - B_2) = QX(B_1 - B_2)$$

This implies $L_2 = QX$. By assumption $L_2$ is irreducible, thus $Q \in \mathbb{F}$ or $X \in \mathbb{F}$ . If $X \in \mathbb{F}$, then $B_1 - B_2$ and $L_1$ would have a common solution, which is not the case. Therefore $Q \in \mathbb{F}$ and since $Q$ is monic $Q = 1$. This implies $X = L_1$ and we get $\text{LCLM}(B_1 - B_2, L_1) = L_2(B_1 - B_2)$. But this would imply that $L_1 \sim_{B_1 - B_2} L_2$. □

**Corollary 4.29.** *Given monic and irreducible $L_1, L_2 \in \mathbb{F}[\delta]$ that are not similar. If there exist monic $K_1, K_2 \in \mathbb{F}[\delta]$ such that $K_2K_1$ is the transposition of $L_1L_2$, then $K_1$ and $K_2$ are unique with this property.*

Also transposition behaves nicely with similarity as the following lemma shows:

**Lemma 4.30.** *[Tsa96, Proposition 3] Given monic, irreducible differential operators $L_1, L_2, K_1, K_2 \in \mathbb{F}[\delta]$ and a monic $B \in \mathbb{F}[\delta]$ such that $L_1L_2 \sim_B K_1K_2$.*
*The differential operators $L_1$ and $L_2$ swap if and only if $K_1$ and $K_2$ swap.*

## 4.4 The Swap Algorithm

In this section fix two irreducible differential operators $L_1$ and $L_2$ in $\mathbb{F}[\delta]$.
We want to determine whether $L_1$ and $L_2$ swap.
By Theorem 4.27 this is equivalent to checking whether there exist

$$B, C \in \mathbb{F}[\delta] \text{ with } L_2B + CL_1 = 1. \tag{4.7}$$

We first give a sketch of the algorithm and then explain the various steps in more detail.

**Algorithm 4.31.**
***Input:*** *$L_1, L_2 \in \mathbb{F}[D]$ irreducible*
***Output:*** *$K_1, K_2, B \in \mathbb{F}[\delta]$ with $L_1 \sim K_1$, $L_2 \sim K_2$ and $L_1L_2 = K_2K_1$ if $L_1$ and $L_2$ do interchange or $\emptyset$ if $L_1$ and $L_2$ do not interchange.*
***Instructions:***
*Step 1): Solve $L_2B + CL_1 = 1$ for $B, C \in \mathbb{F}[\delta]$ or return $\emptyset$ if no solution exists.*
*Step 2): Calculate $K_1$ such that $L_1$ divides $K_1B$ from the right and* $\text{ord}(K_1) = \text{ord}(L_1)$.
*Step 3): Define $K_2$ as $L_1L_2$ divided by $K_1$ from the right.*

**Remark 4.32.** *This algorithm is modelled after an algorithm that appeared in [Ore32b, Satz 3]. The algorithm in [Ore32b] was used to solve the homogeneous equation $L_2B + CL_1 = 0$. The swap-algorithm was implemented in Maple (see Appendix 6.3).*

### 4.4.1 Explanation and Proof of Correctness

Fix two irreducible differential operators $L_1 = \sum_{i=0}^{d_1} f_i \delta^i$ and $L_2 = \sum_{j=0}^{d_2} g_j \delta^j$ with $f_{d_1} \neq 0$ and $g_{d_2} \neq 0$ and $f_0, \ldots, f_{d_1}, g_0, \ldots, g_{d_2} \in \mathbb{F}$.

**Step 1:**

Define $B := \sum_{i=0}^{d_1-1} b_i D^i$ and $C := \sum_{j=0}^{d_2-1} c_j D^j$ with indeterminantes $b_0, \ldots, b_{d_1-1}, c_0, \ldots, c_{d_2-1}$. Now we compute

$$\begin{aligned} CL_1 &= \left( \sum_{j=0}^{d_2-1} c_j \delta^j \right) \left( \sum_{i=0}^{d_1} f_i \delta^i \right) \\ &= \sum_{j=0}^{d_2-1} \sum_{i=0}^{d_1} c_j \delta^j f_i \delta^i \\ &= \sum_{j=0}^{d_2-1} \sum_{i=0}^{d_1} c_j \left( \sum_{k=0}^{j} \binom{j}{k} \delta^k(f_i) \delta^{j-k} \right) \delta^i \\ &= \sum_{m=0}^{d_1+d_2-1} \sum_{j=0}^{d_2-1} c_j \sum_{k=0}^{j} \binom{j}{k} \delta^k(f_{m-j+k}) \delta^m \end{aligned}$$

(the last equality follows from setting $m = i + j - k$ and $f_i = 0$ for $i > d_1$) and similarly (with setting $b_i = 0$ for $i > d_1 - 1$)

$$L_2 B = \sum_{m=0}^{d_1+d_2-1} \sum_{j=0}^{d_2} g_j \sum_{k=0}^{j} \binom{j}{k} \delta^k(b_{m-j+k}) \delta^m$$

Now consider the coefficients of $\delta^0 = \mathrm{Id}, \delta, \delta^2, \ldots, \delta^{d_2+d_1-1}$ in Equation 4.7. They give a system of equations in $c_0, \ldots, c_{d_2-1}$ and $b_0, \delta(b_0), \ldots, \delta_0^{d_2}, b_1, \delta(b_1), \ldots, \delta^{d_2}(b_0), \ldots, \delta^{d_2}(b_{d_1-1})$.

**Lemma 4.33.** *The coefficients of $\delta^{d_2+d_1-1}, \ldots, \delta^{d_1}$ in Equation 4.7 give a linear system (with coefficients in $\mathbb{F}$ and derivatives of $b_0, \ldots, b_{d_1-1}$) in row echelon form for $c_0, \ldots, c_{d_2}$.*

*Proof.* If a summand of the form $c_j \delta^k(f_{m-j+k})$ occurs in the coefficient of $\delta^m$, then we have $j \geq m - d_1$. Assume otherwise $j < m - d_1$, then

$$m - j + k > m - m + d_1 + k = d_1 + k \geq d_1$$

implies $f_{m-j+k} = 0$.
So, for fixed $m$, the smallest index for the elements $c$ is $m - d_1$. Furthermore the coefficient of $c_{m-d_1}$ is $\sum_{k=0}^{m-d_1} \binom{m-d_1}{k} \delta^k(f_{d_1+k}) = f_{d_1} \neq 0$. □

This lemma allows us to exchange all occurrences of $c_0, \ldots, c_{d_2}$ by $\mathbb{F}_0$-linear expressions in

$$b_0, \delta(b_0), \ldots, \delta_0^{d_2}, b_1, \delta(b_1), \ldots, \delta^{d_2}(b_1), \ldots, \delta^{d_2}(b_{d_1-1})$$

in the Equation 4.7.
**From now on, we assume that we have done this replacement in Equation 4.7.**

**Lemma 4.34.** *Let $0 \leq m \leq d_1 - 1$, then $g_{d_2}\delta^{d_2}(b_m)$ occurs as summand in the coefficient of $\delta^m$ in Equation 4.7 and is the summand with highest $\delta$-order.*

*Proof.* First we make sure, that the substitution of the $c_0, \ldots, c_{d_2}$ does not produce any terms having any power of $\delta$ greater or equal than $d_2$:
Let $\tilde{m} \geq d_1$ and $g_j\delta^k(b_{\tilde{m}-j+k})$, a coefficient of $\delta^{\tilde{m}}$. We have the following inequality:

$$d_1 > \tilde{m} - j + k > d_1 - j + k > d_1 - d_2 + k.$$

So $d_2 > k$. Now we check the summands, which originate from $L_2B$: Since $d_2 \geq j \geq k$, we only have to assume $k = d_2$. But this implies $j = d_2$ and therefore $m - j + k = m$. □

We will now transfer the equations coming from Equation 4.7 into a matrix differential equation in $d_1d_2 + 1$ indeterminantes. Beforehand we have to fix some notation:
Define the vector $\vec{b}$ with $d_1d_2$ entries as follows

$$\vec{b} := \left(b_{d_1-1}, \delta(b_{d_1-1}), \ldots, \delta^{d_2-1}(b_{d_1-1}), b_{d_1-2}, \delta(b_{d_1-2}), \ldots, b_0, \ldots, \delta^{d_2-1}(b_0)\right) .$$

In Lemma 4.34 we have seen, that there exist polynomials $\Xi_i \in \mathbb{F}_0[x_1, \ldots, x_{d_1d_2}]$ without constant terms for $i = 0, \ldots, d_1 - 1$ such that the Equations of 4.7 are

$$\begin{aligned} \Xi_i(\vec{b}) \cdot g_{d_2} - g_{d_2}\delta^{d_2}(b_i) &= 0 \text{ for } i = 1, \ldots, d_1 - 1 \\ 1 + \Xi_0(\vec{b}) \cdot g_{d_2} - g_{d_2}\delta^{d_2}(b_0) &= 0 \end{aligned}$$

Now define $\Xi_i^j$ to be $j$-th coefficient of $\Xi_i$ (with respect to the same ordering as in the vector $\vec{b}$) and define the $d_2 \times (d_2 - 1)$-matrix

$$B := \begin{pmatrix} 0 & 1 & 0 & \ldots & \\ 0 & 0 & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 0 & & \ldots & & 0 \end{pmatrix}.$$

We can now formulate an inhomogeneous matrix differential equation as follows:

$$\delta(\vec{b}) = \tilde{A}\vec{b} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ g_{d_2}^{-1} \end{pmatrix}$$

with the matrix $\tilde{A}$ defined as

$$\underbrace{\begin{pmatrix}
\boxed{B} & & & & & & & & \\
\Xi^1_{d_1-1} & \cdots & \Xi^{d_2}_{d_1-1} & \Xi^{d_2+1}_{d_1-1} & \cdots & \Xi^{2d_2}_{d_1-1} & \cdots & \Xi^{d_2(d_1-1)+1}_{d_1-1} & \cdots & \Xi^{d_2d_1}_{d_1-1} \\
 & & & \boxed{B} & & & & & & \\
\Xi^1_{d_1-2} & \cdots & \Xi^{d_2}_{d_1-2} & \Xi^{d_2+1}_{d_1-2} & \cdots & \Xi^{2d_2}_{d_1-2} & \cdots & \Xi^{d_2(d_1-1)+1}_{d_1-2} & \cdots & \Xi^{d_2d_1}_{d_1-2} \\
 & & & & & & \ddots & & & \\
 & & & & & & & \boxed{B} & & \\
\Xi^1_0 & \cdots & \Xi^{d_2}_0 & \Xi^{d_2+1}_0 & \cdots & \Xi^{2d_2}_0 & \cdots & \Xi^{d_2(d_1-1)+1}_0 & \cdots & \Xi^{d_2d_1}_0
\end{pmatrix}}_{:=\tilde{A}}.$$

By introducing a new variable $y$, we homogenize this matrix differential equation:

$$\begin{pmatrix} \delta(\vec{b}) \\ \delta(y) \end{pmatrix} = \underbrace{\begin{pmatrix} \boxed{\tilde{A}} & \begin{matrix} 0 \\ \vdots \\ 0 \\ g_{d_2}^{-1} \end{matrix} \\ \begin{matrix} 0 & \cdots & 0 \end{matrix} & 0 \end{pmatrix}}_{:=A} \begin{pmatrix} \vec{b} \\ y \end{pmatrix} \tag{4.8}$$

**Definition 4.35.** *Given irreducible $L_1, L_2 \in \mathbb{F}[\delta]$, as shown above we can construct a corresponding linear matrix differential equation of the form of Equation 4.8. We call this equation the* swap obstruction equation (SOE) *of $L_1L_2$.*

By construction the rational solutions of Equation 4.8 with non-vanishing $y$-component yield rational solutions for Equation 4.7 and vice versa.
Just in this section the following definition will be become useful:

**Definition 4.36.** *Given an $n$-dimensional matrix differential equation $\delta(Y) = AY$ over the differential field $(\mathbb{F}, \delta)$. We call a matrix $Y \in \mathbb{F}^{n\times n}$ a* rational fundamental solution matrix *for $A$ if and only if the the set of non-zero columns of $Y$ is a basis for* $\mathrm{Soln}_{\mathbb{F}}(\delta(Y) = AY)$.

We reformulate Theorem 4.27 and proposition 4.20 in terms of Algorithm 4.31:

**Theorem 4.37.** *Let $L_1, L_2 \in \mathbb{F}[D]$ irreducible with* $\mathrm{ord}(L_1) = d_1$ *and* $\mathrm{ord}(L_2) = d_2$. *Furthermore let $\delta(\vec{b}, y) = A(\vec{b}, y)$ be the $(d_1d_2+1)-$dimensional swap obstruction equation(SOE) of $L_1L_2$ with $\vec{b}$ a vector of $d_1d_2$ indeterminantes and $y$ an indeterminant. Then:*

- *There exists a non-trivial rational solution $(\vec{b}, 0)^T$ of the SOE with $\vec{b} \in \mathbb{F}^{d_1d_2}$ and* $\mathrm{ord}(L_1) = \mathrm{ord}(L_2)$ *if and only if $L_1$ and $L_2$ are similar.*

- *There exists a rational solution $(\vec{b}, y)^T$ of the SOE with $\vec{b} \in \mathbb{F}^{d_1d_2}$ with $y \neq 0$ if and only if $L_1$ and $L_2$ interchange.*

**Definition 4.38.** *Introduce new variables $\lambda_1, \dots, \lambda_m$ and extend the derivation $\delta$ on $\mathbb{F}[\delta](\lambda_1, \dots, \lambda_m)$ via $\delta(\lambda_i) = 0$ for $i = 1, \dots, m$. This also allows to extend the multiplication of $\mathbb{F}[\delta]$ on $\mathbb{F}[\delta](\lambda_1, \dots, \lambda_m)$ making it a ring. We call the elements $K(\lambda_1, \dots, \lambda_m) \in \mathbb{F}[\delta](\lambda_1, \dots, \lambda_m)$* parametrized differential operators.

**Corollary 4.39.** *For irreducible $L_1$ and $L_2$ of order $d_1$ and $d_2$ there are exactly three possibilities:*

- *$L_1$ and $L_2$ do not swap.*
- *$L_1$ and $L_2$ swap and are not similar. There exist unique $K_1$ and $K_2$ with $L_1L_2 = K_2K_1$ with $L_i \sim K_i$ for $i = 1, 2$.*
- *$L_1$ and $L_2$ swap and are similar. Then $m := d_1d_2$. There exist parametrized differential operators $K_1(\lambda_1, \dots, \lambda_m), K_2(\lambda_1, \dots, \lambda_m) \in \mathbb{F}[\delta](\lambda_1, \dots, \lambda_m)$ with*

  $$L_1L_2 = K_2(\lambda_1, \dots, \lambda_m)K_1(\lambda_1, \dots, \lambda_m).$$

  *In particular $K_2(\lambda_1, \dots, \lambda_m)K_1(\lambda_1, \dots, \lambda_m)$ is a transposition of $L_1L_2$ for every choice of $\lambda_1, \dots, \lambda_m \in \mathbb{F}_0$.*

*Proof.* Assume that $L_1$ and $L_2$ swap. Let $Y$ be a rational fundamental solution matrix of the SOE corresponding to $L_1L_2$. By Lemma 4.28 we know that there is at most one column $Y_{*,i}$ in $Y$ with $Y_{n_1n_2+1,i} \neq 0$. Every entry $Y_{1+k\cdot d_1,i}$ with $k \in \mathbb{N}_0$ is a coefficient of a differential operator $B \in \mathbb{F}[\delta]$. From $B$ we can compute a differential operator $C \in \mathbb{F}[\delta]$ such that Equation 4.7 is satisfied (using Lemma 4.33).
Let $Y_{*,j}$ be another non-zero column of $Y$. In the same fashion we obtain differential operators $Q, P \in \mathbb{F}[\delta]$ with $L_2P + QL_1 = 0$. Thus we also have $L_2(B + \lambda P) + (C + \lambda Q)L_1 = 1$ for every choice of $\lambda \in \mathbb{F}_0$.
There are at most $d_1d_2$ non-zero columns with last entry not equal to zero. Each of those columns yields one parameter. □

**Step 2:**

The following lemma can be found along the lines of [Ore32a, On the bottom of p.224].

**Lemma 4.40.** *Given $L_1, B \in \mathbb{F}[\delta]$ relatively prime with $\operatorname{ord}(L_1) = n_1$ and $\operatorname{ord}(B) = m$, there exist $K_1, Q_1 \in \mathbb{F}[\delta]$ with $\operatorname{ord}(K_1) = n_1$ and $\operatorname{ord}(Q_1) = m$, such that*

$$K_1B + Q_1L_1 = 0 \ .$$

*If we require $K_1$ to be monic, then $K_1$ and $Q_1$ are unique.*

*Proof.* Let $M$ be the least common left multiple of $B$ and $L_1$. Then there exist $K_1, Q_1 \in \mathbb{F}[\delta]$ with $M = K_1B = -Q_1L_1$. Corollary 4.14 yields the right order. □

Thus given a solution $B$ for Equation 4.7, computed in step 1, we can calculate $K_1$ by just dividing $\operatorname{LCLM}(B, L_1)$ from the right by $B$.

**step 3:**

Divide $L_1L_2$ by $K_1$ from the right to obtain $K_2$.

### 4.4.2 Examples

**Remark 4.41.** *Most of the following examples were computed in Maple. Since Maple can only compute rational solutions of differential operators, but not of differential matrix equations, we have to add an extra step (recall Lemma 3.7):*
*The matrix $A$ of the SOE given by $\delta(\vec{b}, y)^T = A(\vec{b}, y)^T$ is similar to a companion matrix $A_L$ of a linear differential operator $L$. We compute the rational solutions of $L$, construct a rational fundamental solution matrix $Y_L$ for $A_L$ and transform it back to a rational fundamental solution matrix $Y$ for $A$.*

**Example 4.42.** *Let $(\mathbb{F}, \delta)$ be the differential field $(\mathbb{C}(x), \delta = \frac{d}{dx})$. Consider the two monic linear differential operators*

$$L_1 = \delta + \frac{2}{x} \text{ and } L_2 = \delta \ .$$

*We want to find $b_0, c_0 \in \mathbb{C}(x)$, such that*

$$1 = c_0 L_1 + L_2 b_0 = (c_0 + b_0)\delta + \frac{2c_0}{x} + b_0' \ .$$

*Replacing $c_0$ by $-b_0$ and adding an additional variable $y$ we can restate this problem as a specific solution of the homogeneous matrix differential equation*

$$\begin{pmatrix} b_0' \\ y' \end{pmatrix} = \begin{pmatrix} \frac{2}{x} & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b_0 \\ y \end{pmatrix}.$$

*Pick the cyclic vector $v_0 = (1,0)^T$ and $v_1 = Av_0 = (\frac{2}{x}, 1)^T$ and denote $T = \begin{pmatrix} 1 & 0 \\ \frac{2}{x} & 1 \end{pmatrix}$. We transform $A$ into a companion matrix:*

$$\begin{aligned} A_L &\coloneqq TAT^{-1} - T(T^{-1})' \\ &= \begin{pmatrix} 0 & 1 \\ \frac{-2}{x^2} & \frac{2}{x} \end{pmatrix} \end{aligned}$$

*$A_L$ corresponds to the linear differential equation*

$$\delta^2(y) - \frac{2}{x}\delta(y) + \frac{2}{x^2}y = 0$$

*with the solutions $x$ and $x^2$. So we have a fundamental solution matrix $Y_L$ for $A_L$, which transforms to a fundamental solution matrix $Y$ for $A$:*

$$\begin{aligned} Y_L &= \begin{pmatrix} x & x^2 \\ 1 & 2x \end{pmatrix} \\ Y = T^{-1}Y_L &= \begin{pmatrix} x & x^2 \\ -1 & 0 \end{pmatrix} \end{aligned}$$

*So we have the specific solution $-x$ and the homogeneous solution $x^2$, therefore for every $\lambda \in \mathbb{C}$ we have $B(\lambda) = -x + \lambda x^2$ and $C(\lambda) = -B(\lambda)$.*
*Now define $K_1 = \delta + a_0$ with $a_0 \in \mathbb{C}$. Dividing $K_1 B(\lambda)$ from the right by $L_1$ yields a remainder of*

$$-a_0 x + a_0 \lambda x^2 + 1 = 0 \ .$$

*Thus for every $\lambda$ and $\mu$ in $\mathbb{C}$ we get*

$$K_1(\lambda) = \delta - \frac{1}{\lambda - x^2 - x}$$

*and finally by dividing $L_1L_2$ by $K_1(\lambda)$*

$$K_2(\lambda) = \delta + \frac{2\lambda x - 1}{x(\lambda x - 1)} \ .$$

*We saw, that for arbitrary $\lambda \in \mathbb{C}$ we have*

$$L_1L_2 = K_2(\lambda)K_1(\lambda) \ .$$

*Since we found several homogeneous solutions and several linear differential operators interchanging with $L_1L_2$, $L_1$ and $L_2$ must be of the same type. In fact we have:*

$$L_1\left(\frac{1}{x}\delta + \frac{1}{x^2}\right) = \left(\frac{1}{x}\delta + \frac{2}{x^2}\right)L_2$$

**Example 4.43.** *We want to check if the irreducible monic linear differential operators*

$$L_1 = \delta^2 + \frac{x^3 + 7x^2 + 3x + 1}{x(x^4 + 4x^3 + 8x^2 + 6x + 1)}\delta + \frac{x^4 + 4x^3 + 7x^2 - 7x - 1}{x^3 + 3x^2 + 5x + 1}$$

*and*

$$L_2 = \delta^2 + \delta - \frac{x}{x+1}$$

*in $\mathbb{C}(x)[\delta]$ swap (again with $\delta = \frac{d}{dx}$). First we define $B := b_1\delta + b_0$ and $C := c_1\delta + c_0$ with $b_0, b_1, c_0, c_1 \in (x)$.*

$$\begin{aligned}
&CL_1 + L_2B - 1\\
=&(c_1 + b_1)\delta^3\\
&+\left(\frac{c_0x^5 + 4c_0x^4 + 8c_0x^3 + 6c_0x^2 + c_0x + c_1x^3 + 7c_1x^2 + 3c_1x + c_1}{x(x^4 + 4x^3 + 8x^2 + 6x + 1)} + b_1 + 2b_1'\right.\\
&\left.+ b_0\right)\delta^2\\
&+\left(\frac{c_0x^8 + 11c_0x^7 + 39c_0x^6 + 75c_0x^5 + 71c_0x^4 + 33c_0x^3 + 9c_0x^2 + c_0x + c_1x^9}{(x^3 + 3x^2 + 5x + 1)(+1)(x^4 + 4x^3 + 8x^2 + 6x + 1)x^2}\right.\\
&+\frac{9c_1x^8 + 37c_1x^7 + 65c_1x^6 + 43c_1x^5 - 53c_1x^4 - 119c_1x^3 - 91c_1x^2 - 26c_1x - 2c_1}{(x^3 + 3x^2 + 5x + 1)(+1)(x^4 + 4x^3 + 8x^2 + 6x + 1)x^2}\\
&\left.+\frac{-xb_1 + b_1'x + b_1' + b_0x + b_0 + b_1''x + b_1'' + 2b_0'x + 2b_0'}{x+1}\right)\delta\\
&+\left(\frac{c_0x^8 + 7c_0x^7 + 24c_0x^6 + 35c_0x^5 + 17c_0x^4 - 31c_0x^3 - 12c_0x^2}{(x^3 + 3x^2 + 5x + 1)^2x^3}\right.\\
&+\frac{-c_0x - c_1x^7 - 8c_1x^6 - 28c_1x^5 - 12c_1x^4 + 37c_1x^3}{(x^3 + 3x^2 + 5x + 1)^2x^3}\\
&\left.+\frac{82c_1x^2 + 22c_1x + 2c_1}{(x^3 + 3x^2 + 5x + 1)^2x^3}\frac{-b_0x + b_0'x + b_0' + b_0''x + b_0''}{x+1} - 1\right)
\end{aligned}$$

*Solving the coefficients of $\delta^3$ and $\delta^2$ for $c_0$ and $c_1$ yields:*

$$\begin{aligned} c_1 &= -b_1 \\ c_0 &= -\frac{7b_1x^3 - b_1x^2 - 2xb_1 - b_1 + b_1x^5 + 4b_1x^4 + 2b_1'x^5 + 8b_1'x^4 + 16b_1'x^3}{x(x^4 + 4x^3 + 8x^2 + 6x + 1)} \\ &\quad - \frac{12b_1'x^2 + 2b_1'x + b_0x^5 + 4b_0x^4 + 8b_0x^3 + 6b_0x^2 + b_0x}{x(x^4 + 4x^3 + 8x^2 + 6x + 1)} \end{aligned}$$

*The matrix $A$ for the homogeneous matrix differential equation is*

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ \frac{x^6+4x^5+10x^4+12x^3-8x-1}{x^2(x+1)(x^3+3x^2+5x+1)} & -1 & \frac{x^6+4x^5+4x^4-21x^3+13x^2+18x+3}{x^3(x^4+4x^3+8x^2+6x+1)} & \frac{2(x^4+4x^3+7x^2-7x-1)}{(x^3+3x^2+5x+1)x^2} & 1 \\ 0 & 0 & 0 & 1 & 0 \\ \frac{-(7x^3-x^2-2x-1+x^5+4x^4)}{x(x+1)(x^3+3x^2+5x+1)} & -2 & \frac{x^7+5x^6+15x^5+28x^4+2x^3-16x^2-16x-3}{x^2(x+1)^2(x^3+3x^2+5x+1)} & \frac{-(x^5+4x^4+6x^3-8x^2-5x-2)}{x(x+1)(x^3+3x^2+5x+1)} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

*and the matrix differential equation becomes*

$$\begin{pmatrix} b_0' \\ b_0'' \\ b_1' \\ b_1'' \\ y' \end{pmatrix} = A \begin{pmatrix} b_0 \\ b_0' \\ b_1 \\ b_1' \\ y \end{pmatrix} .$$

*Next we guess the cyclic vector $v_0 = \left(x+1, x-1, x, x, \frac{1}{x}\right)^T$ and define the matrix*

$$T = (v_0, v_1, v_2, v_3, v_4)^T ,$$

*where $v_i = Av_{i-1} + v_{i-1}'$ for $i = 1, \ldots, 4$. Then*

$$A_L := TAT^{-1} - T(T^{-1})'$$

*has the shape of a companion matrix and the corresponding linear differential equation has exactly one rational solution (up to $\mathbb{C}$-linear dependence):*

$$f := -\frac{-1 - 6x - 23x^2 - 11x^3 + 29x^4 + 52x^5 + 31x^6 + 11x^7 + 2x^8}{x(x^3 + 3x^2 + 5x + 1)^2}$$

*The matrix*

$$Y_L := \begin{pmatrix} f & 0 & 0 & 0 & 0 \\ f' & 0 & 0 & 0 & 0 \\ f'' & 0 & 0 & 0 & 0 \\ f^{(3)} & 0 & 0 & 0 & 0 \\ f^{(4)} & 0 & 0 & 0 & 0 \end{pmatrix}$$

*satisfies $Y_L' = A_L Y_L$ and therefore $Y := T^{-1}Y_L$ satisfies $Y' = AY$. From the entries of*

$$Y = \begin{pmatrix} -\frac{x^3+2x^2+2x+1}{x^3+3x^2+5x+1} & 0 & 0 & 0 & 0 \\ -\frac{x^4+6x^3+4x^2-2x-3}{(x^3+3x^2+5x+1)^2} & 0 & 0 & 0 & 0 \\ -\frac{x(x^2+2x+1)}{x^3+3x^2+5x+1)} & 0 & 0 & 0 & 0 \\ -\frac{x^4+8x^3+10x^2+4x+1}{(x^3+3x^2+5x+1)^2} & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

*we can read of the values for* $b_1$ *and* $b_0$ *and get*

$$B = -\frac{x^3+2x^2+2x+1}{x^3+3x^2+5x+1} - \frac{x(x^2+2x+1)}{x^3+3x^2+5x+1}\delta \ .$$

*Now set* $K_1 := \delta^2 + a_1\delta + a_0$ *and divide the product* $K_1B$ *by* $L_1$*. The remainder*

$$\frac{-(a_1x^4+a_0x^4+2a_0x^3-x^3+2a_1x^3+2a_1x^2-2x^2+a_0x^2-x+a_1x}{x(x^3+3x^2+5x+1))}\delta$$
$$+\frac{-(a_0x^4+2a_0x^3-a_1x^3-x^3-2x^2-2a_1x^2+2a_0x^2+a_0x-2x+a_1x-1+a_1}{x(x^3+3x^2+5x+1))}$$

*vanishes if and only if* $a_1(x) = 0$ *and* $a_0(x) = \frac{1}{x}$*, so*

$$K_1 = \delta^2 + \frac{1}{x} \ .$$

*Finally, dividing* $L_1L_2$ *by* $K_1$ *from the right, we get*

$$K_2 = \delta^2 + \frac{x^5+4x^4+9x^3+13x^2+4x+1}{x(x^4+4x^3+8x^2+6x+1)}\delta - \frac{3x^5+3x^4-9x^3+3x^2+8x+x^6+1}{(x+1)(x^3+3x^2+5x+1)x^2}$$

*and* $L_1L_2 = K_2K_1$ *holds. Furthermore we know that* $L_1$ *is not similar to* $L_2$*.*

### 4.4.3 The Problem of Computing all Right Hand Factors up to Similarity

In this subsection, let $\mathbb{F}$ be (an algebraic extension of) $\mathbb{Q}(x)$ and $\delta = \frac{d}{dx}$ (or any other differential field, in which one can compute solutions of differential operators).
Given a monic differential operator $L \in \mathbb{F}[\delta]$ and a factorization of $L$ into monic, irreducible factors

$$L = L_r \cdots L_1. \tag{4.9}$$

Later on, in Theorem 5.2, we will need to compute the stabilizer of all right hand factors of a certain differential operator. From Theorem 4.18 we know that similar differential operators yield the same stabilizer. So the question we need to answer is:

**Question:** How can we compute all monic right hand factors of $L$ up to similarity.

In the general case we are not able to provide a positive answer.
However there is an algorithm that provides all factorizations in some special cases. The idea for this algorithm can also be found in [Tsa96].
For any monic right hand factor $K$ of $L$, there exists a $Q \in \mathbb{F}[\delta]$ with $L = QK$. Factor $Q$ and $K$ into irreducible monic factors

$$L = \underbrace{K_r \dots K_{t+1}}_{=Q}\underbrace{K_t \dots K_1}_{=K} \ .$$

By Theorem 4.27 we know that this factorization is obtained from the initial factorization in Equation 4.9 by a finite number of transpositions.

**Corollary 4.44.** *[Tsa96, Corollary 3] If no pair of irreducible factors in Equation 4.9 is similar, then there are at most $r!$ distinct irreducible factorizations of $L$.*

So the idea is to compute all possible transpositions of our initial factorization by swapping adjacent irreducible factors.
The algorithm to computing all factorizations for differential operators having no pair of similar, irreducible factors is as follows: For every $\pi$ in the symmetric group on $r$ elements, decompose $\pi$ as a product of transpositions (in the usual sense): $\pi = (a_{2h}\ a_{2h-1}) \cdots (a_2\ a_1)$ for some $h \in \mathbb{N}$ and $\{a_1, \ldots, a_{2h}\} \subseteq \{1, \ldots, r\}$. Furthermore we require $(a_{2j}\ a_{2j-1})$ to be adjacent numbers, meaning $|a_{2j} - a_{2j-1}| = 1$ for $j = 1, \ldots, h$. This ensures that we will only try to swap differential operators that are adjacent in a given factorization.
Use the *swap*-algorithm to check whether $L_{a_2}$ and $L_{a_1}$ swap. If they do not swap, then $\pi$ does not give a new factorization. If they swap we obtain a new factorization of $K$. Proceed to check whether the irreducible factors on position $a_3$ and $a_4$ of this new factorization swap. Continue in the same way until all transpositions of $\pi$ have been used. Denote the irreducible factors of this factorization by $L_{\pi(i)}$ for $i = 1, \ldots, r$.
From Lemma 4.30 and Lemma 4.28 we know that this algorithm is independent of the decomposition into transpositions of the individual elements of the symmetric group. From Corollary 4.44 we know that this process gives all factorizations.
We can still apply this algorithm even if the factorization of $L$ contains a pair of similar operators, which do not swap after application of any number of transpositions. By this we mean that if $L_i$ and $L_j$ with $i < j$ are similar differential operators in Equation 4.9, then we require that for any $\pi \in S_r$ with $\pi(i) + 1 = \pi(j)$ the corresponding differential operators $L_{\pi(j)}$ and $L_{\pi(i)}$ do not swap.
We fix this observation in the following proposition:

**Proposition 4.45.** *If the factorization into irreducible factors of $L$ contains no pair of irreducible similar differential operator that swap after arbitrary number of transpositions. Then we can compute all right hand factors of $L$.*

If the factorization of $L$ has a pair of swapping similar factors, then parametrized differential operators occur (recall Definition 4.38).
In the following we will discuss the problems one encounters, when trying to apply the above approach to parametrized differential operators.

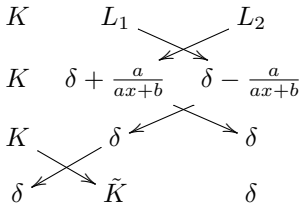
### The set of Transpositions can not be enumerated by elements of the Symmetric Group

Write down the transpositions of irreducible factors as transpositions in the symmetric group $S_r$ (as above, e.g. swapping $L_1$ with $L_2$ is denoted as (1 2)) and form the product $\pi \in S_r$ of them. If $L$ contains no irreducible, similar differential operators, then we have seen that we can recover from $\pi$ the transpositions of irreducible factors we made and get a valid factorization of $L$.
On the other hand, assume that the factorization into irreducible factors of $L$ contains a pair of similar differential operators that swap.
In this case there is no natural way to index these transpositions. In particular, we do not know when we tried all transpositions and thus when we obtained all different irreducible factorizations.
The reason for this is that, when trying to form the product in the symmetric group (on $r$ elements) as above, then cancellations may occur, as seen in the following example.

**Example 4.46.** *Define the differential operators* $K = \delta^2 - x^2\delta - 2x + 1$, $L_1 = \delta + \frac{1}{x}$ *and* $L_2 = \delta - \frac{1}{x}$. *Note that* $L_1$ *is similar to* $L_2$ *. We consider the product* $KL_1L_2$.
*One can show that* $K$ *and* $L_1$ *do not swap (using the swap-algorithm). However we can swap* $L_1$ *with* $L_2$ *and obtain parametrized differential operators* $L_1L_2 = \big(\delta + \frac{a}{ax+b}\big)\big(\delta - \frac{a}{ax+b}\big)$ *(recall example 4.23).*
*Then we can swap the right hand factor* $\delta - \frac{a}{ax+b}$ *to the left and make a choice for the new appearing parameters:*

$$\big(\delta + \frac{a}{ax+b}\big)\big(\delta - \frac{a}{ax+b}\big) = \delta\delta \ .$$

*Now we can swap* $K$ *with* $\delta$*, a differential operator, which is similar but not equal to* $L_1$*. We visualize this as follows:*




*with* $\tilde{K} = \delta^2 - x^2\delta + 1$. *The sequence corresponding to these transpositions in* $S_3$ *is*

$$(23), (23), (12) \ .$$

*The product of this sequence in* $S_r$ *is* $(12)$*, but as mentioned above,* $K$ *and* $L_1$ *do not swap.*

This also shows that a parametrized differential operator may only swap for certain parameter values with another differential operator.

### Similarity and Multiplication are not well behaved

There are differential operators $A, B, L \in \mathbb{F}[\delta]$ with $A \sim B$, $LA \not\sim LB$ and $AL \not\sim BL$.
This can be verified by application of the *swap*-algorithm to the following differential operators:

$$\begin{aligned} A &= \delta^2 + \frac{x-1}{x}\delta - \frac{x^2+1}{x}, \\ B &= \delta^2 + \delta - x, \\ L &= \delta - x \end{aligned}$$

So assume we have factored $L = QL_1L_2R$ with $Q, R \in \mathbb{F}[\delta]$ arbitrary and $L_1, L_2 \in \mathbb{F}[\delta]$ irreducible. Furthermore assume that $L_1$ and $L_2$ swap and are similar. That is, there exists parametrized differential operators

$$K_2(\underbrace{\lambda_1, \ldots, \lambda_k}_{\vec{\lambda}}), \ K_1(\underbrace{\mu_1, \ldots, \mu_k}_{\vec{\mu}}) \in \mathbb{F}(\vec{\lambda}, \vec{\mu})[\delta]$$

with $L_1L_2 = K_2(\vec{\lambda})K_1(\vec{\mu})$, $L_1 \sim K_1(\vec{\mu})$ and $L_2 \sim K_2(\vec{\lambda})$ for every $\vec{\lambda}, \vec{\mu} \in \mathbb{F}_0^k$.
Now for every choice for $\vec{\mu}_1, \vec{\mu}_2 \in \mathbb{F}_0^k$ we have $K_1(\vec{\mu}_1) \sim K_1(\vec{\mu}_2)$, but $K_1(\vec{\mu}_1)R$ must not be similar to $K_1(\vec{\mu}_2)R$.
To give a list of all right hand factors of $L$, we must compute a set $\Lambda$ of values $\vec{\mu} \in \mathbb{F}_0^k$ such that $K_1(\vec{\mu}_1)R \not\sim K_2(\vec{\mu}_2)R$ for any two elements $\vec{\mu}_1, \vec{\mu}_2 \in \Lambda$ that are not equal.

If we had a *swap*-algorithm that worked not only in $\mathbb{F}[\delta]$, but also in $\mathbb{F}(\vec{\mu})[\delta]$, we could fix $\vec{\mu}_1 \in \mathbb{F}_0^k$, add it to $\Lambda$ and compute for which values $\vec{\mu}_2$

$$K_1(\vec{\mu}_1)R \text{ and } K_2(\vec{\mu}_2)R \text{ are similar.} \tag{4.10}$$

Define the set $\mathcal{X} = \left\{\vec{\mu}_2 \in \mathbb{F}_0^k \mid \text{the statement 4.10 holds}\right\}$ and deal with the complement $\mathbb{F}_0^k \backslash \mathcal{X}$ in succession (there is no guarantee that this would terminate after a finite number of steps).

**Swapping Parametrized Differential Operators**

The *swap*-algorithm relies on the algorithm for computing rational solutions.
As seen, the transposition of similar differential operators yields parametrized differential operators, thus elements in $\mathbb{F}(\vec{\mu})[\delta]$.
If one can find an algorithm for computing rational solutions of parametrized differential operators, then the *swap*-algorithm also can be generalized to parametrized differential operators.

**A completely different approach**

In his master thesis [Hei12] A. Heinle gave an efficient algorithm to compute factorizations in Ore domains, which is implemented in the CAS *Singular*.
A generalization of the following idea can also be found in [Hei12, Theorem 3.8].
Note that $\mathbb{Q}(x)[\delta]$ is the Ore localization of $\mathbb{Q}[x][\delta]$. Using the methods of [Hei12] we can compute all right hand factors of elements in $\mathbb{Q}[x][\delta]$.
Now let $K \in \mathbb{Q}(x)[\delta]$ be an arbitrary right hand divisor of $L = QK$. There exists an element $f \in \mathbb{Q}[x]$ such that $fK \in \mathbb{Q}[x][\delta]$. Then we have the factorization $L = Q\frac{1}{f}\, fK$. By an element $g \in \mathbb{Q}[x]$ we get $gQ\frac{1}{f} \in \mathbb{Q}[x][\delta]$ and have a factorization in $\mathbb{Q}[x][\delta]$: $gL = \left(gQ\frac{1}{f}\right) \cdot \left(fK\right)$.
In particular, using Heinles algorithm to compute all right hand factors of $gL$ would also yield $K$.
Thus we can compute all right hand factors of $L$ up to similarity if and only if we can compute a finite set of polynomials $\mathfrak{P}$ having the property: For all right hand factors $K$ of $L$ exists a $g \in \mathfrak{P}$ such that $K$ is similar to a right hand factor of $gL$ in $\mathbb{Q}[x][\delta]$.

After all this discussion, the question of "How can we compute all right hand factors of a given linear differential operator up to similarity?" raised at the beginning of this section, is still open in general.

## 4.5 Tensorial Constructions with Differential Operators

Fix a differential field $(\mathbb{F}, \delta)$.
Given a linear differential operator $L \in \mathbb{F}[\delta]$ and its solution space $V$ in a Picard-Vessiot extension $\mathbb{K}$ corresponding to $L$.
Since $V$ is a vector space, we know a lot of operations to construct new objects from $V$, like $V \otimes V$ or $V \oplus V$. In this section recall that one can mimic those constructions for linear differential operators.

**Theorem 4.47.** *[Sin93, Lemma 3.2] For $L_1, L_2 \in \mathbb{F}[\delta]$ and $\mathbb{K}$ a Picard-Vessiot extension containing a fundamental set of solutions of $L_1$ and $L_2$, there are differential operators $L_3, L_4$ and $L_5$ in $\mathbb{F}[\delta]$ such that:*

*(1)* $\mathrm{Soln}_{\mathbb{K}}(L_3) = \{y_1 + y_2 \mid y_1 \in \mathrm{Soln}_{\mathbb{K}}(L_1),\ y_2 \in \mathrm{Soln}_{\mathbb{K}}(L_2)\}$.

*(2)* $\mathrm{Soln}_{\mathbb{K}}(L_4) = \{y_1 \cdot y_2 \mid y_1 \in \mathrm{Soln}_{\mathbb{K}}(L_1),\ y_2 \in \mathrm{Soln}_{\mathbb{K}}(L_2)\}$.

*(3)* $\mathrm{Soln}_{\mathbb{K}}(L_5) = \{\delta(y) \mid y \in \mathrm{Soln}_{\mathbb{K}}(L_1)\}$ .

*Proof.* In addition to the proof in [Sin93] for $L_3$, the proof for $L_4$ and $L_5$ can be found in [Sin81, Lemma 3.8]. □

**Remark 4.48.** *We already knew how to construct the differential operator $L_3$ in Theorem 4.47: $L_3$ is just the least common left multiple of $L_1$ and $L_2$.*
*Also the differential operator $L_5$ can be computed using the algorithm in Appendix 6.4.5.*

The most important construction for us will be the symmetric power of differential operators:

**Lemma 4.49.** *[vH97, Section 2.1-2.2, Proposition 4] Let $L \in \mathbb{F}[\delta]$ be a monic differential operator of order $n$ whose solution space $V$ is spanned by $\{y_1, \ldots, y_n\}$ in its Picard-Vessiot field $\mathbb{K}$. For any natural number $m$, one can construct a linear differential operator $L^{\circledS m}$ with solution space spanned by the monomials of degree $m$ in $y_1, \ldots, y_n$.*

To prove this lemma, one can also apply Theorem 4.47.(2) multiple times to $L$.

## 4.6 Regular points and Power Series Solutions

**Definition 4.50.** *For a monic linear differential operator $L(y) = \sum_{i=0}^{n} a_i(x)y^{(i)}$ with coefficients $a_i(x) \in \mathbb{C}(x)$, we call $c \in \mathbb{C}$ a* regular point *if $a_i(x)$ does not have a pole in $c$. Otherwise $c$ is called a* singular point.

**Remark 4.51.** *One can extend the notion of regular points to $\infty$ by replacing $x$ by $\frac{1}{x}$.*

**Example 4.52.** *If we set $u(x) = y(\frac{1}{x})$, then its first two derivatives are*

$$u'(x) = -\frac{1}{x^2}y'(\frac{1}{x}) \text{ and}$$
$$u''(x) = \frac{1}{x^4}y''(\frac{1}{x}) + \frac{2}{x^3}y'(\frac{1}{x}) \ .$$

*Now take the differential operator $L = \delta$. Every $a \in \mathbb{C}$ is a regular point for $L$. Next we check $a = \infty$:*
*Substituting the variable $x$ in $L(y(x)) = \delta(y(x))$ by $z = x^{-1}$ yields $L(y(z)) = -z^2\delta(y(z))$. Up to a $\mathbb{C}(z)$-multiple this is equal to $\delta$, which is regular in $a = 0$. Thus $a = \infty$ is a regular point for $L = \delta$.*
*Now consider $K = \delta^2$ at the point $a = \infty$. Again we substitute $z = \frac{1}{x}$ and get*

$$K(y(z)) = z^4\delta^2 + 2z^3\delta \ .$$

*We multiply by $\frac{1}{z^4}$ and obtain the differential operator*

$$\delta^2 + \frac{2}{z}\delta,$$

*which is singular in $a = 0$. Hence $K$ is singular in $a = \infty$.*

The following theorem a well known result of Cauchy and its proof can be found [CH11, theorem 7.1.3].

**Theorem 4.53.** *Let $L(y) = \sum_{i=0}^{n} a_{n-i}(x)y^{(i)} = 0$ be a linear differential equation with coefficients in $\mathbb{C}(x)$. Let $c$ be a regular point of $L(y) = 0$. For every $(c_0, \ldots, c_{n-1}) \in \mathbb{C}^n$ there exists a power series $f = \sum_{i=0}^{\infty} c_i(x-c)^i$ with positive convergence radius and $L(f) = 0$.*

**Corollary 4.54.** *For every regular point $c$ of $L(y) = 0$ and invertible matrix $C \in \mathbb{F}_0^{n\times}$ there exists exactly $n$ $\mathbb{C}$-linear independent power series $f_1, \ldots, f_n$ with positive convergence radius that satisfy $L(f_1) = L(f_2) = \ldots = L(f_n) = 0$.*
*In particular, the choice of a regular point for the differential operator $L$ defines a fundamental solution matrix for the companion matrix of $L$.*

**Remark 4.55.** *In most applications of Corollary 4.54 the matrix $C$ will be the identity. In that case a fundamental set of solutions of is uniquely defined via $\delta^{i-1}(y_j)(c) = \partial_{i,j}$, whereas* $\partial_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$.

## 4.7 Computing Solutions of Factors of Symmetric Powers

The theorem of Cauchy (4.53) has an important application, which can also be found in [SU97, section 4.2].

**Lemma 4.56.** *Let $L, M \in \mathbb{F}[\delta]$ be two differential operators and $\mathbb{K}$ a Picard-Vessiot field corresponding to* $\mathrm{LCLM}(L, M)$. *Assume* $\mathrm{Soln}_{\mathbb{K}}(M) \subseteq \mathrm{Soln}_{\mathbb{K}}(M)\big(\mathrm{LCLM}(L^{\circledS i} \mid i = 0, \ldots, d)\big)$ *for some $d \in \mathbb{N}_0$ and let $K \in \mathbb{F}[\delta]$ be a factor of $M$. Let $c \in \mathbb{F}_0$ be a regular point for $L$ and $K$ and $C \in \mathrm{GL}_n(\mathbb{F}_0)$. This defines a fundamental system of solutions $\{y_1, \ldots, y_n\}$ for $L$ and a fundamental system of solutions $\{z_1, \ldots, z_s\}$ for $K$ (see Corollary 4.54 and Lemma 3.7). Then one can compute polynomials $p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n) \in \mathbb{F}_0[x_1, \ldots, x_n]$ of degree less or equal to $d$ such that $\{p_1(y_1, \ldots, y_n), \ldots, p_s(y_1, \ldots, y_n)\}$ is a fundamental set of solutions for $K$.*

*Proof.* Using Theorem 4.53 compute the power series $T(y_1), \ldots, T(y_n)$ of the solutions $y_1, \ldots, y_n$ of $L$ about the regular point $c$ up to order $m$. Similarly compute the power series $T(z_1), \ldots, T(z_s)$ for the solutions $z_1, \ldots, z_s$ of $K$ about the regular point $c$ up to order $m$. Let $\{h_1, \ldots, h_m\}$ be the set of all monomials in the variables $y_1, \ldots, y_n$ of degree less or equal to $d$. By assumption there exist constants $c_{1,i}, \ldots, c_{m,i}$ such that

$$z_i = \sum_{j=1}^{m} c_{j,i} h_j \text{ for } i = 1, \ldots, s \ .$$

Obtain $T(h_j)$ from $h_j$ by replacing all occurrences of $y_i$ by $T(y_i)$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ . Also replace $z_j$ by $T(z_j)$ for $j = 1, \ldots, s$. This gives a new linear system of equations with equivalent solution:

$$T(z_i) = \sum_{j=1}^{m} c_{j,i} T(h_j) \text{ for } i = 1, \ldots, s \ .$$

□

**Remark 4.57.** *This algorithm has been implemented, see the Appendix 6.2.*

**Example 4.58.** *For* $\mathbb{F} = \mathbb{C}(x),\ \delta = \frac{d}{dx}$ *define the differential equation*

$$L(y) = \delta^2(y) - \frac{1}{2x}\delta(y) - \frac{1}{4x}y = 0.$$

*The second symmetric power of* $L$ *has a right-hand factor* $\delta(y) - \frac{y}{x-1}$*. Denote by* $y_1, y_2$ *a basis for the solution space of* $L$ *and by* $z_1$ *a basis for the solution space of this factor. Here we require* $y_1(c) = 1,\ y_2(c) = 0,\ \delta(y_1)(c) = 0,\ \delta(y_2)(c) = 1$ *and* $z_1(c) = 1$ *for a common regular point* $c$*. Write down the formal power series expansion:*

$$\begin{aligned} y_1(x) &= 1 + a_2(x-c)^2 + a_3(x-c)^3 + \dots\ , \\ y_2(x) &= -\frac{1}{c}(x-c) + a_2(x-c)^2 + a_3(x-c)^3 + \dots\ , \\ z_1(x) &= 1 + a_1(x-c) + a_2(x-c)^2 + \dots\ . \end{aligned}$$

*Set the regular point* $c = 2$ *and compute* $L(y_1) = 0,\ L(y_2) = 0,\ z_1' - \frac{z_1}{x-1} = 0$*. By solving the linear systems we obtain*

$$\begin{aligned} y_1(x) &= 1 + \frac{(x-2)^2}{16} - \frac{(x-2)^3}{192} + \frac{5(x-2)^4}{3072} + \dots\ , \\ y_2(x) &= \frac{-(x-2)}{2} - \frac{(x-2)^2}{16} - \frac{(x-2)^3}{192} + \frac{(x-2)^4}{3072} + \dots\ , \\ z_1(x) &= x - 1 = 1 + (x-2)\ . \end{aligned}$$

*The next step is to compute* $z_1$ *as multi-linear combination of* $y_1$ *and* $y_2$*:*

$$z_1 = \lambda_0 + \lambda_1 y_1 + \lambda_2 y_2 + \lambda_3 y_1^2 + \lambda_4 y_1 y_2 + \lambda_5 y_2^2\ .$$

*Replacing the solutions* $y_1, y_2$ *and* $z_1$ *by their Taylor series expansion yields*

$$\begin{aligned} &(\lambda_0 + \lambda_1 + \lambda_3) \\ &+(\frac{1}{2}\cdot\lambda_2 + \frac{1}{2}\cdot\lambda_4)\cdot(x-2) \\ &+(\frac{1}{16}\cdot\lambda_4 + \frac{1}{16}\cdot\lambda_1 + \frac{1}{16}\cdot\lambda_2 + \frac{1}{8}\cdot\lambda_3 + \frac{1}{4}\cdot\lambda_5)\cdot(x-2)^2 \\ &+(\frac{-1}{96}\cdot\lambda_3\frac{-1}{192}\cdot\lambda_1 + \frac{1}{192}\cdot\lambda_2 + \frac{7}{192}\cdot\lambda_4 + \frac{1}{16}\cdot\lambda_5)\cdot(x-2)^3 \\ &+(\frac{-1}{3072}\cdot\lambda_2 + \frac{11}{1536}\cdot\lambda_3 + \frac{5}{3072}\cdot\lambda_1 + \frac{1}{1024}\cdot\lambda_4 + \frac{7}{768}\cdot\lambda_5)\cdot(x-2)^4 \\ &+(\frac{-9}{20480}\cdot\lambda_1 - \frac{47}{30720}\cdot\lambda_3 + \frac{1}{3072}\cdot\lambda_5 + \frac{7}{61440}\cdot\lambda_2 + \frac{19}{20480}\cdot\lambda_4)\cdot(x-2)^5 \\ &+ \textit{ higher powers in } (x-2)\ . \end{aligned}$$

*The first six coefficients of this Taylor series expansion should equal the coefficients of* $z_1$*. That is we have to solve the linear equation system in* $\lambda_0, \dots, \lambda_5$ *such that the coefficient vector equals* $(1, 1, 0, 0, 0, 0)$*. Solving this yields:*

$$z_1 = y_1^2 + 2y_1y_2 - y_2^2.$$

*As another example for Theorem 2.27, which will be often used together with Lemma 4.56, we compute the stabilizer of the vector space spanned by* $z_1$. *The action of* $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *in* $\mathrm{GL}_n(\mathbb{C})$ *on* $z_1$ *is given via:*

$$z_1 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = y_1^2(a^2 - 2ab - b^2) + y_1y_2(2ac - 2ad - 2cb - 2bd) + y_2^2(c^2 - 2cd - d^2).$$

*By computing the normal form of this polynomial with respect to the ideal* $I = \langle y_1^2 - 2y_1y_2 - y_2^2 \rangle$ *we obtain*

$$\mathcal{E} := \mathrm{Stab}\left(\mathrm{Soln}\left(\delta(y) - \frac{y}{x-1}\right)\right) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid f_1(a,b,c,d) = 0,\ f_2(a,b,c,d) = 0 \right\}$$

*with* $f_1(a,b,c,d) = 2a^2 - 4ab - 2b^2 + 2ac - 2bc - 2ad - 2bd$
*and* $f_2(a,b,c,d) = a^2 - 2ab - b^2 + c^2 - 2cd - d^2$.
*Using techniques from Gröbner basis theory, we can also compute the connected component of* $\mathcal{E}$*:*

$$\mathcal{E}^\circ = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid b - c = 0,\ a - 2c - d = 0 \right\}$$

# Chapter 5

# Torsors and Rational Points

In this chapter fix a linear differential operator

$$L = \sum_{i=1}^{n} a_i \delta^i \in \mathbb{F}[\delta]$$

where $(\mathbb{F}, \delta)$ a differential field with algebraically closed field of constants $\mathbb{F}_0$. Denote by $\mathbb{K}$ a Picard-Vessiot field and by $A \in \mathbb{F}^{n\times n}$ the companion matrix corresponding to $L$.

Although the language and methods used are different to Hrushovskis original paper [Hru02], one can still recognize a lot of his ideas in this chapter.

The central idea to make the computation of the differential Galois group feasible is to switch from the presentation of a Pre-Galois group as some stabilizer of a subset of $\mathbb{K}^{n\times n}$ to an algebraic subgroup of $\mathrm{GL}_n(\mathbb{F}_0)$ and back. We will see that torsors are the main ingredient to make this switch (see also Remark 5.5).

## 5.1 Computing a Pre-Galois Group $\mathscr{H}$

Having developed the techniques of the previous chapter, we are now in the position to compute a first approximation on the differential Galois group. For convenience we will define what such an approximation will look like:

**Definition 5.1.** *Let $\mathscr{G}$ be the Galois group of a matrix differential equation $\delta(Y) = AY$ and Picard-Vessiot field $\mathbb{K}$. Let $F \in \mathrm{GL}_n(\mathbb{K})$ be a fundamental solution matrix and let $\phi\colon \mathscr{G} \to \mathrm{GL}_n(\mathbb{F}_0)$ be the associated representation as in Proposition 3.18. A closed subgroup $\mathscr{H} \subseteq \mathrm{GL}_n(\mathbb{F}_0)$ is a* Pre-Galois group *(for $\mathscr{G}$) if and only if*

$$\mathscr{H}^u \lhd \phi(\mathscr{G})^\circ \subseteq \phi(\mathscr{G}) \subseteq \mathscr{H} \ .$$

From Corollary 2.37 we know that such a Pre-Galois group must exist.

In the following we will construct such a Pre-Galois group. Roughly speaking it will be the stabilizer of solution spaces of right-hand factors of a certain symmetric power of a differential operator $L_n$. Here $L_n$ can be thought of the differential operator whose solution space contains $n$ copies of every solution of $L$.

Fixing a fundamental solution matrix

$$F_A = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1^{(1)} & y_2^{(1)} & \cdots & y_n^{(1)} \\ & & \ddots & \\ \cdots & \cdots & & \cdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{pmatrix} \in \mathbb{K}^{n\times n}$$

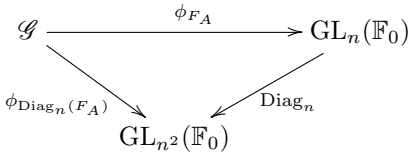
of $\delta(Y) = AY$ (with $y_i^{(j)} := \delta^j(y_i)$ for $1 \leq i, j \leq n$) we obtain by Proposition 3.18 a representation

$$\begin{aligned} \phi_{F_A} \colon \mathscr{G} &\to \mathrm{GL}_n(\mathbb{F}_0) \\ \sigma &\mapsto F_A^{-1}\sigma(F_A) \ . \end{aligned}$$

Also we define the diagonal embedding

$$\begin{aligned} \mathrm{Diag}_n \colon \mathrm{GL}_n(\mathbb{K}) &\to \mathrm{GL}_{n^2}(\mathbb{K}) \\ C &\mapsto \begin{pmatrix} \boxed{C} & & \\ & \ddots & \\ & & \boxed{C} \end{pmatrix} \ . \end{aligned}$$

By defining the block diagonal matrix $B = \mathrm{Diag}_n(A)$ we obtain a matrix differential equation $\delta(Y) = BY$ of dimension $n^2$. Since $B\,\mathrm{Diag}_n(F_A) = \mathrm{Diag}_n(A \cdot F_A) = \mathrm{Diag}_n(\delta(F_A))$, we see that $\mathrm{Diag}_n(F_A)$ is a fundamental solution matrix for $\delta(Y) = BY$.
In particular the differential Galois group of $\delta(Y) = BY$ equals $\mathscr{G}$ and the following diagram commutes:




Here $\phi_{\mathrm{Diag}_n(F_A)}$ is the embedding of $\mathscr{G}$ via $\mathrm{Diag}_n(F_A)$ in $\mathrm{GL}_{n^2}(\mathbb{F}_0)$ (again, use Proposition 3.18).
By Lemma 3.7 the equation $\delta(Y) = BY$ is equivalent to $\delta(Y) = A_nY$ where $A_n$ is the companion matrix of a monic linear differential operator denoted by $L_n$. Given $C \in \mathrm{GL}_{n^2}(\mathbb{F})$ with $A_n = CBC^{-1} - C\delta(C^{-1})$ we know by Proposition 3.3 that $C \cdot \mathrm{Diag}_n(F_A)$ is a fundamental solution matrix for $A_n$.
Since $\mathbb{K}$ is a Picard-Vessiot extension for $L_n$, the differential Galois group corresponding to $L_n$ is also $\mathscr{G}$.
Set $\tilde{F} := C \cdot \mathrm{Diag}_n(F_A)$. As before we obtain an embedding $\phi_{\tilde{F}}$ of $\mathscr{G}$ in $\mathrm{GL}_{n^2}(\mathbb{F}_0)$ by $\phi_{\tilde{F}}(\sigma) = \tilde{F}^{-1}\sigma(\tilde{F})$. As simple calculation shows that representation is same as the one we obtained from $\mathrm{Diag}_n(F_A)$:

$$\begin{aligned} \phi_{\tilde{F}}(\sigma) &= \mathrm{Diag}_n(F_A)^{-1}C^{-1}\sigma(C\,\mathrm{Diag}_n(F_A)) \\ &= \mathrm{Diag}_n(F_A)^{-1}\sigma(\mathrm{Diag}_n(F_A)) = \phi_{\mathrm{Diag}_n(F_A)}(\sigma) \text{ for } \sigma \in \mathscr{G} \ . \end{aligned}$$

Let $(y_{1,1}, \ldots, y_{1,n}, y_{2,1}, \ldots, y_{n,n}) \in \mathbb{K}^{n^2}$ be the first row of the matrix $C \cdot \mathrm{Diag}_n(F_A)$. Since $C \cdot \mathrm{Diag}_n(F_A)$ is a fundamental solution matrix for the matrix differential equation

$\delta(Y) = A_n Y$ and $A_n$ is a companion matrix, the entries of $(y_{1,1}, \ldots, y_{1,n}, y_{2,1}, \ldots, y_{n,n})$ form a basis for the solution space $V_n$ of $L_n$ (cf. Lemma 3.7).
The action of $\mathscr{G}$ on $V_n$ is uniquely determined by the action of $\mathscr{G}$ on $V$. In particular given $\sigma \in \mathscr{G}$, $i, j \in \{1, \ldots, n\}$ and $k \in \{0, \ldots, n-1\}$ we have

$$\begin{aligned}\sigma(\delta^k(y_{i,j})) =& \sigma\big(C \cdot \mathrm{Diag}_n(F_A)\big)_{k+1,\ j+(i-1)n} \\ =& \big(C \cdot \mathrm{Diag}_n(F_A) \cdot \phi_{\bar{F}}(\sigma)\big)_{k+1,\ j+(i-1)n} \\ =& \big(C \cdot \mathrm{Diag}_n(F_A) \cdot \phi_{\mathrm{Diag}_n(F_A)}(\sigma)\big)_{k+1,\ j+(i-1)n} \\ =& \big(C \cdot \mathrm{Diag}_n(F_A) \cdot \mathrm{Diag}_n(\phi_{F_A}(\sigma))\big)_{k+1,\ j+(i-1)n} \ .\end{aligned}$$

The first equality is due to the fact that $C \cdot \mathrm{Diag}_n(F_A)$ is a fundamental solution matrix for a matrix differential equation defined by a companion matrix. For later use, define the two matrices

$$x = \begin{pmatrix} x_{1,1}^{(0)} & \cdots & x_{1,n}^{(0)} \\ & \ddots & \\ x_{n,1}^{(0)} & \cdots & x_{n,n}^{(0)} \end{pmatrix} \text{ and } Y_n = \begin{pmatrix} y_{1,1} & \cdots & y_{1,n} \\ \vdots & \ddots & \vdots \\ y_{n,1} & \cdots & y_{n,n} \end{pmatrix} \ .$$

Here $x_{1,1}^{(0)}, \ldots, x_{n,n}^{(0)}$ are indeterminantes, which will define a polynomial ring. It is important to note that in the computation above (in the case $k = 0$) the equality $\sigma(Y_n) = Y_n \cdot \phi_{F_A}(\sigma)$ holds for $\sigma \in \mathscr{G}$.

**The symmetric power product of $L_n$**

Define the $e$-th symmetric power product of $L_n$

$$\mathbb{L} = \mathrm{LCLM}(L_n^{\circledS i} \mid i = 0, \ldots, e)$$

for any $e \in \mathbb{N}$. The order of $\mathbb{L}$ is $M := \sum_{i=0}^{e} \binom{n^2+i-1}{i}$. The solutions of $\mathbb{L}$ are precisely the polynomials of degree less than or equal to $e$ in the variables $y_{1,1}, \ldots, y_{n,n}$. Denote by $\mathscr{R}$ the set of all right-hand factors of $\mathbb{L}$ with coefficients in $\mathbb{F}$.
In particular, for any $K \in \mathscr{R}$ every solution of $K$ is of the form $P(y_{1,1}, \ldots, y_{n,n})$ for $P$ a polynomial of degree less than or equal to $e$ in the polynomial ring $\mathbb{F}_0[x] = \mathbb{F}_0[x_{1,1}^{(0)}, \ldots, x_{n,n}^{(0)}]$.

If, for any $i, j \in \mathbb{N}$ and $c \in \mathbb{N}_0$, we define $\delta(x_{i,j}^{(c)}) = x_{i,j}^{(c+1)}$, then $K(P(x_{1,1}^{(0)}, \ldots, x_{n,n}^{(0)}))$ is a polynomial in the ring

$$\mathfrak{R} := \mathbb{F}_0[x_{i,j}^{(c)} \mid 1 \leq i, j \leq n, 0 \leq c \leq M] \ .$$

The set of all polynomials in $\mathfrak{R}$ arising this way will be denoted by

$$N := \left\{ K(P(x_{1,1}^{(0)}, \ldots, x_{n,n}^{(0)})) \in \mathfrak{R} \mid K \in \mathscr{R},\ P(x) \in \mathbb{F}_0[x] \text{ with } P(Y_n) \in \mathrm{Soln}_{\mathbb{K}}(K) \right\} \ .$$

We define an action of $\mathscr{G}$ on $\mathfrak{R}$ by

$$\sigma(K(P(x)) = K(P(x \cdot \phi_{F_A}(\sigma)))$$

for all $\sigma \in \mathscr{G}$, $K \in \mathbb{F}[\delta]$ and $P(x) \in \mathbb{F}_0[x]$. By definition this action commutes with the evaluation map $x \mapsto Y_n$, that is $x_{i,j}^{(0)} \mapsto y_{i,j}$ for $i, j = 1, \ldots, n$.

Furthermore we define

$$\begin{aligned} Z &:= \{Y_n \cdot h \mid h \in \mathrm{GL}_n(\mathbb{F}_0),\ K(P(Y_n \cdot h)) = 0 \text{ for all } K(P(x)) \in N\} \\ &= \left\{ Y_n \cdot h \,\middle|\, \begin{array}{l} h \in \mathrm{GL}_n(\mathbb{F}_0) \text{ such that for all } P \in \mathbb{F}_0[x] \text{ and } K \in \mathscr{R}: \\ K(P(Y_n)) = 0 \Rightarrow K(P(Y_n \cdot h)) = 0 \end{array} \right\} \\ \mathscr{H} &:= \mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_0)}(Z) \\ &= \{s \in \mathrm{GL}_n(\mathbb{F}_0) \mid \forall K(P(x)) \in N,\ Y_n \cdot h \in Z:\ K(P(Y_n \cdot s \cdot h)) = 0\} \end{aligned}$$

**Theorem 5.2.** *Let $d$ be the number $B_5(n)$ in Corollary 2.37 and $\mathscr{G}$ the Galois group of $L$. If we chose $e \geq (n+1)d$, then the group $\mathscr{H}$ is a Pre-Galois group. This means that*

$$\mathscr{H}^u \leq \phi_{F_A}(\mathscr{G})^\circ \leq \phi_{F_A}(\mathscr{G}) \leq \mathscr{H}\ .$$

*Proof.* Apply Corollary 2.37 to $\mathscr{P} := \phi_{F_A}(\mathscr{G})$ to find a subgroup $\mathscr{M} \leq \mathrm{GL}_n(\mathbb{F}_0)$ with the property

$$\mathscr{M}^u \lhd \mathscr{P}^\circ \subseteq \mathscr{P} \subseteq \mathscr{M}$$

and $\mathcal{I}(\mathscr{M})$ is $B_5(n)$-bound definable. Denote by $W$ the variables $\{w_{1,1}, \ldots, w_{n,n}\}$ of the coordinate ring of $\mathbb{A}^{n^2}(\mathbb{F}_0)$. Let $\mathcal{I}(\mathscr{M}) \subseteq \mathbb{F}_0[W, r]$ (with $r$ an additional free variable) be the defining ideal of $\mathscr{M}$ and $\mathcal{I}'$ the determinant-free form of $\mathcal{I}(\mathscr{M})$.
Let $\mathcal{I}'$ be spanned by $\{p_\alpha(W) \mid \alpha \in \mathscr{A}\}$ for some index set $\mathscr{A}$ and let $V'$ be the $\mathbb{F}_0$-vector space spanned by $\{p_\alpha(Y_n) \mid \alpha \in \mathscr{A}\}$. The action of $\mathscr{G}$ on $V'$ is given via

$$\sigma(p_\alpha(Y_n)) = p_\alpha(Y_n \cdot \phi_{F_A}(\sigma)) \text{ for } \sigma \in \mathscr{G}, \alpha \in \mathscr{A}.$$

Since $\mathscr{P} \subseteq \mathscr{M}$ the ideal $\mathcal{I}(\mathscr{M})$ is $\mathscr{P}$-stable (see [Hum75, Lemma in Section 8.5]). Thus $V'$ is a $\mathscr{G}$-stable linear subspace of $\bigoplus_{i=0}^{d} \mathrm{Sym}^{\mathrm{i}}(V_n)$ and therefore is the solution space of a right-hand factor $K$ of $\mathbb{L}$ (see Lemma 4.7). Since $\mathscr{H}$ fixes all solution spaces of right-hand factors of $\mathbb{L}$ by definition, the ideal $\mathcal{I}'$ is $\mathscr{H}$-stable.
Now fix arbitrary $\alpha \in \mathscr{A}$ and $s \in \mathscr{H}$. Since $p_\alpha(W) \in \mathcal{I}'$ and $\mathcal{I}'$ is $\mathscr{H}$-stable, we have $p_\alpha(W \cdot s) \in \mathcal{I}'$. So evaluating $p_\alpha(W \cdot s)$ at any element $h \in \mathscr{M}$ gives zero. In particular we have $p_\alpha(\mathrm{Id} \cdot s) = p_\alpha(s) = 0$. This shows that $\mathscr{H} \subseteq \mathscr{M}$.
Thus we have established the following inclusions, which by injectivity of $\phi_{F_A}$ prove the claim:

$$\mathscr{H}^u \subseteq \mathscr{M}^u \subseteq \phi_{F_A}(\mathscr{G})^\circ \subseteq \phi_{F_A}(\mathscr{G}) \subseteq \mathscr{H} \subseteq \mathscr{M}.$$

Here the inclusion $\phi_{F_A}(\mathscr{G}) \subseteq \mathscr{H}$ comes from the fact that the differential Galois group stabilizes the solution space of any right hand factor of $\mathbb{L}$ (see Lemma 4.7). □

**Remark 5.3.** *It is cruical for the proof of the theorem above to work with the symmetric power product of $L_n$ instead of $L$. The ideal $\mathcal{I}'$ is generated by polynomials in $n^2$ variables. Thus we had to construct a differential operator having $n^2$ solutions such that the action of $\mathrm{GL}_{n^2}(\mathbb{F}_0)$ on $\mathbb{F}_0[x]$ is compatible with the action of $\mathscr{G}$ on $\mathbb{F}_0[Y_n]$.*

## 5.2 Characters of the Pre-Galois group

We continue to use the notation of the previous section.

**Lemma 5.4.** *By construction $Z$ is an $\mathscr{H}$-torsor, more precisely*

$$Y_n \cdot \mathscr{H} = Z.$$

*Proof.* $\subseteq$: Take $g \in \mathscr{H}$ and $K(P(x)) \in N$. By construction we have that $Y_n = Y_n \cdot 1 \in Z$. Since $K(P(Y_n \cdot g \cdot h) = 0$ for all $Y_n \cdot h \in Z$, the claim $K(P(Y_n \cdot g)) = 0$ follows.

$\supseteq$: Take $Y_n \cdot g \in Z$ arbitrary. We have to show that $K(P(Y_n \cdot g \cdot h)) = 0$ for any $K(P(x)) \in N$ and any $Y_n \cdot h \in Z$. The action of $h$ on $P(x)$ yields a new polynomial $Q \in \mathbb{F}_0[x]$ such that $P(x \cdot h) = Q(x)$. Since $Y_n \cdot h \in Z$ we have

$$0 = K\left(P(Y_n \cdot h)\right) = K\left(Q\left(Y_n\right)\right) \ .$$

This shows that $Q(Y_n) \in \mathrm{Soln}_{\mathbb{K}}(K)$ and thus $K(Q(x)) \in N$. Since $Y_n \cdot g \in Z$ we have

$$0 = K(Q(Y_n \cdot g)) = K(P\left(Y_n \cdot g \cdot h\right)) \qquad \square$$

**Remark 5.5.** *The Pre-Galois group $\mathscr{H}$ constructed so far is defined as the stabilizer of certain subsets of $\mathbb{K}^{n\times n}$. We need to compute the connected component of $\mathscr{H}$. The idea for doing this is as follows: First compute the defining ideal of $\mathscr{H}$ explicitly using Lemma 4.56. Then using Gröbner bases (see Theorem 1.25) we compute its primary decomposition, which in turn yields the defining ideal of $\mathscr{H}^\circ$ and hence a description of $\mathscr{H}^\circ$.*
*The problem is that $\mathscr{H}^\circ$ is no longer has the additional descirption of being the stabilizer of some subset of $\mathbb{K}^{n\times n}$. To go back from $\mathrm{GL}_n(\mathbb{F}_0)$ to such a stabilizer-description, one needs a rational point of $Y_n \cdot \mathscr{H}(\overline{\mathbb{F}})$. The next lemma will show the usefulness of torsors and how this works. The same idea will be used again in Proposition 5.21.*
*The idea of using Tosors and rational points of them was proposed the proof of [Hru02, Lemma 2F.3].*

In the following we will denote by $\mathbb{U}$ a universal Picard-Vessiot ring (of $\mathrm{Diff}_{\mathbb{F}}$) as defined in [vdPS03, Chapter 10, Section 1].

**Proposition 5.6.** *Let $\mathscr{H}$ and $Y_n$ be as defined in Section 5.1. There exists $g \in \mathrm{GL}_n(\overline{\mathbb{F}})$ such that*

$$(Y_n \cdot \mathscr{H}^\circ)(\mathbb{U}) = (g\mathscr{H}^\circ)(\mathbb{U}) \ .$$

*Proof.* Since $\phi(\mathscr{G}) \subseteq \mathscr{H}$ the torsor $Y_n \cdot \mathscr{H}$ is also $\mathscr{G}$-stable. Now assume that $\mathcal{I}(\mathscr{H})$ is generated by $\{p_\alpha(x) \mid \alpha \in \mathscr{A}\} \subseteq \mathbb{F}_0[x]$, then $\tilde{I} \coloneqq \mathcal{I}(Y_n \cdot \mathscr{H}) = \langle p_\alpha(Y_n^{-1}x) \mid \alpha \in \mathscr{A}\rangle \subseteq \mathbb{K}[x]$. By [vdPS03, Lemma 1.29] we know that $\tilde{I}$ is generated over $\mathbb{K}$ by $\tilde{I} \cap \mathbb{F}[x]$ and therefore $Y_n \cdot \mathscr{H}$ is defined over $\mathbb{F}$.
By [Spr09, Lemma 11.2.4] there exists $\tilde{g} = Y_n \cdot \tilde{h} \in (Y_n \cdot \mathscr{H})(\overline{\mathbb{F}})$ and thus

$$Y_n \cdot \mathscr{H} = Y_n \cdot \tilde{h} \cdot \mathscr{H} = \tilde{g} \cdot \mathscr{H} \ .$$

Let $g_1\mathscr{H}^\circ, \ldots, g_s\mathscr{H}^\circ$ be the irreducible components of $\mathscr{H}$ with $g_1, \ldots, g_s \in \mathrm{GL}_n(\mathbb{F}_0)$.
There exists $i \in \{1, \ldots, s\}$ with $\tilde{h}^{-1} \in g_i\mathscr{H}^\circ$. For any $h \in \mathrm{GL}_n(\mathbb{U})$ we have

$$\begin{aligned} Y_n h \in (Y_n \cdot \mathscr{H}^\circ)(\mathbb{U}) &\Leftrightarrow h \in \mathscr{H}^\circ(\mathbb{U}) \\ \Leftrightarrow Y_n h = \tilde{g}\tilde{h}^{-1}h = \tilde{g}g_i g_i^{-1}\tilde{h}^{-1}h &\in (\tilde{g}g_i \cdot \mathscr{H}^\circ)(\mathbb{U}) \end{aligned}$$

and therefore $(Y_n \cdot \mathscr{H}^\circ)(\mathbb{U}) = (\tilde{g}g_i \cdot \mathscr{H}^\circ)(\mathbb{U})$. $\square$

**Remark 5.7.** *Given $\tilde{g} \in (Y_n \cdot \mathscr{H})(\overline{\mathbb{F}})$ as in the previous proof, we can compute $g \in \mathrm{GL}_n(\overline{\mathbb{F}})$ as in Proposition 5.6 as follows:*
*Compute the decomposition of $\mathscr{H} \subseteq \mathbb{A}^{n^2}(\mathbb{F}_0)$ into its irreducible components $g_1\mathscr{H}^\circ, \ldots, g_s\mathscr{H}^\circ$ with $g_1, \ldots, g_s \in \mathrm{GL}_n(\mathbb{F}_0)$ using Gröbner basis techniques (see Theorem 1.25).*

*Given the minimal polynomial $P_{i,j}(y) \in \mathbb{F}[y]$ for the $(i,j)$-th entry $g_{i,j}$ of $\tilde{g}$ for $1 \leq i,j \leq n$, one can compute differential operators $L_{i,j}$ of minimal order with the property $L_{i,j}(g_{i,j}) = 0$ for $1 \leq i,j \leq n$ (see [CSTU02, Section 2]).*
*Compute the Taylor series of the entries of $Y_n$ and $g_{i,j}$ about a common regular point of $L_n$ and $L_{i,j}$ for all $i,j \in \{1,\ldots,n\}$ up to a certain degree $m$ (as in Theorem 4.53). Such a point exists, because $L_n$ and $L_{i,j}$ can only have a finite number of singular points.*
*If for the approximations $Y_n \notin \tilde{g}g_i \cdot \mathscr{H}^\circ(\mathbb{U})$ for all but one $i \in \{1,\ldots,s\}$ holds, then we are done (set $g = \tilde{g}g_i$). Otherwise increase $m$ and and check again. This process terminates, since multiplication with $\tilde{g}$ is a homeomorphism.*

We have to be able to efficiently compute $g \in \mathrm{GL}_n(\overline{\mathbb{F}})$ mentioned in Proposition 5.6. In a more general formulation this can be stated as being able to find $\overline{\mathbb{F}}$-rational points of varieties:

**Assumption 5.8.** *Let $\mathscr{U}$ be a subvariety of $\mathbb{A}^m(\mathbb{U})$. If $\mathscr{U}$ is defined over $\mathbb{F}$, then we can compute $\tilde{g} \in \mathscr{U}(\overline{\mathbb{F}})$.*

Of course it would suffice to be able to find a $\overline{\mathbb{F}}$-rational point for the given variety:

**Assumption 5.9.** *We can compute $\tilde{g} \in \mathrm{GL}_n(\overline{\mathbb{F}})$ such that $\tilde{g} \cdot \mathscr{H} = Y_n \cdot \mathscr{H}$.*

If one could solve the first assumption, the second easily follows. To be able to continue we will require that the weak Assumption 5.9 can be solved.
In the following we fix $g \in \mathrm{GL}_n(\overline{\mathbb{F}})$ as in Proposition 5.6.
The statement of the next lemma can also be found in [Hru02, Lemma 2.2].

**Lemma 5.10.** *For a $g$ as in Proposition 5.6 and a character $\chi\colon \mathscr{H}^\circ \to \mathbb{F}_0^\times \in X(\mathscr{H}^\circ)$ define $h := \chi(g^{-1}Y_n)$. Then the logarithmic derivative $\delta(h)h^{-1}$ lies in $\overline{\mathbb{F}}$.*

*Proof.* For $\sigma \in \mathscr{G}^\circ$ and with $\chi(\phi(\sigma)) \in \mathbb{F}_0$, we now have

$$\sigma\left(\frac{\delta(h)}{h}\right) = \sigma\left(\frac{\delta(\chi(g^{-1}Y_n))}{\chi(g^{-1}Y_n))}\right) = \frac{\chi(\phi(\sigma))\ \delta(\chi(g^{-1}Y_n))}{\chi(\phi(\sigma))\ \chi(g^{-1}Y_n)} = \frac{\delta(h)}{h}\ .$$

Since the fixed field of $\mathscr{G}^\circ$ is $\overline{\mathbb{F}}$, the claim follows. □

**Theorem 5.11.** *Let $g$ be as in Proposition 5.6. If $\mathbb{F}$ is a subset of $\mathbb{C}(t)$, then a set of generators $\langle \chi_1,\ldots,\chi_l\rangle$ for $X(\mathscr{H}^\circ)$ can be calculated. Furthermore if $h_i := \chi_i(g^{-1}Y_n)$ for $i = 1,\ldots,l$, then $\{h_1,\ldots,h_l\}$ can be computed.*

*Proof.* Let $E$ be the bound on the degree of generators of $X(\mathscr{H}^\circ)$ (considered as elements of $\mathbb{F}_0[x,t]$), which can be computed according to Theorem 2.25. Thus if we compute all characters of $\mathscr{H}^\circ$ up to degree $E$, we obtain a generating set. For any $\chi \in X(\mathscr{H}^\circ)$ of degree $m$, $\chi(g^{-1}Y_n)$ is an element of degree $m$ in $\mathbb{F}_0[g_{i,j},\ Y_n \mid 1 \leq i,j \leq n]$. Here $g_{i,j}$ denote the entries of $g$.
For $i,j = 1,\ldots,l$ let $L_{i,j} \in \mathbb{F}[\delta]$ be a differential operator with $L_{i,j}(g_{i,j}) = 0$ (see [CSTU02, Section 2]). If we define $K = \mathrm{LCLM}(L_{i,j}, L_n \mid 1 \leq i,j \leq n)$ and

$$S := \mathrm{LCLM}\left(K^{\circledS i} \mid i = 1,\ldots,E\right)\ ,$$

then $h_i = \chi_i(g^{-1}Y_n)$ is a solution of $S$ for $i = 1,\ldots,l$.
Since the logarithmic derivative of $h_i$ lies in $\overline{\mathbb{F}}$, computing all first order right hand factors in $\overline{\mathbb{F}}[\delta]$ yields all $h_i$.

On the other hand, let $T = \delta - \frac{\delta(a)}{a}$ with $\frac{\delta(a)}{a} \in \overline{\mathbb{F}}$ be a right factor of $S$. Since the solutions of $S$ are polynomials in the entries of $Y_n$ and $g$, the same is true for $a$, which solves $T(a) = 0$. Thus $\frac{\delta(a)}{a}$ is fixed by $\mathscr{H}^\circ$. From Lemma 3.21 we know that $T$ yields a character of $\mathscr{H}^\circ$.
The computation of right hand factors of $S$ with coefficients in $\overline{\mathbb{F}}$ is feasible due to [CW04b].□

**Remark 5.12.** *If we had another way to compute $h_1, \dots, h_l$, which are only required to apply Theorem 5.14, one would not need to be able to find a rational point of $Y_n \cdot \mathscr{H}$ and thus Assumption 5.9 could be dropped.*

## 5.3 Computation of $\phi(\mathscr{G})^\circ$

In this section we develop a method to compute $\phi(\mathscr{G})^\circ$. This is analog to Hrushovski's work and references to the corresponding results in [Hru02] are given. A main difference is that we use results of Compoint and Singer, which simplify the approach.
Let $\{\chi_1, \dots, \chi_l\}$ be generators for the group of characters $X(\mathscr{H}^\circ)$. Using Theorem 5.11, we can compute $h_i := \chi_i(g^{-1}Y_n)$ with logarithmic derivative in $\overline{\mathbb{F}}$. Now define the map

$$\begin{aligned} \varphi\colon \mathscr{H}^\circ &\to (\mathbb{F}_0^\times)^l \\ h &\mapsto (\chi_1(h), \dots, \chi_l(h)). \end{aligned}$$

Note that this is the same map Hrushovkis used in [Hru02, Corollary 2.2C]. The field $\mathbb{F}_1 := \mathbb{F}\left(\frac{\delta(h_1)}{h_1}, \dots, \frac{\delta(h_l)}{h_l}\right)$ is a finite algebraic extension of $\mathbb{F}$. We define the exponential field extension $\mathbb{E} := \mathbb{F}_1(h_1, \dots, h_l)$. The solution space of the differential operator $\mathrm{LCLM}\left(\delta - \frac{\delta(h_i)}{h_i} \mid i = 1, \dots, l\right) \in \mathbb{F}_1[\delta] \subseteq \overline{\mathbb{F}}[\delta]$ is spanned by $h_1, \dots, h_l$. The corresponding differential Galois group $\mathrm{Gal}(\mathbb{E}/\overline{\mathbb{F}})$ shall be denoted by $\Gamma$.
Since the kernel of $\varphi$ is $\mathscr{H}^u$, the image is isomorphic to a torus. The next proposition will describe this torus.
The following statement can be found along the lines of [Hru02, Corollary 2.2C and Lemma 2.3].

**Proposition 5.13.** *$\varphi(\phi(\mathscr{G})^\circ) = \mathscr{T}$ for*

$$\mathscr{T} := \left\{(c_1, \dots, c_l) \in (\mathbb{F}_0^\times)^l \mid \exists \sigma \in \Gamma\ \forall i \in 1, \dots, l\colon\ \sigma(h_i) = c_i h_i\right\}\ .$$

*Proof.* Take any $\sigma \in \mathscr{G}^\circ$ and denote its image by $c_\sigma \in \phi(\mathscr{G})^\circ$, then we have

$$\sigma(h_i) = \sigma\left(\chi_i\left(g^{-1}Y_n\right)\right) = \chi_i\left(g^{-1}Y_n c_\sigma\right) = \chi_i(c_\sigma)h_i\ .$$

Since $\phi(c_\sigma) = (\chi_1(\sigma), \dots, \chi_l(\sigma))$ we have seen that $\phi(c_\sigma) \in \mathscr{T}$.
Now let $(c_1, \dots, c_l) \in \mathscr{T}$ with $\sigma(h_i) = c_i h_i$ for some $\sigma \in \Gamma$. By differential Galois theory (Theorem 3.17) we have the isomorphism

$$\Gamma \cong \mathrm{Gal}(\mathbb{K}/\overline{\mathbb{F}})/\mathrm{Gal}(\mathbb{K}/\mathbb{E})$$

and thus a surjective map

$$\psi\colon \mathscr{G}^\circ \to \Gamma\ .$$

For the given $\sigma \in \Gamma$ take a pre-image $\tau \in \mathscr{G}^\circ$.
For $i = 1, \dots, l$ we have:

$$c_i h_i = \sigma(h_i) = \tau(h_i) = \chi_i(c_\tau)h_i = \chi_i(c_\tau)h_i$$

Thus $\varphi(c_\tau) = (c_1, \dots, c_l)$. □

The following theorem and proposition can be found in [CS99]. We adopted the notations to our setting and removed unused results:

**Theorem 5.14.** *[CS99, Proposition 2.4] If $\mathbb{F}_1$ is a finitely generated algebraic extension of $\mathbb{C}(t)$ one can compute the following objects:*

- *A subset $S = \{h_{i_1}, \dots, h_{i_r}\}$ of $\{h_1, \dots, h_l\}$,*
- *$f_1, \dots, f_l \in \mathbb{F}_1$ and*
- *for $j = 1, \dots, l,\ i = 1, \dots, r$ integers $n_j, n_{i,j}, n_j \neq 0$*

*such that $\{h_{i_1}, \dots, h_{i_r}\}$ is a transcendence basis of $\mathbb{E}$ over $\mathbb{F}_1$ and the equations*

$$h_j^{n_j} = f_j \prod_{t=1}^{r} h_{i_t}^{n_{t,j}}$$

*hold for $i = 1, \dots, l$ if $S$ is not empty, or $h_j^{n_j} = f_j$ is $S$ is empty.*

**Proposition 5.15.** *[CS99, Proposition 2.5] Define $N$ to be the least common multiple of $n_1, \dots, n_l$. The homomorphism*

$$\begin{aligned} \eta\colon \left(\mathbb{F}_0^\times\right)^r &\to \mathrm{Gal}(\mathbb{E}/\overline{\mathbb{F}}) \leq \mathrm{GL}_l(\mathbb{F}_0) \\ (\lambda_1, \dots, \lambda_r) &\mapsto \left( \prod_{t=1}^{r} \lambda_{i_t}^{N n_{t,1} n_1^{-1}}, \prod_{t=1}^{r} \lambda_{i_t}^{N n_{t,2} n_2^{-1}}, \dots, \prod_{t=1}^{r} \lambda_{i_t}^{N n_{t,l} n_l^{-1}} \right) \end{aligned}$$

*is surjective and has finite kernel.*

**Remark 5.16.** *In Proposition 5.15 the map $\eta$ does not map to $\mathrm{Gal}(\mathbb{E}/\overline{\mathbb{F}})$, but to a representation of this group in $\mathrm{GL}_l(\mathbb{F}_0)$. In particular for any $\tau \in \Gamma = \mathrm{Gal}(\mathbb{E}/\overline{\mathbb{F}})$ there exists $\lambda \in \left(\mathbb{F}_0^\times\right)^r$ such that for all $i = 1, \dots, l$*

$$\tau(h_i) = \eta(\lambda) \cdot h_i \ .$$

The stated results of [CS99] also yield relations for the characters restricted to $\phi(\mathscr{G})^\circ$.

**Lemma 5.17.**

$$\phi(\mathscr{G})^\circ \subseteq \mathcal{V}\left( \left\{ \chi_j^{n_j} - \prod_{t=1}^{r} \chi_t^{n_{t,i}} \mid j = 1, \dots, l \right\} \right)$$

*Proof.* Take $\sigma \in \mathscr{G}^\circ$ and $i \in \{1, \dots, l\}$. Since $\mathscr{G}^\circ = \mathrm{Gal}(\mathbb{K}/\overline{\mathbb{F}})$ we have $\sigma(f_i) = f_i$ and thus

$$\begin{aligned} \sigma\left(h_i^{n_i}\right) &= \sigma(f_i) \prod_{t=1}^{r} \sigma(h_t)^{n_{t,i}} = f_i \prod_{t=1}^{r} \sigma(h_t)^{n_{t,i}} \\ &= \left( f_i \prod_{t=1}^{r} h_i^{n_{t,i}} \right) \cdot \prod_{t=1}^{r} \chi_i(\sigma)^{n_{t,i}} = h_i^{n_i} \cdot \prod_{t=1}^{r} \chi_i(\sigma)^{n_{t,i}} \end{aligned}$$

On the other hand we have

$$\left(\sigma(h_i)\right)^{n_i} = \chi_i(\sigma)^{n_i} \cdot h_i^{n_i}$$

Putting both equations together and dividing by $h_i^{n_i}$ we have

$$\chi_i(\sigma)^{n_i} = \prod_{t=1}^{r} \chi_i(\sigma)^{n_{t,i}} \ .$$

□

**Remark 5.18.** *The following simple computations give the motivation for the upcoming Theorem 5.19: Due to the surjectivity of $\eta$ we have*

$$\begin{aligned}\varphi(\phi(\mathscr{G})^\circ) = \mathscr{T} &= \left\{(c_1,\dots,c_l) \in (\mathbb{F}_0^\times)^l \mid \exists \sigma \in \Gamma \colon \sigma(h_i) = c_i h_i \right\} \\ &= \left\{(c_1,\dots,c_l) \in (\mathbb{F}_0^\times)^l \mid \exists \lambda \in (\mathbb{F}_0^\times)^r \colon \eta(\lambda)(h_i) = c_i h_i \right\} \\ &= \left\{(c_1,\dots,c_l) \in (\mathbb{F}_0^\times)^l \mid \exists \lambda \in (\mathbb{F}_0^\times)^r \colon \eta(\lambda)_i = h_i \right\} \\ &= \eta\big((\mathbb{F}_0^\times)^l\big)\ .\end{aligned}$$

*So $\phi(\mathscr{G})^\circ$ lies in the preimage of $\eta\big((\mathbb{F}_0^\times)^l\big)$:*

$$\begin{aligned}\phi(\mathscr{G})^\circ \subseteq& \varphi^{-1}\left(\eta\left(\left(\mathbb{F}_0^\times\right)^l\right)\right) \\ &= \left\{\sigma \in \phi(\mathscr{H})^\circ \mid \exists \lambda \in (\mathbb{F}_0^\times)^r \colon \varphi(\sigma) = \eta(\lambda)\right\} \\ &= \left\{\sigma \in \phi(\mathscr{H})^\circ \;\middle|\; \exists (\lambda_1,\dots,\lambda_r) \in (\mathbb{F}_0^\times)^r \colon \chi_i(\sigma) = \prod_{t=1}^{r} \lambda_t^{N\cdot n_{i,t}\cdot n_i^{-1}}\right\}\end{aligned}$$

*Note that this is the analog to the pullback mentioned in [Hru02, Algorithm B, step e)].*

**Theorem 5.19.** *If we define*

$$H = \mathscr{H}^\circ \cap \mathcal{V}\left(\left\{\chi_j^{n_j} - \prod_{t=1}^{r} \chi_t^{n_{t,i}} \mid j = 1,\dots,l\right\}\right)$$

*then $H^\circ = \phi(\mathscr{G})^\circ$.*

*Proof.* We will prove the following facts:

1) $\varphi(H) \supseteq \mathscr{T}$
2) $\mathrm{Ker}(\varphi) \subseteq \phi(\mathscr{G})^\circ \cap H$
3) $[H : \phi(\mathscr{G})^\circ] = [\varphi(H) : \varphi(\phi(\mathscr{G})^\circ)]$
4) The index of $\varphi(\phi(\mathscr{G})^\circ)$ in $\varphi(H)$ is finite.

As $\phi(\mathscr{G})^\circ$ is irreducible and lies in $H$ (due to Lemma 5.17), the statements 3) and 4) immediately imply the theorem.
1): Since $\mathscr{T} = \varphi(\phi(\mathscr{G})^\circ)$ and $\phi(\mathscr{G})^\circ \subseteq H$ this point is clear.
2): The kernel of $\varphi$ is the intersection of the kernels of all characters of $\mathscr{H}^\circ$, which equals $\overline{\mathscr{H}^u}$.

$$\ker(\varphi) = \mathscr{H}^u \subseteq \phi(\mathscr{G})^\circ.$$

3): Define the restrictions $\varphi_1 := \varphi\mid_{\phi(\mathscr{G})^\circ}$ and $\varphi_2 := \varphi\mid_H$. Using 2), we get the equations $\overline{\ker}(\varphi) = \ker(\varphi_1) = \ker(\varphi_2)$. Using the isomorphism theorems we have

$$H/\phi(\mathscr{G})^\circ \cong (H/\ker(\varphi))\,/\,(\phi(\mathscr{G})^\circ/\ker(\varphi)) \cong \varphi(H)/\varphi(\phi(\mathscr{G})^\circ)$$

4): Recall that $N$ is the least common multiple of $n_1,\dots,n_l$, define $N_i = \frac{N}{n_i}$ and take an arbitrary element $c = (c_1,\dots,c_l) \in \varphi(H)$.

$$c_i^N = (c_i^{n_i})^{N_i} = \prod_{t=1}^{r} c_t^{n_{t,i}N_i}$$

With this calculation and Proposition 5.15 we see that $c^N \in \mathrm{Gal}(E/\overline{\mathbb{F}})$. Since $c^N$ acts on $(h_1,\dots,h_l)$ via component-wise multiplication, we have $c^N \in \mathscr{T}$. □

## 5.4 Computation of $\phi(\mathscr{G})$

After we found defining equations for $\phi(\mathscr{G})^\circ$ the idea in this section goes as follows: We construct an $\phi(\mathscr{G})^\circ$-torsor, which is defined over a finite algebraic extension of $\mathbb{F}$. Let $\Theta$ denote the corresponding (algebraic) Galois group. Now $\phi(\mathscr{G})$ turns out to be the stabilizer of the defining equations of $\phi(\mathscr{G})^\circ$ up to the action of $\Theta$. We will make this more precise later on.
Recall that $g \in \mathrm{GL}_n(\overline{\mathbb{F}})$ was chosen such that $Y_n \cdot \mathscr{H}^\circ = g \cdot \mathscr{H}^\circ$.
We can compute the defining ideal $\mathcal{I}(\mathscr{H}^\circ) \subseteq \mathbb{F}_0[x,t]$ using Gröbner basis techniques (as in Remark 5.5). Furthermore let $\langle r_i \mid i = 1,\dots,s\rangle \subseteq \mathbb{F}_0[x]$ be the determinant-free form of $\mathcal{I}(\mathscr{H}^\circ)$.

**Lemma 5.20.** *Here $\mathscr{H}$ is as defined in Section 5.1. Define the ideal $J$ in $\mathbb{F}_0(g)[x]$ generated by*

$$\{r_i(g^{-1}x) \mid i = 1,\dots,s\} \cup \left\{ \chi_i(g^{-1}x)^{n_i} - \prod_{t=1}^{r} \chi_t(g^{-1}x)^{n_{t,i}} \mid i = 1,\dots,l \right\}.$$

*We have $Y_n \cdot \mathrm{GL}_n(\mathbb{F}_0) \cap \mathcal{V}(J) = Y_n \cdot H$.*

*Proof.* $\subseteq$: Take an arbitrary element $Y_n \cdot h$ with $h \in \mathrm{GL}_n(C)$.

$$Y_n \cdot h \in \mathcal{V}(J) \Rightarrow r_i(g^{-1}Y_n h) = 0 \text{ for } i \in I \ \Rightarrow h \in \mathscr{H}^\circ.$$

Thus $g^{-1}Y_n h \in \mathscr{H}^\circ$ and since $g^{-1}Y_n \in \mathscr{H}^\circ$ we get $h \in \mathscr{H}^\circ$. Also we have for $j = 1,\dots,l$:

$$\begin{aligned} 0 =& \chi_j(g^{-1}Y_n h)^{n_j} - \prod_{t=1}^{r} \chi_t(g^{-1}Y_n h)^{n_{t,j}} \\ =& \chi_j(g^{-1}Y_n)^{n_j}\chi_j(h)^{n_j} - \underbrace{\prod_{t=1}^{r} \chi_t(g^{-1}Y_n)^{n_{t,j}}}_{=\chi_j(g^{-1}Y_n)^{n_j}} \prod_{t=1}^{r} \chi_t(h)^{n_{t,j}} \\ \Rightarrow& \chi_j(h)^{n_j} - \prod_{t=1}^{r} \chi_t(h)^{n_{t,j}} = 0 \end{aligned}$$

$\supseteq$: Take $Y_n \cdot h \in Y_n \cdot H$ arbitrary with $h \in H$. Then $g^{-1}Y_n h \in \mathscr{H}^\circ$, so $r_i(g^{-1}Fh) = 0$.

$$\begin{aligned} & \chi_j(g^{-1}Fh)^{n_j} - \prod_{t=1}^{r} \chi_t(g^{-1}Fh)^{n_{t,j}} \\ =\ & \chi_j(g^{-1}F)^{n_j}\chi_j(h)^{n_j} - \underbrace{\prod_{t=1}^{r} \chi_t(g^{-1}F)^{n_{t,j}}}_{\chi_j(g^{-1}F)^{n_j}} \underbrace{\prod_{t=1}^{r} \chi_t(h)^{n_{t,j}}}_{\chi_j(h)^{n_j}} = 0 \end{aligned}$$

Since $H \subseteq \mathscr{H}^\circ \subseteq \mathrm{GL}_n(C)$, $h$ is also invertible. □

**Proposition 5.21.** *There exists $\tilde{g} \in \mathrm{GL}_n(\overline{\mathbb{F}})$ such that*

$$Y_n \cdot H^\circ(\mathbb{U}) = \tilde{g} \cdot H^\circ(\mathbb{U})$$

*and therefore*

$$Y_n \cdot \phi(\mathscr{G})^\circ(\mathbb{U}) = \tilde{g} \cdot \phi(\mathscr{G})^\circ(\mathbb{U}) \ .$$

*Proof.* The proof goes exactly as the proof of Proposition 5.6. The only difference is that $Y_n \cdot \phi(\mathscr{G})^\circ$ is $\phi(\mathscr{G})^\circ$-stable and therefore defined over $\overline{\mathbb{F}}$. □

Here we also need to be able to compute a rational point of a variety defined over $\overline{\mathbb{F}}$. A weaker assumption in this case is as follows:

**Assumption 5.22.** *We can compute $\tilde{g} \in \mathrm{GL}_n(\overline{\mathbb{F}})$ such that $Y_n \cdot H^\circ(\mathbb{U}) = \tilde{g} \cdot H^\circ(\mathbb{U})$.*

Denote by $\mathbb{F}_2$ the normal closure of the algebraic field extension of $\mathbb{F}$ generated by the entries of $\tilde{g}$. Furthermore we denote by $\Theta$ the (algebraic) Galois group of $\mathbb{F}_2$ over $\mathbb{F}$. If the ideal $\mathcal{I}(H^\circ) \subseteq \mathbb{F}_0[x]$ is generated by $\tilde{c}_1, \ldots, \tilde{c}_p$ and $c_i(x) := \tilde{c}_i(\tilde{g}^{-1}x)$ for $i = 1, \ldots, p$, then

$$\mathcal{I}(Y_n \cdot \phi(\mathscr{G})^\circ) = \langle c_1, \ldots, c_p \rangle \ .$$

**Theorem 5.23.**

$$\phi(\mathscr{G}) = \{a \in \mathrm{GL}_n(\mathbb{F}_0) \mid \exists \tau \in \Theta\colon \ \tau(c_i)(Y_n \cdot a) = 0 \text{ for all } i = 1, \ldots, p\}$$

*Proof.* $\subseteq$: Let $a \in \phi(\mathscr{G})$, thus there is $\sigma \in \mathscr{G}$ with $\sigma(Y_n) = Y_n \cdot a$. There exists $\tau \in \mathrm{Gal}(\mathbb{U}/\mathbb{F})$ with $\tau\,|_{\mathbb{K}} = \sigma$ and $\tau\,|_{\mathbb{F}_2} \in \Theta$.

$$0 = \tau\Big(\underbrace{c_i(Y_n)}_{=0}\Big) = \tau(c_i)\,(\tau(Y_n)) = \tau(c_i)(Y_n \cdot a)$$

$\supseteq$: Take $a \in \mathrm{GL}_n(\mathbb{F}_0)$ and $\tau \in \Theta$ with $\tau(c_i)(Y_n \cdot a) = 0$. There exists $\tilde{\tau} \in \mathrm{Gal}(\mathbb{U}/\mathbb{F})$ with $\tilde{\tau}\,|_{\mathbb{F}_2} = \tau^{-1}$ and $\tilde{\tau}(Y_n) = Y_n \cdot h$ for some $h \in \phi(\mathscr{G})$.

$$0 = \tilde{\tau}\big(\underbrace{\tau(c_i)(Y_n \cdot a)}_{=0}\big) = c_i(Y_n \cdot h \cdot a)$$

□

Thus we have seen that $Y_n \cdot h \cdot a \in Y_n \cdot \phi(\mathscr{G})^\circ$. This implies $ha \in \phi(\mathscr{G}^\circ)$ and therefore $a \in \phi(\mathscr{G})$.

**Remark 5.24.** *As mentioned in the introduction to this chapter, although methods and proofs are vastly different, one can recognize the same ideas already in Hrushovksis paper [Hru02]. The idea to use torsors to compute $\mathscr{H}^\circ$ as we did in Proposition 5.6 can be found in [Hru02, Lemma 2F.3]. The results of [Hru02, 2.2-2.4] correlate to Section 5.3. The Theorem 5.23 is almost identical to [Hru02, Algorithm C, p.116].*

# Chapter 6

# Appendix: Implementation

Here we list implementations of presented algorithms in *Maple*. In particular the *swap*-algorithm.
Some of this algorithm requires the packages *DEtools, combinat, LinearAlgebra*, which have to be loaded before-hand. Also it might be convenient to specify the ring of differential operators before starting calculations. So a common worksheet starts with

```
with(DEtools):
with(LinearAlgebra):
with(combinat):
_Envdiffopdomain := [Dx,x];
read "/Path/To/SwapLib";
```

For example the differential operator $\delta^2 + x\delta + \frac{1}{x}$ is represented in *Maple* via `Dx^2 +x*Dx + 1/x`.
The functions `matrix2op`, `op2matrix`, `order`, `LC` and `findSim` do the obvious. Since the main algorithms rely on them, we state implementations of those in Section 6.4.

## 6.1 Functions already provided by maple

There are several functions, which are used by the algorithm below or are just useful in general. A good overview is provided by the *DEtools* website `http://www.maplesoft.com/support/help/Maple/view.aspx?path=DEtools`.
Let $L, K \in \mathbb{C}(x)[\delta]$ with $\delta = \frac{d}{dx}$. Let $o$ be the return value of `diffop2de(L,y(x))`.

| function call | description |
|---|---|
| `mult(L,K)` | Returns the product of $LK$. |
| `rightdivision(L,K)` | Returns a tuple $[Q, R]$ with $L = QK + R$ and $\mathrm{ord}(R) < \mathrm{ord}(Q)$. |
| `DFactor(L)` | Returns a list $[L_1, \ldots, L_s]$ such that $L = L_1 \cdots L_s$ and $L_i$ is irreducible for $i = 1, \ldots, s$. |
| `diffop2de(L,y(x))` | Replaces every occurrence of `Dx^i` by $\frac{d^i y(x)}{dx^n}$ |
| `dsolve(o,y(x))` | Tries to compute solutions of the differential equation $o$. |
| `ratsols(o,y(x))` | Tries to compute rational solutions of the differential equation $o$. |
| `expsols(o,y(x))` | Tries to comp. exponential solutions of the differential equation $o$. |
| `LCLM(L,K)` | Computes the least common left multiple of $K$ and $L$. |
| `GCRD(L,K)` | Computes the greatest common right divisor of $K$ and $L$. |
| `symmetric_power(L,n)` | Computes the $n$-th symmetric power of $L$ for $n \in \mathbb{N}$. |

## 6.2 Computing Solutions of Symmetric Power Factors

**Input:** A linear differential operator $L$ of order $n$, a right hand factor $K$ of the $d$-th symmetric power of $L$ and a regular point $c$ of $L$ and $K$.
**Explanation:** The choice of a regular point $c$ of $L$ fixes a basis $y_1, \ldots, y_n$ of the solution space of $L$ (see Corollary 4.54). Let $\vec{y}_1, \ldots, \vec{y}_m$ be all monomials in the variables $y_1, \ldots, y_n$ of degree $d$. Every solution of $K$ is a sum of those monomials. This algorithm computes the coefficients of those sums.
**Output:** The program prints a table, which gives a bijection among natural numbers and monomials of degree $d$ in $n$. The program returns a list $H$ of tables. Every table $H[i]$ defines the coefficients $c_{i,j}$ of an arbitrary element $\sum_{j=1}^{m} c_{i,j}\vec{y}_m$.
**Example:** If we set $L = \delta^2 - \frac{1}{2x}\delta - x$, $K = \delta^2 - \frac{1}{2x}\delta - 4x$, $d = 2$ and $c = 1$, then the algorithm prints the table

```
[[2,0], 3]
[[1,1], 4]
[[0,2], 5]
```

and returns `table([1 = [h[3] = 1, h[4] = 0, h[5] = 4],`
`  2 = [h[3] = 0, h[4] = 1, h[5] = 0]])` .
This tells us that the solution space of $K$ is spanned by two elements $z_1$ and $z_2$, which can be expressed in terms of fixed solutions $y_1, y_2$ as follows:

$$z_1 = 1 \cdot y_1^2 + 0 \cdot y_1 y_2 + 4 \cdot y_2^2$$
$$z_2 = 0 \cdot y_1^2 + 1 \cdot y_1 y_2 + 0 \cdot y_2^2$$

```
taylorExpLeq := proc (L,K,d,c)
        local k,y1,s,j,a,b, ordL,m,i,n,x,sz,SZ,Z,z,S,T,Y,y,T1,v,
            summand,h,l,TZ,Rel,H2;

        ordL:=order(L);
        n:=order(K);

        m:=0;
        for i from 1 to d-1 do
                m:=m+eval(binomial(ordL+i-1,i));
        end do;
        b:=0;
        m:= m+eval(binomial(ordL+d-1,d));

        print(m);
        l:= diffop2de(L,y1(x));
        k:= diffop2de(K,y1(x));

        #compute taylor series of solutions y[i] of L
        s:= x-> add( a[j] * (x-c)^j , j = ordL..m);

        for i from 1 to ordL do
                S[i]:= simplify(subs( y1(x) = 1/((i)!)*(x-c)^(i-1) +
                s(x),l));
                T[i]:= series(S[i],x=c,m);
```

```
                Y[i] :=eval( solve( {seq(coeff(T[i],x-c,j),
                j=0..m-ordL)},[seq(a[j],j=ordL..m)]))[1];
                y[i]:= unapply( 1/((i)!)*(x-c)^(i-1)
                +(subs(Y[i],s(x))),x);
        end do;


        # compute taylor expansions of solutions z[i] of K
        for i from 1 to n do
            sz[i]:= x-> add( a[j] * (x-c)^j , j = n..m-1);
            SZ[i]:=simplify( subs( y1(x)=1/((i)!)*(x-c)^(i-1)+sz[i](x)
            ,k));
            TZ[i]:= series(eval(SZ[i]),x=c,m);
            Z[i]:= eval(solve({seq(coeff(TZ[i],x-c,j),j=0..m-n-1)},
            [seq(a[j],j=n..m-1)]))[1];
            z[i]:=unapply( 1/((i)!)* (x-c)^(i-1)+subs(Z[i],sz[i](x))
            ,x);
        end do;

        #compute the general polynomial T1 in y_i
        T1:=0;
        for i from b to m do
                v:=eval(inttovec(i,ordL));
                summand:=1;
                for j from 1 to ordL do
                        summand:=summand*y[j](x)^v[j];
                end do;
                T1:=T1+h[i]*summand;
        end do;

        H2:=table();
        for i from 1 to n do
                Rel := series(T1-z[i](x),x=c,m);
                H2[i]:=solve({seq(coeff(Rel,x-c,j),j=0..m-1)},[seq(h[j
                    ],j=b..m)])[1];
        end do;

        for i from b to m do
                print([inttovec(i,ordL), i]);
        end do;
for i from 1 to n do
    print(H2[i]);
end do;
        return H2;
end proc;
```

## 6.3 Swap Algorithm

**Input:** Two linear differential operators $L_1, L_2$ and a cyclic vector $w_0$ for the corresponding SOE.

**Output:** Nothing, if $w_0$ is not cylcic or $L_1$ and $L_2$ don't swap. Otherwise returns, two linear differential operators $K_1, K_2$ with $L_i \sim K_i$ for $= 1, 2$ and a Boolean variable similar. The

variable similar is `true` if and only if $L_1 \sim L_2$.

```
swap := proc (L1, L2, w0)

        local n1,n2,C, B, A, Eq, Res, c, b, Zeile, Coefficients, ode,
            i, j, k, l, T, v, Sols, SolsRat, Yl, Y, Pivott, B1, C1, K,
            R, Coeffs1, Coeff1Size, Solve, Remainder, K1, K2, similar;
        uses  LinearAlgebra;
        n1 := order(L1);
        n2 := order(L2);

        if nops(DFactor(L1)) > 1 then
                print("first operator is reducible");
                return;
        end if;
        if nops(DFactor(L2)) > 1 then
                print("second operator is reducible");
                return;
        end if;

        similar := false;
        C := add(c[k](x)*Dx^k, k = 0 .. n2-1);
        B := add(b[k](x)*Dx^k, k = 0 .. n1-1);
        Eq := seq(coeff(convert(diffop2de(sort(mult(C, L1)+mult(L2, B)
            -1, [Dx]), y(x)), D), ((Di)(y))(x), 1), i = 0 .. n1+n2-1);

        Res := solve({seq(Eq[i], i = n1+1 .. n1+n2)}, [seq(c[i](x), i
            = 0 .. n2-1)]);
        Res := Res[1];
        Eq := seq(subs(Res, Eq[k]), k = 1 .. n1+n2);

        A := Matrix(n1*n2+1, n1*n2+1);
        for k to n1*n2 do A[k, k+1] := 1 end do;
        Zeile[n2] := -Matrix(1, n1*n2, [seq(seq(coeff(Eq[1], ((Dj)(b[i
            ]))(x), 1), j = 0 .. n2-1), i = 0 .. n1-1)])/coeff(Eq[1],
            ((Dn2)(b[0]))(x), 1);
        Zeile[n2] := Matrix(1, n1*n2+1, [Zeile[n2], 1]);
        for l from 2 to n1 do
                Zeile[n2*l] := -Matrix(1, n1*n2+1, [seq(seq(coeff(Eq[l
                    ], ((Dj)(b[i]))(x), 1), j = 0 .. n2-1), i = 0 .. n1
                    -1), 0])/coeff(Eq[l], ((Dn2)(b[l-1]))(x), 1)
        end do;

        for k from 1 to n1*n2+1 do
                for l to n1 do
                        A[n2*l, k] := Zeile[n2*l][1, k]
                 end do
        end do;

        A := Transpose(A);
        v[0] := Matrix(n1*n2+1, 1);
        for i from 1 to n1*n2+1 do
                v[0][i, 1] := w0[i, 1]
        end do;
        for i from 1 to n1*n2+1 do
```

```
        v[i] := simplify(MatrixMatrixMultiply(A, v[i-1])+map(
            diff, v[i-1], x))
end do;

if Determinant(Matrix([seq(v[i], i = 0 .. n1*n2)])) = 0 then
    print("Vector is not cylic"); return;
end if;

T := Matrix([seq(v[i], i = 0 .. n1*n2+1)]);
Coefficients := NullSpace(T);

ode := add((diff(g(x), `$`(x, i)))*Coefficients[1][i+1], i = 1
    .. n1*n2+1)+g(x)*Coefficients[1][1];
T := (LinearAlgebra[MatrixInverse](Matrix([seq(v[i], i = 0 ..
    n1*n2)])));
Sols := Vector(n1*n2+1); SolsRat := ratsols(ode, g(x));
if nops(SolsRat) = 0
        then print("no rational solutions found");
        return {};
end if;
for i to nops(SolsRat) do
        Sols[i] := SolsRat[i]
end do;

Yl := Matrix(n1*n2+1, n1*n2+1);
for i from 1 to n1*n2+1 do
        Yl[1, i] := Sols[i];
        for j from 1 to n1*n2 do
                Yl[j+1, i] := diff(Sols[i], `$`(x, j))
        end do;
end do;
Y := simplify(MatrixMatrixMultiply(Transpose(T), Yl));
Pivott := 0;
for i from 1 to n1*n2+1 do
        if Y[n1*n2+1, i] <> 0 then
                Pivott := i;
        end if;
end do;

if Pivott <> 0 then
        Y := Y/Y[n1*n2+1, Pivott];
end if;


NonZeroColumn:=0;
for i from 1 to n1*n2+1 do
        for j from 1 to n1*n2+1 do
                if Y[j,i] <> 0 and i <> Pivott then
                        similar := true;
                        NonZeroColumn:=i;
                end if;
        end do;
end do;
```

```
        print(Y);

        if Pivott = 0 then
                print("Operators are similar but dont swap");
                B1 := eval(subs(seq(b[i](x) = Y[1+i*n2, NonZeroColumn
                    ], i = 0 .. n1-1), B));
                C1 := eval(subs(seq(b[i](x) = Y[1+i*n2, NonZeroColumn
                    ], i = 0 .. n1-1), convert(subs(Res, C), diff)));
                return(B1,C1);
        end if;
        B1 := eval(subs(seq(b[i](x) = Y[1+i*n2, Pivott], i = 0 .. n1
            -1), B));

        C1 := eval(subs(seq(b[i](x) = Y[1+i*n2, Pivott], i = 0 .. n1
            -1), convert(subs(Res, C), diff)));

        K := Dx^n1+add(a[k](x)*Dx^k, k = 0 .. n1-1);
        R := rightdivision(mult(K, B1), L1);
        Remainder := simplify(R[2]);
        Coeffs1 := dcoeffs(diffop2de(Remainder, g(x)), g(x));
        Coeff1Size := nops([Coeffs1]);
        if 1 < Coeff1Size then
                Solve := solve({seq(Coeffs1[i], i = 1 .. Coeff1Size)},
                     [seq(a[i](x), i = 0 .. n1-1)]);
        else
                Solve := solve({seq(Coeffs1, i = 1 .. Coeff1Size)}, [
                    seq(a[i](x), i = 0 .. n1-1)]);
        end if;
        K1 := subs(Solve[1], K);

        K2 := rightdivision(mult(L1, L2), K1);

        K2 := simplify(K2[1]);
        return (K2, K1, similar ,Y,B1);
 end proc;
end module;
```

## 6.4 Further Implementations

This section contains further implementations, which are required by the previous algorithms. Most of them are straightforward and as one would expect them to be. However for the sake of completeness we state them here.

### 6.4.1 Matrix to Differential Operator

**Input:** A matrix $B \in \mathbb{C}(x)$ and a cyclic vector $w$ for $B$.
**Output:** A linear differential operator corresponding to $B$ in the sense of lemma 3.7.

```
matrix2op := proc(B, w)
        local A,n,v,i,T,dB, Coeff, L;

        A:=Transpose(B);
        n:=Dimension(A)[1];
```

```
        v[0]:=Matrix(n,1);

        for i from 1 to n do
                v[0][i,1]:= w[i,1];
        end do;
        for i from 1 to n do
                v[i]:= simplify(MatrixMatrixMultiply(A, v[i-1])
                +map(diff, v[i-1], x));
        end do;
        T:=Matrix([seq(v[i],i=0..n-1)]);
        dB:=Determinant(T);
        if dB=0 then
                print("Vector is not cyclic!"); return;
        end if;
        T:=Matrix([seq(v[i],i=0..n)]);

        Coeff:= NullSpace(T);

        L:= add( Coeff[1][i+1]*Dx^i, i=1..n)+Coeff[1][1];
        return L;
end proc;
```

### 6.4.2 Differential Operator to Matrix

**Input:** A monic differential operator $L_1$.
**Output:** The companion matrix $A_{L_1}$ corresponding to $L_1$.

```
op2matrix := proc( L1)
        local d,A,i;
        if LC(L1) <> 1 then
                print("Differential operator is not monic!");
                return;
        end if;
        d := order(L1);
        A:=Matrix(d,d);
        for i from 1 to d-1 do
                A[i,i+1]:=1;
        end do;
        for i from 1 to d do
                A[d,i]:= -coeff(L1,Dx,i-1);
        end do;
        return A;
end proc;
```

### 6.4.3 Order of a Differential Operator

**Input:** A linear differential operator $L$.
**Output:** The order of $L$.

```
order := proc (L1)
        local ssum, i;
        i := 0;
        ssum := 0;
```

```
        while simplify(L1 - ssum) <> 0 do
                ssum := ssum + coeff(convert(diffop2de(
                sort(L1, [Dx]), y(x)), D),
                ((Di)(y))(x), 1)*Dx^i;
                i:= i+1;
        end do;
        return i-1;
end proc;
```

### 6.4.4 Leading Coefficient of a Differential Operator

**Input:** A linear differential operator $L = \sum_{i=0}^{n} a_i \delta^i$ with $a_n \neq 0$.
**Output:** The leading coefficient $a_n$

```
LC := proc (L1)
        local n1;
        n1 := order(L1);
        return coeff(convert(diffop2de(sort(L1, [Dx]), y(x)), D), ((D
            n1)(y))(x), 1);
end proc;
```

### 6.4.5 Find a similar Differential Operator

**Input:** A linear differential operator $L$ of order $n > 1$ and a vector $w \in \mathbb{C}(x)^n$.
**Output:** A linear differential operator, whose solution space is spanned by $\sum_{i=0}^{n} w_i \delta^i(y)$ for any solution $y$ of $L$.
This algorithm was taken from [Sin96, p.20]

```
findSim := proc (L,w)
        local n1,eq, i, Z, S,T, c,EQ, Coeffs, L1;
        n1 := order(L);

        if n1 = 1 then
                print("works only for differential operators of order
                    >1");
                return 1;
        end if;

        Coeffs := LC(L);
        L1 :=  1/Coeffs* L;
        Z[0] := add( w[i,1]*Dx^(i-1), i=1..n1);
        for i from 1 to n1 do
                Z[i]:= mult(Dx,Z[i-1]);
        end do;


        S[0]:= Dx^n1 = -L1 + Dx^n1;
        for i from 1 to n1 do
                S[i] := Dx^(n1+i) = -mult(Dx^i,L1)+ Dx^(n1+i);
        end do;

        # Reverse the order of S. Necessary for subs to work correctly
        for i from 0 to n1 do
                T[i]:=S[n1-i];
```

```
        end do;

        eq := add( c[i](x)*Z[i], i=0..n1-1);
        eq := (eq+ Z[n1]);
        eq := subs( seq( T[i],i=0..n1),eq);
        EQ := seq(coeff(convert(diffop2de(sort(eq, [Dx]),  y(x)), D),
            ((Di)(y))(x), 1), i = 0 .. n1-1);
        EQ := solve( {seq(EQ[i],i=1..n1)},[seq(c[n1-i](x),i=1..n1)])
            [1];
        return subs(EQ, add(c[i](x)*Dx^(i),i=0..n1-1)+Dx^n1     );
end proc;
```

# Bibliography


[Abr89] S. A. Abramov, *Rational solutions of linear differential and difference equations with polynomial coefficients*, Zh. Vychisl. Mat. i Mat. Fiz. **29** (1989), no. 11, 1611–1620, 1757. MR 1025995 (90m:39002)

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR MR0242802 (39 #4129)

[Bek94] Emanuel Beke, *Die Irreducibilität der homogenen linearen Differentialgleichungen*, Math. Ann. **45** (1894), no. 2, 278–294. MR 1510863

[Beu00] Frits Beukers, *The maximal differential ideal is generated by its invariants*, Indag. Math. (N.S.) **11** (2000), no. 1, 13–18. MR 1809657 (2001j:12004)

[Bor91] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. MR 1102012 (92d:20001)

[BW93] Thomas Becker and Volker Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993, A computational approach to commutative algebra, In cooperation with Heinz Kredel. MR 1213453 (95e:13018)

[CH11] Teresa Crespo and Zbigniew Hajto, *Algebraic groups and differential Galois theory*, Graduate Studies in Mathematics, vol. 122, American Mathematical Society, Providence, RI, 2011. MR 2778109 (2012b:12008)

[CLO07] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, third ed., Undergraduate Texts in Mathematics, Springer, New York, 2007, An introduction to computational algebraic geometry and commutative algebra. MR MR2290010 (2007h:13036)

[Com98] Elie Compoint, *Differential equations and algebraic relations*, J. Symbolic Comput. **25** (1998), no. 6, 705–725. MR 1631355 (2000a:12006)

[CS99] Elie Compoint and Michael F. Singer, *Computing Galois groups of completely reducible differential equations*, J. Symbolic Comput. **28** (1999), no. 4-5, 473–494, Differential algebra and differential equations. MR 1731934 (2000m:12010)

[CSTU02] Olivier Cormier, Michael F. Singer, Barry M. Trager, and Felix Ulmer, *Linear differential operators for polynomial equations*, J. Symbolic Comput. **34** (2002), no. 5, 355–398. MR 1937466 (2003j:13035)

[CW04a] É. Compoint and J. A. Weil, *Absolute reducibility of differential operators and Galois groups*, J. Algebra **275** (2004), no. 1, 77–105. MR 2047442 (2005c:12009)

[CW04b] ———, *Absolute reducibility of differential operators and Galois groups*, J. Algebra **275** (2004), no. 1, 77–105. MR 2047442 (2005c:12009)

[DGP99] Wolfram Decker, Gert-Martin Greuel, and Gerhard Pfister, *Primary decomposition: algorithms and comparisons*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 187–220. MR 1672046 (99m:13049)

[Dub90] Thomas W. Dubé, *The structure of polynomial ideals and Gröbner bases*, SIAM J. Comput. **19** (1990), no. 4, 750–775. MR MR1053942 (91h:13021)

[Duc09] Alina N. Duca, *The socle series of indecomposable injective modules over a principal left and right ideal domain*, Rings, modules and representations, Contemp. Math., vol. 480, Amer. Math. Soc., Providence, RI, 2009, pp. 101–132. MR 2508147 (2011b:16012)

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116)

[Hei12] Albert Heinle, *Factorization, similarity and matrix normal forms over certain ore domains*, Master's thesis, RWTH Aachen, 2012.

[Hru02] Ehud Hrushovski, *Computing the Galois group of a linear differential equation*, Differential Galois theory, Banach Center Publ., vol. 58, Polish Acad. Sci., Warsaw, 2002, pp. 97–138. MR MR1972449 (2004j:12007)

[Hum75] James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York-Heidelberg, 1975, Graduate Texts in Mathematics, No. 21. MR 0396773 (53 #633)

[Kat87] Nicholas M. Katz, *A simple algorithm for cyclic vectors*, Amer. J. Math. **109** (1987), no. 1, 65–70. MR 878198 (88b:13001)

[Kov86] Jerald J. Kovacic, *An algorithm for solving second order linear homogeneous differential equations*, J. Symbolic Comput. **2** (1986), no. 1, 3–43. MR 839134 (88c:12011)

[Ore32a] Oystein Ore, *Formale theorie der linearen differentialgleichungen. (erster teil)*, Journal fr die reine und angewandte Mathematik (Crelle's Journal), 1932, pp. 221–234, Heft 167.

[Ore32b] Öystein Ore, *Formale theorie der linearen differentialgleichungen. (zweiter teil).*, Journal für Mathematik **168** (1932(?)), 233–252 (ger).

[Ore33] Oystein Ore, *Theory of non-commutative polynomials*, Ann. of Math. (2) **34** (1933), no. 3, 480–508. MR 1503119

[OV90] A. L. Onishchik and È. B. Vinberg, *Lie groups and algebraic groups*, Springer Series in Soviet Mathematics, Springer-Verlag, Berlin, 1990, Translated from the Russian and with a preface by D. A. Leites. MR MR1064110 (91g:22001)

[Poo60] E. G. C. Poole, *Introduction to the theory of linear differential equations*, Dover Publications Inc., New York, 1960. MR 0111886 (22 #2746)

[Sin81] Michael F. Singer, *Liouvillian solutions of nth order homogeneous linear differential equations*, Amer. J. Math. **103** (1981), no. 4, 661–682. MR 623132 (82i:12028)

[Sin93] ———, *Moduli of linear differential equations on the Riemann sphere with fixed Galois groups*, Pacific J. Math. **160** (1993), no. 2, 343–395. MR 1233356 (94k:12009)

[Sin96] ———, *Testing reducibility of linear differential operators: a group-theoretic perspective*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 2, 77–104. MR 1462491 (98e:12007)

[Spr09] T. A. Springer, *Linear algebraic groups*, second ed., Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2009. MR MR2458469 (2009i:20089)

[Sta73] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996. MR 0327712 (48 #6054)

[SU97] Michael F. Singer and Felix Ulmer, *Linear differential equations and products of linear forms*, J. Pure Appl. Algebra **117/118** (1997), 549–563, Algorithms for algebra (Eindhoven, 1996). MR 1457855 (98g:12010)

[Tsa96] S. P. Tsarev, *An algorithm for complete enumeration of all factorizations of a linear ordinary differential operator*, Proceedings of the 1996 international symposium on Symbolic and algebraic computation (New York, NY, USA), ISSAC '96, ACM, 1996, pp. 226–231.

[TY05] Patrice Tauvel and Rupert W. T. Yu, *Lie algebras and algebraic groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005. MR MR2146652 (2006c:17001)

[vdPS03] Marius van der Put and Michael F. Singer, *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 328, Springer-Verlag, Berlin, 2003. MR MR1960772 (2004c:12010)

[VGS+97] Wolmer V. Vasconcelos, Daniel R. Grayson, Michael Stillman, David Eisenbud, and Jüurgen Herzog, *Computational methods in commutative algebra and algebraic geometry*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1997.

[vH97] Mark van Hoeij, *Factorization of differential operators with rational functions coefficients*, J. Symbolic Comput. **24** (1997), no. 5, 537–561. MR 1484068 (98j:12007)

[vHW97] Mark van Hoeij and Jacques-Arthur Weil, *An algorithm for computing invariants of differential Galois groups*, J. Pure Appl. Algebra **117/118** (1997), 353–379, Algorithms for algebra (Eindhoven, 1996). MR 1457846 (98k:12005)

# Index